МВД РЕСПУБЛИКИ КАЗАХСТАН
КАРАГАНДИНСКАЯ АКАДЕМИЯ МВД РК
им. БАРИМБЕКА БЕЙСЕНОВА
ЮРИДИЧЕСКИЙ ИНСТИТУТ
КАФЕДРА ДОСУДЕБНОГО РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ

«УТВЕРЖДАЮ»
Начальник кафедры
досудебного расследования преступлений
Карагандинской академии
МВД РК им. Б. Бейсенова
к.ю.н., полковник полиции
А.К. Калиев
«____» _____ 2018 г.

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ПО ДИСЦИПЛИНЕ

RUPSSKIVT 4315 «Расследование уголовных правонарушений, связанных в сфере компьютерной информации и высоких технологий»
Специальность: 5В030300 - «Правоохранительная деятельность»

форма обучения: ФЗО
курс: 4 (н.2017) ВНЮР
4 (н.2017) СЮР
количество кредитов: 1 (45 часов)
лекций: 4
семинарских занятий: 3
практических занятий: 2
СРОП: 1
СРОП: 35

Караганда 2018

Учебно-методический комплекс по дисциплине «Расследование уголовных правонарушений, связанных в сфере компьютерной информации и высоких технологий»

Составитель: доцент кафедры досудебного расследования преступлений, майор полиции Кемпирова Ж.С.

В результате освоения дисциплины «Расследование уголовных правонарушений, связанных в сфере компьютерной информации и высоких технологий» обучающиеся получат глубокие теоретические знания и практические умения и навыки структурного анализа доказательств, применения методов проверки доказательств и структур вспомогательных комплексов, систем доказательств, версий и оценки их роли в построении систем доказательств, что поможет достичь высокой эффективности в раскрытии и расследовании преступлений по делам данной категории.

Рассмотрен на заседании кафедры досудебного расследования преступлений «__» _____ 2018 г., Протокол №____

Начальник кафедры досудебного
расследования преступлений
к.ю.н., полковник полиции Калиев А. К.

Утверждена на заседании УМС «__» _____ 2018 г. Протокол №____

Министерство внутренних дел Республики Казахстан

Карагандинская академия им. Баримбека Бейсенова

Юридический институт

Кафедра досудебного расследования преступлений

«Утверждаю»
Заместитель начальника академии
по учебной работе
д.ю.н., профессор
полковник полиции
_____ З.С. Токубаев

«_____»_____2018 г.

Рабочая учебная программа (SYLLABUS)
по дисциплине

RUPSSKIVT 4215 «Расследование уголовных правонарушений связанных в сфере компьютерной информации и высоких технологий»

Специальность: 5В030300 Правоохранительная деятельность

форма обучения – ФЗО
курс: 4 (н.2017) ВНЮР
количество кредитов: 1 (45 часов)
лекций: 4
семинарских занятий: 3
практических занятий: 2
СРОП: 1
СРОП: 35
форма контроля – экзамен

Караганда 2018

Рабочая учебная программа (SYLLABUS) по дисциплине «Расследование уголовных правонарушений связанных в сфере компьютерной информации и высоких технологий» для специальности 5В030300 «Правоохранительная деятельность».

Составитель: доцент кафедры досудебного расследования преступлений, майор полиции Кемпирова Ж.С.

Рассмотрен на заседании кафедры_____

«__»_____ 2018 г., протокол №__

Начальник кафедры
Досудебного расследования преступлений
полковник полиции Калиев А.К.

Утверждена на заседании УМС_____

«__»_____ 2018 г., протокол №__

2.1. Основная информация:

1. Шифр и название специальности	5В030300 «Правоохранительная деятельность»
2. Курс, семестр	4 курс (н.2017) ВНЮР
3. Цикл дисциплины	Компонент по выбору. RUPSSKIVT 4215
4. Количество кредитов	1
5. Место проведения занятий	Учебные аудитории, лекционный зал
6. Лекторы (Ф.И.О., должность, ученая степень, др. контактная информация)	Доцент кафедры досудебного расследования преступлений Ногайбаева Алтынай Сансызбаевна; старший преподаватель кафедры досудебного расследования преступлений Хасенов Ербол Амантаевич; контактный телефон – 30-34-03, внут.- 333, 307.
7.Преподаватели, ведущие остальные виды занятий (Ф.И.О., должность, ученая степень, др. контактная информация)	Преподаватели кафедры досудебного расследования преступлений.

2.2. Пререквизиты: Теория государства и права. Нормы права. Система права и ее структура. Толкование норм права. Правовые отношения. Правонарушения и юридическая ответственность. Правоохранительные органы: Прокуратура РК. Органы внутренних дел РК. Органы досудебного расследования в РК. Уголовное право РК. Часть общая: Понятие преступления. Состав преступления. Уголовная ответственность и ее основания. Субъект преступления. Обстоятельства, исключающие уголовную ответственность. Стадии преступления. Соучастие в преступлении. Понятие, цели, система и виды наказаний. Назначение наказания. Освобождение от уголовной ответственности и наказания. Отсрочка исполнения наказания. Погашение и снятие судимости. Принудительные меры медицинского характера. Уголовное право. Часть особенная. Все разделы.

2.3. Постреквизиты: «Досудебное расследовани», «Криминалистика», «Прокурорский надзор в РК», «Уголовный процесс», «Основы оперативно-розыскной деятельности», «Судебная риторика», «Основы судебной медицины и психиатрии».

2.4. Краткое описание дисциплины

Цель: подготовка обучающихся по специальности 5В030300 - «Правоохранительная деятельность», которые способны после окончания института выполнять поставленные перед правоохранительными органами задачи по предупреждению, раскрытию и расследованию уголовных правонарушений. Кроме того, изучение обучающимися данной дисциплины

способствует в дальнейшем развитие навыков в составлении процессуальных документов.

В процессе изучения данной учебной дисциплины обучающийся должен:

- закрепить имеющиеся теоретические знания и практические навыки с учетом происшедших изменений и дополнений в уголовном и уголовно-процессуальном законодательстве;

- выработать умение и навыки применения уголовно-процессуальных норм в штатных и нештатных ситуациях, связанных с расследованием уголовных дел по осуществлению взаимодействия с другими правоохранительными органами РК;

- закрепить убежденность в необходимости строжайшего соблюдения законности и недопустимости любого нарушения закона, чем бы оно, не мотивировалось; совершенствовать навыки по составлению организационно-распорядительных документов и деловых бумаг следователя, оформлять материалы уголовного дела и приложения к нему.

знать:

— нормы права, имеющие основополагающее значение для достижения задач уголовного судопроизводства;

— теоретические основы квалификации общеуголовных правонарушений;

— основы раскрытия и расследования уголовных правонарушений, отнесенных к подследственности органов досудебного расследования ОВД;

— основы взаимодействия с другими правоохранительными органами и с общественностью;

— основы форм и методов взаимодействия оперативных подразделений с другими службами в ходе предупреждения, раскрытия и расследования уголовных правонарушений;

— теоретические основы принятия процессуальных, тактических и организационных решений в ходе расследования;

— процессуальный порядок применения мер процессуального принуждения в отношении подозреваемых в совершении уголовных правонарушений;

— теоретические основы производства неотложных и первоначальных следственных действий;

— тактико-технические возможности криминалистической техники;

— общую характеристику оперативных и криминалистических учетов;

— перечень современных технико-криминалистических средств, методов и приемов фиксации, поиска, обнаружения, изъятия и исследования вещественных доказательств в целях раскрытия и расследования уголовных правонарушений;

уметь:

— правильно применять нормы права, имеющие основополагающие значения для достижения задач уголовного судопроизводства;

— принимать уголовно-процессуальные, тактические и организационные решения;

— оформлять и использовать сведения, полученные в процессе проведения оперативно- розыскных мероприятий;

— составлять статистические карточки и пользоваться оперативными и криминалистическими учетами;

— использовать технико-криминалистические средства, методы и приемы фиксации, поиска, обнаружения, изъятия и исследования вещественных доказательств в целях раскрытия и расследования уголовных правонарушений;

— разрабатывать и выдвигать следственные версии, обеспечивающие раскрытие уголовных правонарушений и установление виновных лиц;

— организовывать и проводить следственные действия в соответствии с уголовно- процессуальным законодательством;

— осуществлять взаимодействие со службами и подразделениями правоохранительных органов Республики Казахстан и других стран;

— обеспечивать реализацию прав и исполнение обязанностей участниками процесса, принимать меры к обеспечению безопасности;

— исчислять процессуальные сроки и решать вопросы об их продлении;

Дисциплина изучается обучающимися на 4 курсе. В конце обучающиеся сдают экзамен. Основными формами обучения являются лекции, семинарские и практические занятия, СРОП.

На занятиях для усвоения и закрепления навыков практической работы в сфере уголовного судопроизводства обучающиеся решают ситуационные задачи, составляют процессуальные документы.

Ожидаемые результаты: Изучение данной дисциплины способно привить умения и навыки проведения следственных действий, закрепления результатов, составления наиболее сложных процессуальных документов и деловых бумаг следователя. Приобретение данных навыков позволит в практической деятельности самостоятельно проводить расследование по уголовным делам.

2.5. График выполнения и сдачи заданий по дисциплине:

№	Виды работ	Цель и содержание задания	Ссылка на список рекомендованной	Форма контроля (согласно рейтинг-шкале)	Баллы (согласно рейтинг-шкале)	Форма отчетности	Сроки сдачи
1	2	3	4	5	6	7	8
1	1.Проверка конспектов. 2.Решение задач	Текущий контроль			0-100	Ответ Конс-пект	по расписанию

2.	1. Проверка конспектов 2. Опрос по теме 3.Решение задач	Текущий контроль			0-100	Ответ Конс-пект	по расписанию
3.	1. Проверка конспектов 2. Опрос по теме 3.Решение задач	Текущий контроль			0-100	Ответ Конс-пект Тест	по расписанию

2.6. Политика курса.

а) обязательное посещение всех аудиторных и внеаудиторных занятий СРОП согласно расписания.

б) регулярная подготовка к занятиям;

в) активность во время семинарских, практических и СРОП занятий

г) отработка в определенное преподавателем время пропущенных занятий;

д) соблюдение дисциплины.

Недопустимо:

а) опоздание и уход с занятий;

б) несвоевременная сдача заданий;

в) пользование сотовыми телефонами во время занятий, посторонние разговоры, жевание жевательной резинки;

г) обман и плагиат.

2.7. Список рекомендованной литературы

№ п/п	Автор, наименование	Год, место издания
1. Нормативные правовые акты		
1	Конституция РК принятая на республиканском референдуме 30 августа 1995 г. (с изменениями и дополнениями на 10.03.2017г.).	//http://online.zakon.kz.
2	Уголовный кодекс Республики Казахстан № 226-v-ЗРК от 03.07. 2014г. (с изменениями и дополнениями по состоянию на 09.01.2018 г.).	//http://online.zakon.kz.
3	Уголовно-процессуальный кодекс Республики Казахстан № 231-V-ЗРК от 04.07.2014г. (с изменениями и дополнениями по состоянию на 24.05.2018 г.).	//http://online.zakon.kz.
4	Закон республики казахстан от 23 апреля 2014 года № 199-v «об органах внутренних дел Республики Казахстан» (с изменениями и дополнениями по	//http://online.zakon.kz.

	состоянию на 24.05.2015 г.).	
5	Приказ Генерального прокурора Республики Казахстан от 22 сентября 2014 года №91 «Об утверждении Правил применения научно-технических средств фиксации хода и результатов следственных действий»	//http://online.zakon.kz.
6	Приказ Генерального Прокурора Республики Казахстан «Об утверждении правил приема и регистрации заявлений и сообщений об уголовных правонарушениях, а также ведения Единого реестра досудебных расследований» №89 от 19.09.2014г. с изм. и доп. от 10.08.2015 г. №99, 23.09.2016 №148.	//http://online.zakon.kz.
7	Приказ Генерального Прокурора Республики Казахстан «Об утверждении Положения о Департаменте по надзору за законностью досудебной стадии уголовного процесса ГП» № 125 от 09.10.2012г.	//http://online.zakon.kz.
8	Приказ Генерального Прокурора Республики Казахстан «Об усилении прокурорского надзора за соблюдением конституционных прав и свобод человека и гражданина в уголовном процессе» № 46 от 17.08.2006г.	//http://online.zakon.kz.
9	Инструкции «О порядке изъятия, учета, хранения, передачи и уничтожения вещественных доказательств, документов по уголовным делам, гражданским делам и делам об административных правонарушениях судом, органами прокуратуры, досудебного следствия, дознания и судебной экспертизы». Совместный приказ Министра юстиции Республики Казахстан от 12 ноября 1998 г. N 121, Генерального прокурора Республики Казахстан от 1 декабря 1998 года N 1043ца, Председателя КНБ Республики Казахстан от 8 декабря 1998 года N 73, Министра финансов Республики Казахстан от 22 декабря 1998 года N 598, Министра внутренних дел Республики Казахстан от 2 декабря 1998 года N 429, Министра государственных доходов Республики Казахстан от 28 декабря 1998 года N 111. Зарегистрирован Министерством юстиции Республики Казахстан 30.12.1998 г. N 658	//http://online.zakon.kz.
10	Закон Республики Казахстан от 30.03.1999 N 353-I ЗРК "О порядке и условиях содержания лиц в специальных учреждениях, обеспечивающих временную изоляцию от общества"	//http://online.zakon.kz.

11	Закон Республики Казахстан от 10 июля 1998 года № 279-I о наркотических средствах, психотропных веществах, прекурсорах и мерах противодействия их незаконному обороту и злоупотреблению ими (с изменениями и дополнениями по состоянию на 29.12.2014 г.)	//http://online.zakon.kz.
12	Нормативное Постановление Верховного суда РК от 20.04.2006 N 4 "О некоторых вопросах оценки доказательств по уголовным делам"	//http://online.zakon.kz.
13	Приказ Министра внутренних дел Республики Казахстан от 6 мая 2004 года № 256 О внесении изменений и дополнений в приказ Министра внутренних дел Республики Казахстан от 6 июля 2001 года № 543 «О мерах по совершенствованию деятельности следствия, дознания, оперативно-криминалистической службы органов внутренних дел Республики Казахстан»	//http://online.zakon.kz.
14	Закон Республики Казахстан «О судебно-экспертной деятельности в Республике Казахстан» (с изменениями и дополнениями по состоянию на 29.09.2014 г.)	//http://online.zakon.kz.
15	Приказ Генерального Прокурора Республики Казахстан от 02 мая 2018 года № 60 «О некоторых вопросах организации прокурорского надзора».	//http://online.zakon.kz.
	2. Основная литература	
16	Назарбаев Н.А. «Новые возможности развития в условиях четвертой промышленной революции». Послание Президента Республики Казахстан народу Казахстана от 10 января 2018 года.	Официальный сайт Президента Республики Казахстан. //http://www.akorda.kz/
17	Капсалямов К.Ж. Уголовное преследование и способы собирания доказательств.	Астана, 2001.
18	Бекжанов А.А., Ташибаев К.У., Турсынов Е.Т. Производство дознания по УПК РК.	Караганда, 1998.
19	Сарсенбаев Т.Е., Хан А.Л. Уголовный процесс. Досудебное производство.	Астана, 2000.
20	Тяжина А.О., Ногайбаева А.С. Новеллы досудебного расследования по УПК Республики Казахстан: учебно-практическое пособие (краткий анализ в схемах)	Караганда, 2015.
21	Тяжина А.О., Ногайбаева А.С., Бейсенбаев А.Ж. Досудебное производство по уголовным делам: образцы процессуальных документов.	Караганда, 2014.
22	Кенжетаев Д.Т., Калиев А.К., Балтабаев Т.Н.	Караганда, 2014.

	Примерные образцы уголовно-процессуальных документов досудебного расследования.	
23	Громов В.И. Заключение эксперта как источник доказательства.	М.://Юстиция.1997. № 9
24	Шурухнов Н.Г. Тактика следственного осмотра и освидетельствования Криминалистика: Курс лекций.	Москва: Эксмо. 2006.
25	Журсимбаев С.К. Роль прокурора при отправлении уголовного правосудия.	Алматы, 2002 год.
	3. Дополнительная литература	
26	Руководство для следователей/ Под ред. Н.А. Селиванова В.А., Снеткова.	Москва, 1998 г.
27	Бахин В., Когамов М., Карпов Н. Допрос на предварительном следствии (уголовно – процессуальные и криминалистические вопросы): Монография. Изд. 2-е.	Алматы: Жеті жарғы, 2004. 192с.
28	Диков Д., Сейгер К., Фонстрох У. Компьютерные преступления	Москва, 1999 г.
29	Ляпунов Ю.И., Максимов В.С. Ответственность за компьютерные преступления	Москва,// Законность. 1997. № 1.
30	Бахарев Н.В. Очная ставка: уголовно процессуальные и криминалистические вопросы	Москва: Госюриздат1 983.
31	Гаврилов А.К. Следственные действия: (процессуальная характеристика, тактические и психологические особенности) А.К. Гаврилов, Б.П. Смагоринский.	Москва: ИКФ Экмос,1994 г.
32	Алиев Т.Т. Доказательства, понятие, свойства / Т.Т. Алиев, Н.А. Громов, А.И. Гришин // Закон и право.	А. - 2002 г. - №3.
33	Скоромников К.С. Расследование преступлений в сфере компьютерной информации // Руководство для следователей / Под ред. Н.А.Селиванова, В.А. Снеткова.	Москва, 1997.
34	Шуменова Р.Т. Система процессуальных гарантий обеспечения принципов уголовного судопроизводства. Монография.	Алматы, 2003 г. с.89
35	Бегалиев К. А Меры пресечения по УПК РК// Гос. и право.	Алматы, 2003 г.
36	Расследование неправомерного доступа к компьютерной информации. Научно-практической пособие / Под ред. Н.Г. Шурухнова.	Москва, 1999г.
37	Жалыбин С. М. Обеспечение прав человека при уголовном преследовании. - Правовая реформа в Казахстане.	Алматы – 2001г. № 1.

2.8. ТЕМАТИЧЕСКИЙ ПЛАН

по дисциплине «Расследование уголовных правонарушений, связанных в сфере компьютерной информации и высоких технологий» для преподавания обучающимся 4 курса ВНЮР (набор 2017 г.) факультета заочного обучения юридического института в 2018-2019 учебном году

Количество кредитов - 1 (45 часов)

№ п/п	Номер темы	Название темы	Кол-во кредитов (часов)	Аудиторные часы			СРОП		СРО
				лекции	семинарские занятия	практические занятия	аудиторные	внеаудиторны	
1	1	Общая характеристика досудебного расследования в сфере компьютерной информации и высоких технологий	15	1	1	1			12
2	2	Деятельность следователя по проверке законности и обоснованности повода к началу досудебного расследования в сфере компьютерной информации и высоких технологий	16	2	1	1			12
3	3	Процессуальный порядок определения статуса потерпевшего, организация и проведение допроса потерпевшего	14	1	1			1	11
Итого в семестре:			45	4	3	2		1	35

2.9. Планы занятий

Тема 1. Общая характеристика досудебного расследования в сфере компьютерной информации и высоких технологий

Лекция – 1 час

Цель занятия: выработка профессиональных навыков по принятию процессуальных решений, составлению сопутствующих процессуальных документов; привитие навыков по использованию законодательных и иных нормативных актов в работе с доказательствами; привитие уважительного отношения к закону.

План лекции

1. Понятие и значение преступления в сфере высоких информационных технологий.
2. Направления преступной деятельности в информационной сфере и их классификация.

Тезисы лекции:

Компьютерно-информационные технологии функционируют относительно давно, и их развитие происходит огромными темпами, что связано с большой заинтересованностью в этом широких слоев населения. Преступления, связанные с использованием компьютерной техники, - это лишь специализированная часть преступной деятельности в информационной сферы. К данной категории относятся и преступления, при совершении которых осуществляется неправомерный доступ к охраняемой законом компьютерной информации. В течение последних 15-20 лет по мере компьютеризации хозяйственно-управленческой и финансово коммерческой деятельности появились новые виды преступлений, которые стали называться компьютерными, исходя из терминологии зарубежной юридической практики. Первое преступление подобного типа в бывшем СССР было зарегистрировано в 1979 г. в городе Вильнюсе. Тогда ущерб государству составил около 80 тысяч рублей. Этот случай явился определенной отправной точкой в развитии и исследовании нового вида преступлений.

Только в последние годы появились работы по проблемам борьбы с компьютерной преступностью, в которых рассматриваются в основном уголовно-правовые и криминологические аспекты этого явления. Как нередко случалось уже ранее, например, ситуация с наркоманией или с организованной преступностью, борьба с этим социально опасным явлением началась лишь после того, как материальные потери от этого вида преступлений достигли существенных размеров и стали резко выделяться на общем фоне потерь от обычных видов обще уголовной преступности.

Для того чтобы четко определить суть проблемы, для любой науки вполне логичен подход, когда все исследователи конкретной предметной области организуют свое общение на основе единообразно понимаемых терминов и пытаются обеспечить некую стабильность понятий нотерминологического аппарата.

Так, А. В. Дулов к компьютерным преступлениям относит «различные преступления, совершаемые с помощью компьютеров, с нарушением их деятельности». Нам кажется, подобное определение является довольно

широким и содержащим существенную неточность: результатом компьютерного преступления не обязательно должно быть нарушение деятельности самих компьютеров. Общественно-опасные последствия могут наступать и при нормальном функционировании программно-аппаратных средств компьютера при условии неверных исходных данных, при ошибках оператора или программиста, при кражах машинного времени, неправомерном доступе и т. д.

Н. А. Селиванов относит к компьютерным преступлениям, преступления, предметом которых является компьютерная информация, либо средством совершения которых выступает электронно-вычислительная техника, используемая с целью совершения противоправного посягательства на иной объект. Опровергая данную точку зрения, В. В. Крылов считает, что подход, согласно которому в законодательстве следует отражать конкретные технические средства, себя не оправдывает и поэтому нецелесообразно принимать термин «компьютерные преступления» за основу для наименования в криминалистике всей совокупности преступлений в области информационных отношений. Компьютер, по его мнению, является лишь одной из разновидностей информационного оборудования и проблемами использования этого оборудования не исчерпывается совокупность отношений, связанных с обращением конфиденциальной документированной информации. В. В. Крылов предлагает рассматривать в качестве базового понятия «информационные преступления», исходя из того, что сложившаяся система правоотношений в области информационной деятельности позволяет абстрагироваться от конкретных технических средств. Он делает вывод, что преступления в области компьютерной информации, выделенные в отдельную главу УК, являются частью информационных преступлений, объединенных общим инструментом обработки информации — компьютером.

Ю.М. Батурин подразделяет объекты компьютерных атак натри категории сами компьютеры, объекты, которые могут быть атакованы с помощью компьютера как инструмента, объекты, для которых компьютер является окружением.

Представляется обоснованным не включать в состав объектов компьютерных преступлений первую категорию по данной классификации в случаях, когда компьютеры являются не более чем имуществом, абсолютно равнозначным любым другим материальным вещам, и не подлежат выделению в отдельную правовую категорию единственно по признаку их наименования.

Классической точки зрения о том, что рамки компьютерных преступлений можно ограничить использованием ПК в качестве инструмента (орудия) и предмета посягательства, придерживается и Н. Ф. Ахраменко, при этом указывает, что сам компьютер не может быть рассмотрен как предмет компьютерных преступлений, так как «предметом посягательств при их совершении является отнюдь не техника как таковая (ей ущерб, как правило, не наносится), а информация, хранимая, обрабатываемая или передаваемая

этой техникой. Определяя объект компьютерных посягательств, мы исходим из того, что преступления такого рода с гораздо большим основанием следует, отнести к информационным». На наш взгляд, предмет компьютерных преступлений следует еще больше расширить: помимо информации включить еще нормальное функционирование вычислительной техники и течение информационных процессов.

Несомненно, данный перечень мнений не является исчерпывающим, однако важно другое: необходимо различать преступления в сфере высоких информационных технологий и так называемые компьютерные преступления. К сожалению, последний термин настолько прочно вошел в обиход научных и практических работников, как в Казахстане, так и за рубежом, что стал уже традиционным, и некоторые авторы полагают, что вряд ли стоит его менять, «поскольку многие названия со временем приобретают условный характер».

Различие в терминологии указывает не только на обеспокоенность общества новой угрозой, но и на отсутствие полного понимания сути этой угрозы. Важно, что терминологическая неточность изложения закона или методологической рекомендации по его исполнению может повлечь неправильное его применение, а, следовательно, и негативные последствия.

Следует отметить, что общепризнанного определения преступления, совершаемого с ииспользованием или в отношении средств вычислительной техники, компьютерной информации, программного обеспечения, на сегодняшний день не имеется, вообще, а уголовное право иностранных государств охватывает этим понятием различные по своему характеру и степени общественной опасности виды противоправных деяний.

Наиболее распространенное определение — «преступление, совершенное с использованием компьютерной техники или направленное против безопасности компьютерной информации» — не отвечает потребностям науки и практики сегодняшнего дня и нуждается в уточнении.

К вопросу криминализации правонарушений в сфере высоких информационных технологий сегодня в мире существует три подхода.

Первый заключается в отнесении к преступлениям несанкционированного доступа в защищенные компьютерные системы, заражения вирусами, противоправного использования компьютерных систем и информации. Он характерен для таких стран, как Норвегия, Сингапур, Словакия, Филиппины, Южная Корея.

Второй подход заключается в признании компьютерными преступлениями лишь тех деяний, которые связаны с причинением ущерба имуществу и электронной обработке информации (Австрия, Дания, Швеция, Швейцария, Япония). Например, в законодательстве Австрии, Дании, предусматривается уголовная ответственность за неправомочное вмешательство в функционирование информационно-вычислительных систем.

Третий подход характерен для стран с высоким уровнем компьютеризации (США, Великобритания, Франция, Германия,

Нидерланды) и развитой правовой базой. Он состоит в криминализации деяний, связанных не только с имущественным ущербом, но и с нарушением прав личности, с угрозой национальной безопасности и т. д. Так, из содержания норм уголовного права Великобритании следует, что его санкции применяются к «злоумышленникам, причинившим с помощью ПК ущерб или использовавшим информацию в своих целях». В 80-е годы системой уголовной юстиции ФРГ был предложен целый ряд уголовно-правовых определений исследуемой категории противоправных деяний. Уголовная полиция этой страны к преступлениям в сфере высоких технологий относит «все противоправные действия, при которых электронная обработка информации является орудием их совершения и(или) их объектом».

Для того чтобы понять, что же представляет собой «охраняемая законом компьютерная информация», мы приведем краткий перечень некоторых видов информации, охраняемых законодательством Республики Казахстан, которые одновременно подлежат защите — государственные секреты; служебная и коммерческая тайна; банковская тайна; нераскрытая информация; личная и семейная тайны, тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений; тайна усыновления (удочерения) ребенка; адвокатская тайна; тайна пенсионных накоплений получателя.

При этом информация — это сведения или данные, объективно отражающие различные стороны и элементы окружающего мира и деятельности человека на определенном этапе развития общества, представляющие для него какой-либо интерес, и материализованные в форме, удобной для использования, передачи, хранения и обработки (преобразования) человеком или автоматизированными средствами.

«Охраняемая законом компьютерная информация», как вид информации, представляет собой сведения, зафиксированные на машинном, магнитном носителе, представленные в форме набора состояний элементов ПК, иных электронных средств обработки, хранения и передачи информации.

Компьютерная техника и средства коммуникаций на территории Республики Казахстан используются в большей степени не как объекты посягательства (для сравнения, неправомерный доступ к компьютерной информации, хищение машинного времени, а также денежных средств посредством электронной транзакции — вот далеко не полный перечень преступлений, с которыми вынуждены бороться правоохранительные органы США, Канады, стран Европы и т. д.), а в большей степени как средства преступной деятельности. Причина — высокая латентность данного вида преступлений и слабо развитые, а иногда даже отсутствующие компьютерно-информационные сети. За рубежом, например, активно борются с проблемой латентности.

Еще одна из причин роста таких преступлений в Казахстане — это разрыв в уровнях развития информационного общества по сравнению с Западом, порождающий иногда абсурдные ситуации, нестыковки моральных,

правовых стандартов и норм. Создаются условия для соблазна, искушения воспользоваться более удобной и дешевой формой обеспечения информацией. Взять, например, проблему сохранения интеллектуальной собственности. Лицензионные программы стоят очень дорого для массового потребителя, и нет моральных преград, пользоваться «взломанными» программами, которые во много раз дешевле.

Одним из новых направлений для преступной деятельности в информационной сфере является использование глобальных коммуникационных информационных систем с удаленным доступом к совместно используемым ресурсам сетей, таких как Интернет. В настоящее время Интернет, использующий в большинстве случаев телефонные линии, представляет собой глобальную систему обмена информационными потоками, объединяющую около 30000 мелких локальных сетей и более 30 миллионов пользователей, число которых постоянно растет. Вполне закономерно, что подобная информационная сеть, объединившая огромное число людей с возможностью подключения к ней любого человека, стала не только предметом преступного посягательства, но и очень эффективным средством совершения преступлений.

Используя Интернет в качестве среды для противоправной деятельности, преступники очень часто делают акцент на возможности, которые им дает сеть, обмена информацией, в том числе и криминального характера. Аналогичная ситуация складывается и при использовании компьютерных мини процессоров, составляющих основу современной мобильной или так называемой сотовой телефонной связи. Однако следует отметить, что большинство ее видов при эксплуатации позволяют оперировать лишь аудио и небольшими по объему частями текстовой информации, в то время как подключение этих устройств к цифровым каналам Интернет позволяет передавать не только аудио-, но и видеоинформацию, а также практически не ограниченные объемы текстовой и графической информации.

Другая черта сети Интернет, которая привлекает преступников, - возможность осуществлять в глобальных масштабах информационно психологическое воздействие на людей. Преступное сообщество весьма заинтересовано в распространении своих доктрин и учений, в формировании общественного мнения, благоприятного для укрепления позиций представителей преступного мира, и в дискредитации правоохранительных органов. При этом можно выделить следующие характерные особенности преступлений в сфере высоких информационных технологий: неоднородность объекта посягательства; выступление компьютерной информации, как в качестве объекта, так и в качестве средства преступления; многообразие предметов и средств преступного посягательства; выступление компьютера либо в качестве предмета, либо в качестве средства совершения преступления.

С учетом особенностей совершения преступлений с использованием информационных технологий на сегодняшний день является актуальным

целый комплекс юридических и технических проблем, связанных с: неадекватным состоянием национального законодательства (в уголовном законодательстве отсутствует соответствующая общественной опасности содеянного оценка действий, по своей сути являющихся преступлениями, но не нашедших разрешения; в уголовно-процессуальном законодательстве не определены процедуры в от ношении материальных объектов, не имеющих вещественных признаков — «электронные» доказательства, «электронные обыски и выемки» и т. п.); несформированностью структур правоохранительных органов, призванных бороться с данными видами преступлений, отсутствие оперативно розыскных методик по их предупреждению и раскрытию, судебно-следственной практики, по такого рода делам, специально обученного личного состава; крайне низкой оснащённостью правоохранительных органов специальными аппаратными и программными средствами, без которых эффективная борьба с этим новым видом преступлений практически невозможна; низкой профессиональной подготовкой сотрудников спецподразделений.

В связи с чем становится актуальным определение направленности совершенствования борьбы с «компьютерной» преступностью путем создания Концепции «Стратегия и тактика борьбы с преступностью в сфере высоких информационных технологий», а также внесения дополнений в уголовно процессуальное законодательство.

Существенную помощь в исследовании какого-либо предмета оказывает проведение классификации этого предмета или явления. Аналогично понятию преступлений в сфере высоких информационных технологий в литературе нет единого мнения о том, каким образом и по каким критериям классифицировать преступления в этой сфере. Одной из первых попыток было предложенное Ю. М. Батуриным разделение преступлений по способу их совершения: методы перехвата; методы несанкционированного доступа; методы манипуляции.

Определенный интерес представляет также предложенная В. А. Мещеряковым классификация, строящаяся на идеи не столько преступлений, сколько совокупности возможных противоправных посягательств в этой сфере.

1. Неправомерное завладение информацией или нарушение исключи тельного права ее использования:

-неправомерное завладение информацией как совокупностью сведений, документов (нарушение исключительного права владения);

-неправомерное завладение информацией как товаром;

-неправомерное завладение информацией как идеей (алгоритмом, методом решения задачи).

2. Неправомерная модификация информации:

-как товара с целью воспользоваться ее полезными свойствами (снятие защиты);

-как идеи, алгоритма и выдача за свою (подправка алгоритма);

-как совокупности фактов, сведений.

3. Разрушение информации:

-разрушение информации как товара;

-уничтожение информации.

4. Действие или бездействие по созданию (генерации) информации с заданными свойствами:

-распространение по телекоммуникационным каналам информационно вычислительных сетей информации, наносящей ущерб государству, обществу и личности;

-разработка и распространение компьютерных вирусов и прочих вредоносных программ для ПК;

- преступная халатность при разработке (эксплуатации) программного
обеспечения, алгоритма в нарушение установленных технических норм и правил.

5. Действия, направленные на создание препятствий пользования информацией законным пользователям: неправомерное использование ресурсов автоматизированных систем (памяти, машинного времени и т. п.); информационное «подавление» узлов телекоммуникационных систем (создание потока ложных вызовов).

Указанная классификация имеет ощутимое преимущество перед остальными — ее основанием являются не абстрактные юридические модели, а реальные правонарушения, совершаемые в настоящее время.

Наиболее удачной на тот период времени, по нашему мнению, является классификация, предложенная Марком Экенвайлером, в которой он выделяет три основные категории (с дальнейшей дифференциацией) в зависимости от способа использования компьютера при совершении преступлений:

1. Компьютер является объектом правонарушения, когда цель преступника — похитить информацию или нанести вред интересующей его системе:

-изъятие средств компьютерной техники с находящейся в ней информацией;

-хищение информации;

-хищение услуг (получение несанкционированного доступа к какой-то системе с целью безвозмездного пользования предоставляемыми ею услугами);

-повреждение системы. Данная группа объединяет преступления, совершаемых с целью разрушить или изменить данные, являющиеся важными для владельца или одного или многих пользователей системы — объекта несанкционированного доступа.

2. Компьютеры используются как средства, способствующие совершению преступления: как средство совершения традиционных преступлений (как правило, мошенничество); как средство атаки на другой компьютер, средство совершения иного компьютерного преступления.

3. Компьютер используется как запоминающее устройство (например, после взлома системы создается специальная директория для хранения

файлов, содержащих программные средства преступника, пароли для других узлов, списки украденных номеров кредитных карточек и т. п.)

Предложенная классификация позволит систематизировать уголовно правовые аспекты определения видов преступлений в сфере высоких информационных технологий, а также определить способы совершения, конкретные приемы их применения, используемые при этом технические средства, методы подготовки и исполнения преступления и множество иных обстоятельств, имеющих следственно-оперативное значение при расследовании и раскрытии преступлений в сфере высоких информационных технологий.

Методические рекомендации:

1. Изучить основную литературу.
2. Ознакомиться с дополнительной литературой.
3. Законспектировать основные положения нормативных актов, вопросы лекционных занятий и т.д.

Список рекомендованной литературы

1, 3, 6, 13, 17, 19, 20, 21, 22, 26, 31, 32.

Тема 1. Общая характеристика досудебного расследования в сфере компьютерной информации и высоких технологий

Семинар – 1 час

Цель занятия: выработка профессиональных навыков по принятию процессуальных решений, составлению сопутствующих процессуальных документов; привитие навыков по использованию законодательных и иных нормативных актов в работе с доказательствами; привитие уважительного отношения к закону.

Вопросы занятия:

1. Преступления в сфере высоких информационных технологий .
2. Понятие и значение преступления в сфере высоких информационных технологий.
3. Направления преступной деятельности в информационной сфере и их классификация.
4. Основные обстоятельства, подлежащие установлению и доказыванию при расследовании преступлений в сфере высоких информационных технологий.
5. Общие условия производства досудебного расследования преступления в сфере высоких информационных технологий.
6. Правовое регулирование отношений в области компьютерной информации.

Задание: подготовить устный ответ.

Список рекомендованной литературы

1, 3, 6, 13, 17, 19, 20, 21, 22, 26, 34, 37.

Тема 1. Общая характеристика досудебного расследования в сфере компьютерной информации и высоких технологий

Практическое занятие – 1 час

Цель занятия: выработка профессиональных навыков по принятию процессуальных решений, составлению сопутствующих процессуальных документов; привитие навыков по использованию законодательных и иных нормативных актов в работе с доказательствами; привитие уважительного отношения к закону.

Вводная:

В УВД г. Энска поступило заявление от юриста торгового порта «Заря», о том, что после увольнения с должности ведущего инженера программиста Шамилова А.Н. была удалена с сервера вся бухгалтерская и финансовая информация, справочные и персональные сведения о судах, коммерческих партнерах и сотрудниках. Деятельность торгового порта в течение двух дней была парализована, поскольку предприятие оказалось неспособным выполнять свои обязательства по получению и отправки грузов.

В ходе оперативно-розыскных мероприятий было установлено, что гражданин Шамилов А.Н. из хулиганских побуждений уничтожил информацию, составляющую коммерческую тайну торгового порта, где он ранее работал. Используя сеть Интернет, через домашний компьютер он подключился к базе данных и удалил с сервера всю имеющуюся информацию.

Задание:

1. С учетом полученной информации необходимо дать анализ сложившейся ситуации.
2. Какое процессуальное решение необходимо принять в данной ситуации.
3. Составьте план проведения первоначальных следственных действий и оперативно-розыскных мероприятий.
4. С учетом полученной информации допросить лицо, сообщившее об уголовном правонарушении.
5. Проведите имитацию допроса подозреваемого лица Шамилова А.Н. и составьте соответствующий протокол.

Порядок контроля и оценки знаний:

1. Оценка правильности и содержательности ответов (использование УПК и норм. актов)

2. Оценка активного участия в дискуссии.

3. Качество составленных документов.

4. Качество проведения процессуальных действий.

Выступление с подготовленной презентацией в программе PoverPoint 2003-2007.

Нормативно правовые акты: 2,3,6.

Основная литература: 2,3,7.

Дополнительная литература: 24,25,26,30,31,32,33,35,36,37,38,39, 40.

Тема 1. Общая характеристика досудебного расследования в сфере компьютерной информации и высоких технологий

СРО – 12 часов

Защита рефератов по темам:

1. Деятельность правоохранительных органов, осуществляющих прием, регистрацию и разрешение сообщений о преступлениях в сфере компьютерной информации и высоких технологий.

2. Типичные следственные ситуации и планирование расследования преступлений

3. Возмещение вреда, причиненного преступлениями против собственности.

4. Новые методики исследования объектов, собранных в ходе расследования преступлений против собственности.

Самостоятельная работа обучающихся:

1. Задание: обучающиеся по данной теме по указанию преподавателя изучают вопросы ее актуальности и значимости, спорные и нерешенные проблемы, пути и выходы решения в соответствии с уголовно-процессуальным законодательством Республики Казахстан. По рекомендации преподавателя обучающиеся могут изучить архивные материалы, статистические данные, справки и отчеты, статьи и другие источники. По выборке данного материала обучающиеся составляют справки, отчеты, тезисы к докладу, реферату, статьи и т.д.

2. Форма проведения СРО: обучающиеся под руководством преподавателя обсуждают проблемы, связанные с организационно-распорядительной деятельностью начальника управления, отдела, отделения. Обсуждение докладов обучающихся, выбравших по данной теме письменную работу.

3. Методические рекомендации к выполнению: при подготовке к занятию необходимо опираться на ранее усвоенные знания и использовать нормативные, теоретико-прикладные источники, а так же учебники и учебные пособия по теме занятия.

Основная литература: 2,3,7. 22, 23, 24, 25, 26, 27.

Дополнительная литература: 24,25,26,30,31,32, 36, 37, 38, 39, 40.

Тема 2. Деятельность следователя по проверке законности и обоснованности повода к началу досудебного расследования в сфере компьютерной информации и высоких технологий

Лекция – 1 час

Цель занятия: выработка профессиональных навыков по принятию процессуальных решений, составлению сопутствующих процессуальных документов; привитие навыков по использованию законодательных и иных нормативных актов в работе с доказательствами; привитие уважительного отношения к закону.

Вопросы лекции:

1. Следственные ситуации первоначального этапа расследования преступлений в сфере высоких информационных технологий в сфере компьютерной информации и высоких технологий.
2. Поводы к началу досудебного расследования в сфере компьютерной информации и высоких технологий?

Тезисы лекции:

Одна из особенностей преступлений в сфере высоких информационных технологий, как нами уже было отмечено, заключается в том, что они чрезвычайно латентны (около 90 %). Это связано с тем, что после совершения компьютерного преступления потерпевший обычно не выказывает особой заинтересованности в поимке преступника, а сам преступник, будучи пойман, всячески рекламирует свою деятельность (но это проявляется не во всех случаях). Возможные причины подобного поведения — жертва компьютерного преступления, как правило, совершенно убеждена, что затраты на его раскрытие (включая потери, понесенные в результате утраты, например, банком своей репутации) существенно превосходят уже причиненный ущерб, а сам преступник в результате огласки приобретает широкую известность в деловых и криминальных кругах.

Между тем раскрывать преступления, совершаемые в сфере высоких информационных технологий, сложно, т. к. нередко преступники прибегают к различным уловкам, маскируют свои преступные деяния многочисленными объективными и субъективными причинами, которые действительно могут иметь место.

Как уже установлено, что определение основных направлений расследования и особенности тактики отдельных следственных действий зависят от характера исходных данных. Под исходной следственной ситуацией понимается объективно сложившаяся в первый период расследования его информационная среда, обстановка проведения и другие условия расследования, от которых зависит тактика и последовательность

проведения первоначальных следственных действий, оперативно-розыскных и организационных мероприятий. По делам рассматриваемой категории можно выделить следующие исходные следственные ситуации:

1.Информация о причинах возникновения общественно опасных деяний, способе их совершения и личности правонарушителя отсутствует.

2.Имеются сведения о причинах возникновения преступления, способе его совершения, но нет сведений о личности преступника.

3.Известны причины возникновения преступления, способы его совершения и сокрытия, личность преступника и другие обстоятельства.

В первых двух следственных ситуациях обычно планируются и осуществляются следующие первоначальные следственные действия, оперативно розыскные и организационные мероприятия: допрос заявителя или лиц, на которых указано в исходной информации как на возможных свидетелей; решение вопроса о возможности задержания преступника с поличным и о необходимых в связи с этим мероприятиях; вызов необходимых специалистов для участия в осмотре места происшествия; осмотр места происшествия; проведение оперативно-розыскных мероприятий в целях установления причин совершения преступления, выявления лиц, виновных в его совершении, обнаружения следов и других вещественных доказательств; выемка и последующий осмотр средств электронно – вычислительной техники, предметов, материалов и документов (в т.ч. находящихся в электронной форме на машинных носителях информации), характеризующих производственную операцию, в ходе которой по имеющимся данным совершены преступные действия; допросы свидетелей (очевидцев); допросы подозреваемых (свидетелей), ответственных за данный участок работы, конкретную производственную операцию и защиту конфиденциальной информации; обыски на рабочих местах и по месту проживания подозреваемых; назначение программно-технической, радиотехнической, технической, бухгалтерской и иных экспертиз; дальнейшие действия, которые планируются с учетом дополнительной информации.

Для третьей следственной ситуации может быть предложена следующая программа расследования и действий следователя на первоначальном этапе:

- изучение поступивших материалов с позиций их полноты, соблюдения норм уголовно-процессуального законодательства и порядка передачи в органы следствия. При необходимости принятие мер к получению недостающей информации;

-начало досудебного расследования;

-вызов необходимых специалистов для участия в осмотре места происшествия;

-осмотр места происшествия;

-личные обыски задержанных, их рабочих мест и места проживания;

-допрос подозреваемых;

-выемка и осмотр вещественных и письменных доказательств;

-изъятие и осмотр подлинных документов, удостоверяющих личность задержанных, а также документов, характеризующих те производственные операции, в процессе которых допущены нарушения и преступные действия (в т. ч. и тех документов, которые находятся в электронной форме на машинных носителях информации);

-допрос лиц, названных в документах, переданных в следственные органы, как допустивших нарушения, ответственных за работу (де нежные средства, материальные ценности, услуги и т. п.) по фактам установленных нарушений;

-истребование, а при необходимости производство выемки нормативных актов и документов, характеризующих порядок и организацию работы в данном подразделении (в т. ч. с конфиденциальной информацией, бланками строгой отчетности, использование СВТ ит. п.);

-допрос свидетелей, причастных к соответствующим производственным операциям или подозреваемых в связях с лицами, совершившими преступные действия;

-анализ полученной информации и решение вопроса о необходимости назначения экспертиз, проведения ревизии или проверки, в т. ч. повторной (по каким позициям, за какой период и с участием каких специалистов).

При выполнении вышеуказанных программ следует учитывать особенности методики расследования конкретного вида преступления, о совершении которого выдвинуты версии. Учитывая конкретные обстоятельства, следователем могут быть выдвинуты и проверены следующие общие версии:

1.Преступление совершено сотрудником данного учреждения либо лицом, имеющим свободный доступ к компьютерной технике.

2.Преступление совершено сторонним лицом, входящим в круг родственников, друзей, знакомых сотрудников учреждений.

3.Преступление совершено группой лиц по предварительному сговору или организованной группой с участием сотрудника данного учреждения либо лица, имеющего свободный доступ к компьютерной технике и в совершенстве владеющего навыками работы с ней.

4.Преступление совершено лицом или группой лиц, не связанных с деятельностью учреждения и не представляющих ценность компьютерной информации.

5.Преступление действительно имело место при тех обстоятельствах, которые вытекают из первичных материалов.

6.Ложное заявление о преступлении.

Приведенный перечень следственных версий является общим, и в зависимости от конкретной ситуации может быть расширен. При этом типичными частными версиями являются версии: о личности преступника (преступников); о способах совершения преступления; об обстоятельствах, при которых было совершено преступление; о размерах ущерба, причиненного преступлением.

Так, рассматривая главу 7 УК РК, можно отметить, что данная норма фактически предусматривает ответственность за совершение трех составов преступлений: неправомерный доступ к охраняемой законом компьютерной информации; создание, использование и распространение вредоносных программ для ПК; нарушение правил эксплуатации ПК, системы ПК или их сети. Рассмотрим особенности расследования данных преступлений более подробно.

Данную необходимость обуславливает дефицит криминалистических рекомендаций по методике и тактике расследования указанных составов преступлений, в связи с чем, представляется обоснованным предложить методические рекомендации и схемы расследования указанных преступлений, которые будет выглядеть следующим образом.

1. Первоначальный этап расследования неправомерного доступа к охраняемой законом компьютерной информации.

Признаками совершения указанного состава могут являться:

-появление в компьютере фальшивых или искаженных данных;

-не обновление в течение длительного времени в автоматизированной информационной системе кодов, паролей и других защитных средств;

-частые сбои в процессе работы компьютеров;

-участившиеся жалобы клиентов компьютерной системы или сети;

-осуществление сверхурочных работ без видимых на то причин;

-немотивированные отказы некоторых сотрудников, обслуживающих компьютерные системы или сети, от отпусков;

-неожиданное приобретение сотрудником домашнего дорогостоящего компьютера;

-чистые дискеты либо диски, принесенные на работу сотрудниками компьютерной системы под сомнительными предлогами;

-участившиеся случаи перезаписи отдельных данных без серьезных на то причин;

-чрезмерный интерес отдельных сотрудников к содержанию чужих распечаток (листингов), выходящих из принтеров.

При наличии указанных признаков либо иного сигнала о совершенном преступлении следует установить:

1.Факт неправомерного доступа к компьютерной информации.

2.Место несанкционированного проникновения в компьютерную систему или сеть.

3.Время несанкционированного доступа.

4.Надежность средств защиты компьютерной информации.

5.Способ совершения несанкционированного доступа.

6. Круг лиц, совершивших неправомерный доступ

7. Виновность и мотивы лиц, совершивших неправомерный доступ к компьютерной информации.

8.Наличие последствий преступления.

9.Наличие обстоятельств, способствовавших преступлению.

2. Первоначальный этап расследования создания, использования распространения вредоносных программ для ПК.

Признаков совершения данных преступлений нет. Как правило, обнаружить можно лишь их результаты — сбои в процессе работы компьютерной системы или сети, жалобы клиентов и т. п.

При расследовании создания вредоносных программ для ПК подлежат установлению следующие обстоятельства:

-факт создания вредоносной программы для ПК;

-способ создания вредоносной программы;

-факт использования и распространения вирусной программы;

-предназначение вредоносной программы и механизм действия;

-место, время создания, используемое для этого программное обеспечение и компьютерная техника;

-круг лиц, виновных в создании, использовании и распространении вирусных программ для ПК;

-цель и мотив создания программы;

-осведомленность лица, использовавшего программу, о ее вредоносных свойствах, наличие или отсутствие умысла на использование и распространение данной программы;

-характер и размер вреда, причиненного данным преступлением;

-наличие обстоятельств, способствовавших совершению расследуемого преступления.

Вредоносная программа, как правило, обнаруживается в момент, когда уже явно проявляются последствия ее применения. Вместе с тем она может быть обнаружена и на машинных носителях информации, в частности, путем изучения информации обложки компакт-диска. Кроме того, выявляется она также в процессе антивирусной проверки, производимой пользователем компьютерной системы перед началом работы на компьютере, особенно часто практикуемой при использовании чужих машинных носителей или получении электронной почты.

Наибольшую сложность для расследования представляет совершение преступления в условиях неочевидности. Здесь основными направлениями расследования должны быть:

- пресечение противоправной деятельности;

- выяснение механизма преступления и уточнение отдельных его обстоятельств;

- установление лица, распространяющего вредоносную программу;

- получение сведений о личности потерпевших;

- установление суммы материального ущерба;

-сбор доказательств о причастности установленного лица к каждым выявленным эпизодам преступной деятельности;

-выяснение причин и условий, способствовавших совершению преступления;

- получение характеризующего личность подозреваемого материала.

Наиболее распространенными условиями, способствовавшими совершению данного преступления, являются: использование не сертифицированного программного обеспечения; использование нелегальных копий программ для ПК; отсутствие резервных копий программ и системных файлов; отсутствие учета и контроля за доступом к компьютерным системам- использование компьютеров не по назначению (для компьютерных игр обучения посторонних, написания программ лицами, в обязанности которых это не входит); нерегулярное проведение антивирусной проверки компьютерной системы и машинных носителей, и др.

3. Первоначальный этап расследования нарушения правил эксплуатации ПК, системы ПК или их сети.

При расследовании нарушения правил эксплуатации ПК, системы ПК или их сети подлежат установлению следующие обстоятельства:

1) факт преступного нарушения правил эксплуатации ПК, системы ПК или их сети;

2) место и время совершения преступления;

3) характер информации, являющейся предметом посягательства;

4) способ и механизм нарушения правил эксплуатации ПК, системы ПК или их сети;

5) характер и размер ущерба, причиненного преступлением;

6) виновность лица;

7) обстоятельства, способствовавшие совершению преступления.

Наиболее распространенными поводами к началу досудебного расследования по указанным составам преступлений являются: сообщения должностных лиц организаций или их объединений (40%); заявления граждан (35%); непосредственное обнаружение органом дознания, следователем или прокурором сведений, указывающих на признаки преступления (20%); сообщения в средствах массовой информации и иные поводы (5 %).

По оценкам ведущих зарубежных и отечественных специалистов 90 % компьютерных преступлений остаются необнаруженными или о них не сообщается в правоохранительные органы по различным причинам.

Список рекомендованной литературы

1, 3, 5, 6, 7, 8, 13, 20, 21, 22,26, 32, 33.

Тема 2. Деятельность следователя по проверке законности и обоснованности повода к началу досудебного расследования в сфере компьютерной информации и высоких технологий

Лекция – 1 час

Цель занятия: выработка профессиональных навыков по принятию процессуальных решений, составлению сопутствующих процессуальных

документов; привитие навыков по использованию законодательных и иных нормативных актов в работе с доказательствами; привитие уважительного отношения к закону.

Вопросы лекции:

1. Особенности проведения отдельных следственных действий на первоначальном этапе расследования преступлений в сфере высоких информационных технологий

Тезисы лекции:

Общее изучение сущности рассматриваемого вопроса предполагает анализ следующих следственных действий, чье проведение характерно для первоначального этапа расследования по делам о преступлениях, совершенных в сфере высоких информационных технологий:

По мнению Э. Мелик, целями следственных действий при расследовании данного вида преступлений могут являться:

- осмотр и изъятие компьютерной техники;
- поиск и изъятие информации и следов воздействия на нее непосредственно на носителях информации ПК и ее устройствах;
- поиск и изъятие информации и следов воздействия на нее вне ПК.

Полагаем, что указанные цели усекают перечень следственных действий, производство которых возможно при расследовании преступлений в сфере высоких информационных технологий, проводимых с целью установления обстоятельств, имеющих значение для дела. На этот счет думается, что необходимо расширить перечень указанных целей и дополнить их, где: целями следственных действий, проводимых при расследовании и раскрытии преступлений в сфере высоких информационных технологий, являются: установление и уточнение обстоятельств, происшедшего события (способ, место, время, личность совершившего преступное посягательство и пр.); выявление, фиксация, изъятие и оценка следов преступления (как традиционных криминалистических, так и нетрадиционных - информационных следов преступлений в сфере высоких технологий), различных вещественных доказательств; получение информации, необходимой для построения и проверки следственных версий и осуществления розыскной работы по делу; поиск и изъятие информации и следов воздействия на нее непосредственно на носителях информации ПК и ее устройствах; поиск и изъятие информации и следов воздействия на нес вне ПК; обнаружение предметов и объектов преступлений; осмотр и изъятие компьютерной техники; установление лиц, способствующих совершению преступления; определение принадлежности компьютерной информации; проверка и оценка следственных версий; установление причин и условий, способствовавших совершению преступления; получение новых доказательств.

Таким образом, приступая к непосредственному исследованию особенностей проведения отдельных следственных действий при

расследовании преступлении в сфере высоких информационных технологий (исходя из указанных целей), мы выделяем следующие виды следственных действий, чье рассмотрение будет осуществлено далее: осмотр (включая несколько его разновидностей), обыск и выемка, допрос, следственный эксперимент, предъявление для опознания, назначение экспертиз.

По своей сути, все перечисленные действия могут быть проведены как на первоначальном этапе расследования преступлений в сфере высоких информационных технологий, так и на последующем. Данный факт определяется конкретными условиями расследования преступления. Вместе с тем, исследование сущности установления события преступления и лица его совершившего свидетельствует о том, что успешность проведения перечисленных действий и определяет достижение задач, направленных на быстрое и полное раскрытие преступления, изобличение и привлечение к уголовной ответственности лиц, его совершивших.

Рассматривая следственные действия, производство которых осуществляется при расследовании преступлений указанной категории, еще раз отметим, что проводятся они в строгом соответствии с правилами, регламентированными действующим уголовно-процессуальным законодательством, но с учетом некоторых особенностей.

Следственный осмотр — это следственное действие, состоящее в непосредственном восприятии, анализе и фиксации следователем или лицом, проводящим дознание, различных материальных предметов и отдельных их элементов в целях обнаружения следов преступления и других вещественных доказательств, выяснения обстановки происшествия, а также иных обстоятельств, имеющих значение для дела. Цель осмотра места происшествия по делам указанной категории - установление конкретного СВТ, выступающего в качестве предмета и (или) орудия совершения преступления и имеющего следы преступной деятельности. При производстве следственного действия целесообразно использовать тактический прием «от центра - к периферии», где «центром» (отправной точкой осмотра места происшествия) являются СВТ, находящиеся на месте осмотра. Исследование специфики следственного осмотра производится, исходя из этапов его производства: подготовительного, рабочего, заключительного.

1. Подготовительный этап. В процессе подготовки к проведению этого следственного действия, еще до выезда на место происшествия необходимо решить ряд организационных вопросов, которые в последующем обеспечат качество проведения осмотра места происшествия.

Рассматриваемое следственное действие должно быть заблаговременно подготовлено и детально спланировано, необходимо предварительно провести следующую работу: с учетом сложившейся следственной ситуации, наметить круг лиц, участвующих в осмотре; определить последовательность действия лиц при осмотре места происшествия; пригласить соответствующих квалифицированных специалистов; подготовить соответствующую компьютерную технику и программное обеспечение, которые будут

использоваться для считывания и хранения изъятой информации, при обнаружении изменений в компьютерной информации, исследовании полученной информации, обнаружении информационных следов преступления; перед началом осмотра разъяснить цели проведения следственного действия и задачи, стоящие перед специалистами, а также их права и обязанности; провести подбор и инструктаж понятых, в качестве которых целесообразнее привлекать лиц, обладающих минимально необходимыми знаниями в области СВТ и компьютерных технологий, разъяснить их права и обязанности.

2. Рабочий этап. Прежде чем приступить к осмотру, следователь и участники следственно-оперативной группы должны знать и соблюдать общие правила обращения с вычислительной техникой и носителями информации. Несоблюдение этих правил может привести к потере важной для расследования информации и нанесению материального ущерба, вызванного этими действиями.

Общими правилами обращения с вычислительной техникой и носителями информации являются: все включения (выключения) компьютеров и других технических средств производятся только специалистом или под его руководством; применение средств криминалистической техники - магнитных искателей, ультрафиолетового осветителя, инфракрасного преобразователя, во избежание разрушения носителей информации и микросхем памяти ПК, должно быть согласовано со специалистом; необходимо исключить попадания мелких частиц и порошков на рабочие части компьютеров (разъемы, дисковод, вентилятор и др.); при работе с магнитными носителями информации запрещается прикасаться руками к рабочей поверхности дисков, подвергать их электромагнитному воздействию, сгибать диски, хранить без специальных конвертов (пакетов, коробок); диапазон допустимых температур при хранении и транспортировке должен варьироваться в температурных пределах от 0 до + 50 граду сов Цельсия; со всеми непонятными вопросами, затрагивающими терминологию, устройство и функционирование вычислительной техники необходимо обращаться только к специалисту.

На рабочей (исследовательской) стадии осмотра места происшествия каждый объект подлежит тщательному обследованию. В этот период времени важно установить - не содержится ли на компьютере информация, которая может способствовать более плодотворному и целенаправленному осмотру (различные планы помещений, участков местности, пароли, коды доступа, шифры и т. п.). Для этого специалистом проводится экспресс-анализ компьютерной информации путем просмотра содержимого дисков. Интерес могут представлять файлы с текстовой или графической информацией. Следует обращать внимание не только на наличие (отсутствие) физических повреждений компьютерной техники, магнитных носителей и т. п., но и на состояние окон, дверей и запорных устройств на них.

3. Заключительный этап. Изъятие средств компьютерной техники производится только в выключенном состоянии. При этом должны быть

выполнены и отражены в протоколе следующие действия: установлено включенное состояние оборудования и зафиксирован порядок его отключения; описано точное местонахождение изымаемых предметов и их расположение относительно друг друга и окружающих предметов (с приложением необходимых схем и планов); описан порядок соединения между собой всех устройств с указанием особенностей соединения (цвет, количество, размеры, характерные индивидуальные признаки соединительных проводов, кабелей, шлейфов, разъемов, штекеров и их спецификация); - определено отсутствие либо наличие компьютерной сети, используемый канал (каналы) связи и телекоммуникаций. В последнем случае установлен тип связи, используемая аппаратура, абонентский номер, позывной либо рабочая частота; произведено разъединение (с соблюдением всех необходимых мер предосторожности) аппаратных частей (устройств) с одновременным опломбированием их технических входов и выходов; определен вид упаковки и транспортировки изъятых предметов.

Транспортировка и хранение компьютерной техники и информации должны осуществляться в условиях, исключающих ее повреждение, в том числе в результате воздействия метало детекторов, используемых для проверки багажа в аэропортах. Хранят компьютеры и их комплектующие в сухом, отапливаемом помещении. Следует удостовериться, что в нем нет грызунов, которые часто являются причиной неисправности аппаратуры. Учитывая нестандартность обстановки, в которой может производиться осмотр места происшествия, вопрос о возможности изъятия компьютерной техники и информации, способе упаковки, транспортировки и хранении изъятых объектов решается следователем в каждом конкретно случае совместно со специалистом. Процессуальный порядок изъятия объектов определяется общими требованиями Уголовно-процессуального кодекса.

Осмотр средств вычислительной техники (СВТ), участвовавших в преступлении, производят для достижения следующих целей: обнаружения следов, образовавшихся в результате происшествия или совершения преступления, и других вещественных доказательств для установления, кем, с какой целью и при каких обстоятельствах было совершено преступление; выяснения обстановки происшествия для восстановления механизма совершения преступления; установления технического состояния СВТ.

Обыск, выемка. Обыск - следственное действие, в процессе которого производится поиск и принудительное изъятие объектов, имеющих значение для правильного решения задач уголовного судопроизводства. Выемка — следственное действие, в процессе которого производится изъятие объектов, имеющих значение для правильного решения задач уголовного судопроизводства, в тех случаях, когда их местонахождение точно известно следователю.

Задачами обыска при расследовании преступлений в сфере высоких информационных технологий являются отыскание и изъятие:

1) орудий, используемых для совершения преступления в сфере компьютерной информации, в том числе носителей информации,

примененных для копирования похищенной информации или содержащие программы «взлома» защиты компьютера, вредоносные программы, иные программы и файлы данных (например, библиотеки паролей и имен), использованные при совершении преступления;

2) компьютерной информации;

3) специальной литературы, посвященной вопросам компьютерной безопасности, эксплуатации ПК, создания вредоносных программ, неправомерного доступа к компьютерной информации, принципов и алгоритмов организации компьютерных сетей, программного обеспечения и пр.;

4) иных вещественных доказательств и документов, имеющих значение для дела;

5) разыскиваемого лица.

При производстве выемки следует придерживаться рассмотренных нами рекомендаций по осмотру, обыску с учетом процессуальной процедуры производства данного следственного действия.

Допрос. Допрос подозреваемого. При допросе лица в качестве подозреваемого в каждом конкретном случае, как минимум, необходимо получить ответы на следующие вопросы: «Где и кем (в какой должности) работал подозреваемый; к какой компьютерной информации имеет доступ; какие операции с информацией он имеет право проводить; какова его категория доступа к информации; умеет ли работать подозреваемый на компьютере, владеет ли он определенным программным обеспечением, каков уровень его квалификации; кто научил его работать с конкретным программным обеспечением; какие идентификационные коды и пароли закреплены за ним (в том числе при работе в компьютерной сети); к каким видам программного обеспечения имеет доступ подозреваемый; каков источник его происхождения; обнаруживались ли программы, источник происхождения которых неизвестен; какие виды операций с компьютерной информацией данное лицо выполняло в исследуемое время; из какого источника или от кого конкретно подозреваемый узнал о содержании информации, к которой произвел неправомерный доступ; какой способ использовал подозреваемый для совершения неправомерного доступа к компьютерной информации; как подозреваемому удалось проникнуть в компьютерную систему (сеть); откуда подозреваемый мог узнать пароль (код) доступа к информации».

При установлении факта сбоев в работе средств компьютерной техники и устройств защиты информации в период работы данного лица в определенное время возможна постановка следующих вопросов: «Обнаруживал ли он сбои в работе программ, компьютерные вирусы и другие нарушения в нормальном функционировании программного обеспечения; обнаруживал ли подозреваемый случаи незаконного проникновения в свой компьютер, незаконного подключения к компьютерной сети; имеет ли он ограничения на допуск в помещения, где установлена компьютерная техника и какие именно; ознакомлен ли он с

порядком работы с информацией, инструкциями о порядке проведения работ; не было ли случаев нарушения подозреваемым распорядка дня, порядка проведения работ, порядка доступа к компьютерной информации; не поступало ли к подозреваемому от других лиц предложений о передаче какой-либо компьютерной информации, программного обеспечения; неизвестны ли ему лица, проявлявшие интерес к получению идентификационных кодов и паролей».

Круг вопросов, подлежащих выяснению у подозреваемого, определяется конкретной следственной ситуацией, сложившейся по уголовному делу:

- при допросе подозреваемого в совершении создания вредоносных программ для ПК требуется установить уровень его профессиональной подготовленности как программиста, опыт работы по созданию программ конкретного класса на данном языке программирования, знание алгоритмов работы программ, подвергшихся воздействию;

- при расследовании преступлений, связанных с распространением вредоносных программ, особенно компьютерных вирусов, требуется выяснить: соблюдались ли требования противовирусной защиты, каков уровень владения соответствующими программами, каким образом был нарушен режим использования программных средств.

Кроме этого, необходимо установить конкретные факты несоблюдения режима доступа на объект, доступа к средствам вычислительной техники и программным средствам, способы преодоления программных и аппаратных средств защиты информации и другие обстоятельства, способные облегчить совершение преступления.

При допросе подозреваемого требуется выяснить все обстоятельства подготовки и совершения преступления, алгоритм функционирования вредоносной программы, а также на какую информацию и как она воздействует, характер наступающих последствий, связанных с нарушением работы ПК, их системы или сети и несанкционированным уничтожением, блокированием, модификацией или копированием информации и какие действия по их преодолению могут быть наиболее эффективны.

В ходе допросов свидетелей выясняются следующие обстоятельства: на какой рабочей станции могли быть нарушены правила эксплуатации компьютерной сети и где она расположена; могли ли быть нарушены правила эксплуатации данной локальной сети на рабочей станции, расположенной в определенном месте (если нарушение правил произошло непосредственно на файловом сервере, то место нарушения этих правил может совпадать с местом наступления вредных последствий).

Основная литература: 2,3,7. 22, 23, 24, 25, 26, 27.
Дополнительная литература: 24,25,26,30,31,32.

Тема 2. Деятельность следователя по проверке законности и обоснованности повода к началу досудебного расследования в сфере компьютерной информации и высоких технологий

Семинар – 1 час

Цель занятия: выработка профессиональных навыков по принятию процессуальных решений, составлению сопутствующих процессуальных документов; привитие навыков по использованию законодательных и иных нормативных актов в работе с доказательствами; привитие уважительного отношения к закону.

Вопросы занятия:

1. Следственные ситуации первоначального этапа расследования преступлений в сфере высоких информационных технологий в сфере компьютерной информации и высоких технологий.
2. Поводы к началу досудебного расследования в сфере компьютерной информации и высоких технологий?
3. Особенности проведения отдельных следственных действий на первоначальном этапе расследования преступлений в сфере высоких информационных технологий

Задание: подготовить устный ответ.

Список рекомендованной литературы

1, 3, 6, 13, 17, 19, 20, 21, 22, 26, 34, 37.

Тема 2. Деятельность следователя по проверке законности и обоснованности повода к началу досудебного расследования в сфере компьютерной информации и высоких технологий

Практическое занятие – 1 час

Цель занятия: выработка профессиональных навыков по принятию процессуальных решений, составлению сопутствующих процессуальных документов; привитие навыков по использованию законодательных и иных нормативных актов в работе с доказательствами; привитие уважительного отношения к закону.

Вводная:

Согласно приказу №23 компании «Вымпел-Ком» г.Энск «О приеме работника на работу», Денисов А.Г. был принят на должность специалиста офиса обслуживания и продаж, и приступил к работе с 1 августа 2018г. Для работы в компьютерной программе, обеспечивающей удаленный доступ через программу «1С» к базе данных «Amdocs»,предназначенной для

обслуживания абонентов данной компании Денисов А.Г. получил индивидуальный и конфиденциальный логин и пароль, составляющие его служебную учетную запись. В соответствии с должностной инструкцией Денисов А.Г. обязан был осуществлять обработку персональных данных физических лиц – абонентов компании «Вымпел-Ком», в том числе сбор, хранение, ввод, использование, изменение и уничтожение обрабатываемых персональных данных; обеспечивать конфиденциальность обрабатываемых персональных данных. Денисов А.Г. испытывая материальные трудности, действуя из корыстной заинтересованности с целью получения выгоды заинтересованности с целью получения выгоды имущественного характера для себя решил совершить неправомерный доступ к охраняемой компьютерной информации, содержащей персональные данные клиентов компании «ВымпелКом».

Денисов А.Г. был осведомлен о том, что сим-карта, применяемая в средствах мобильной связи в качестве идентификационного модуля абонента, содержит сведения о подключенных к абонентскому номеру услугах и установленных приложениях, в том числе предназначенных для осуществления операций приема, выдачи и перевода денежных средств, в который данный абонентский номер выступает в качестве идентификатора соответствующей учетной записи.

Задание:

1. С учетом полученной информации необходимо дать анализ сложившейся ситуации.
2. Какое процессуальное решение необходимо принять в данной ситуации.
3. Составьте план проведения первоначальных следственных действий и оперативно-розыскных мероприятий.
4. С учетом полученной информации допросить лицо, сообщившее об уголовном правонарушении.
5. С учетом полученной информации составьте план проверочных мероприятий, с целью чего заполните таблицу:

Установленные обстоятельства	Обстоятельства, требующие уточнения и дополнения	Необходимые действия

6. Определите структуру протокола осмотра места происшествия и процессуальный порядок его проведения, составьте протокол осмотра с учетом полученной вводной задания.
7. Составьте протокол осмотра вещественных доказательств (компьютер).

Порядок контроля и оценки знаний:

1. Оценка правильности и содержательности ответов (использование УПК и норм. актов)

2. Оценка активного участия в дискуссии.

3. Качество составленных документов.

4. Качество проведения процессуальных действий.

Выступление с подготовленной презентацией в программе PoverPoint 2003-2007.

Основная литература: 2,3,7.

Дополнительная литература: 24,25,26,30,31,32,33,35,36,37,38,39, 40.

Список рекомендованной литературы

1, 3, 6, 13, 17, 19, 20, 21, 22, 26, 31, 32.

Тема 2. Деятельность следователя по проверке законности и обоснованности повода к началу досудебного расследования в сфере компьютерной информации и высоких технологий

СРО – 12 часов

Методические рекомендации:

1. Изучить основную литературу.
2. Ознакомиться с дополнительной литературой.
3. Законспектировать основные положения нормативных актов, вопросы лекционных занятий и т.д.

Выполнить письменно ситуационные задачи и быть готовым доложить решения по ним.

Материал для самоконтроля

Тестовые задания для самоконтроля (раздаточный материал)

Самостоятельная работа обучающихся

1.Задания: обучающиеся по данной теме по указанию преподавателя изучают вопросы ее актуальности и значимости, спорные и нерешенные проблемы, пути и выходы решения в соответствии с уголовно-процессуальным законодательством Республики Казахстан. По рекомендации преподавателя обучающийся может изучить архивные материалы, статистические данные, справки и отчеты, статьи и другие источники. По выборке данного материала обучающийся составляет справки, отчеты, тезисы к докладу, реферату, статьи и т.д.

2.Форма проведения СРО: обучающиеся под руководством преподавателя обсуждают проблемы, связанные с организационно-распорядительной деятельностью начальника управления, отдела, отделения. Обсуждение докладов обучающихся, выбравших по данной теме письменную работу.

3.Методические рекомендации к выполнению: При подготовке к занятию необходимо опираться на ранее усвоенные знания и использовать нормативные, теоретико-прикладные источники, а так же учебники и учебные пособия по теме занятия.

4. Рекомендуемая литература: теоретические (монографии, учебные пособия, практикумы) и нормативные источники, рекомендованные для подготовки к лекционным и семинарским занятиям.

Список рекомендованной литературы

1, 3, 5, 6, 7, 8, 13, 20, 21, 22,26, 32, 33.

Тема 3. Процессуальный порядок определения статуса подозреваемого, организация и проведение допроса подозреваемого

Лекция – 1 час

Цель занятия: выработка профессиональных навыков по принятию процессуальных решений, составлению сопутствующих процессуальных документов; привитие навыков по использованию законодательных и иных нормативных актов в работе с доказательствами; привитие уважительного отношения к закону.

Вопросы лекции:

1. Особенности проведения допроса подозреваемого на первоначальном этапе расследования преступлений в сфере высоких информационных технологий

Тезисы лекции:

Допрос подозреваемого. При допросе лица в качестве подозреваемого в каждом конкретном случае, как минимум, необходимо получить ответы на следующие вопросы: «Где и кем (в какой должности) работал подозреваемый; к какой компьютерной информации имеет доступ; какие операции с информацией он имеет право проводить; какова его категория доступа к информации; умеет ли работать подозреваемый на компьютере, владеет ли он определенным программным обеспечением, каков уровень его квалификации; кто научил его работать с конкретным программным обеспечением; какие идентификационные коды и пароли закреплены за ним (в том числе при работе в компьютерной сети); к каким видам программного обеспечения имеет доступ подозреваемый; каков источник его происхождения; обнаруживались ли программы, источник происхождения которых неизвестен; какие виды операций с компьютерной информацией данное лицо выполняло в исследуемое время; из какого источника или от кого конкретно подозреваемый узнал о содержании информации, к которой произвел неправомерный доступ; какой способ использовал подозреваемый для совершения неправомерного доступа к компьютерной информации; как подозреваемому удалось проникнуть в компьютерную систему (сеть); откуда подозреваемый мог узнать пароль (код) доступа к информации».

При установлении факта сбоев в работе средств компьютерной техники и устройств защиты информации в период работы данного лица в определенное время возможна постановка следующих вопросов:

«Обнаруживал ли он сбои в работе программ, компьютерные вирусы и другие нарушения в нормальном функционировании программного обеспечения; обнаруживал ли подозреваемый случаи незаконного проникновения в свой компьютер, незаконного подключения к компьютерной сети; имеет ли он ограничения на допуск в помещения, где установлена компьютерная техника и какие именно; ознакомлен ли он с порядком работы с информацией, инструкциями о порядке проведения работ; не было ли случаев нарушения подозреваемым распорядка дня, порядка проведения работ, порядка доступа к компьютерной информации; не поступало ли к подозреваемому от других лиц предложений о передаче какой-либо компьютерной информации, программного обеспечения; неизвестны ли ему лица, проявлявшие интерес к получению идентификационных кодов и паролей».

Следует иметь в виду, что на первом допросе подозреваемый может попытаться объяснить факт неправомерного доступа к компьютерной информации некриминальными причинами (случайностью, стечением определенных обстоятельств, посторонним воздействием и т. п.). Может рассказывать о неправомерном доступе к компьютерной информации, как о факте, который совершился при отсутствии преступного умысла.

Для изобличения таких лиц хорошие результаты дает правильная реализация информации о преступной деятельности этого лица, полученной при проведении оперативно-розыскных мероприятий, а так же предъявление предметов и документов, принадлежащих подозреваемому и использовавшихся для неправомерного доступа к компьютерной информации. Умелое использование указанных сведений оказывает определенное воздействие на допрашиваемого и позволяет получить правдивые показания на первом допросе.

Для успешного проведения допроса подозреваемого необходимо тщательно изучить все материалы дела, особенности личности подозреваемого, способы совершения преступления, доказательства, указывающие на виновность конкретного лица, и т. п. Ко времени привлечения лица в качестве подозреваемого следствие должно располагать двумя категориями доказательств. В первой из них предусматривается доказывание обстоятельств, свидетельствующих о том, что расследуемое событие (деяние) имело место, во второй — что это деяние совершено привлекаемым к уголовной ответственности лицом, и оно соответствует составу преступления, предусмотренного соответствующей статьей УК.

Как отмечает ряд авторов, допрос подозреваемого является одним из-важнейших, наиболее сложных и зачастую конфликтных следственных действий. Не преследуя цели рассмотрения тактики допроса подозреваемого в целом, отметим, что обвиняемые дают правдивые показания в тех случаях, когда убедятся, что расследованием установлен круг фактических данных. Поэтому обычно наиболее результативны приемы представления допрашиваемым собранных по делу доказательств и подробного изложения обстоятельств преступления без ссылки на источники.

Круг вопросов, подлежащих выяснению у подозреваемого, определяется конкретной следственной ситуацией, сложившейся по уголовному делу:

- при допросе подозреваемого в совершении создания вредоносных программ для ПК требуется установить уровень его профессиональной подготовленности как программиста, опыт работы по созданию программ конкретного класса на данном языке программирования, знание алгоритмов работы программ, подвергшихся воздействию;

- при расследовании преступлений, связанных с распространением вредоносных программ, особенно компьютерных вирусов, требуется выяснить: соблюдались ли требования противовирусной защиты, каков уровень владения соответствующими программами, каким образом был нарушен режим использования программных средств.

Кроме этого, необходимо установить конкретные факты несоблюдения режима доступа на объект, доступа к средствам вычислительной техники и программным средствам, способы преодоления программных и аппаратных средств защиты информации и другие обстоятельства, способные облегчить совершение преступления.

При допросе подозреваемого требуется выяснить все обстоятельства подготовки и совершения преступления, алгоритм функционирования вредоносной программы, а также на какую информацию и как она воздействует, характер наступающих последствий, связанных с нарушением работы ПК, их системы или сети и несанкционированным уничтожением, блокированием, модификацией или копированием информации и какие действия по их преодолению могут быть наиболее эффективны.

В ходе допросов свидетелей выясняются следующие обстоятельства:

- на какой рабочей станции могли быть нарушены правила эксплуатации компьютерной сети и где она расположена;

- могли ли быть нарушены правила эксплуатации данной локальной сети на рабочей станции, расположенной в определенном месте (если нарушение правил произошло непосредственно на файловом сервере, то место нарушения этих правил может совпадать с местом наступления вредных последствий).

Время нарушения правил можно установить путем допроса свидетелей из числа лиц, участвующих в эксплуатации ПК. При этом могут быть заданы такие вопросы: «Каким образом в данной компьютерной системе фиксируются факты и время отклонения от установленных правил (порядка) эксплуатации ПК?». «Когда могло быть нарушено определенное правило эксплуатации ПК, после которого наступили известные вредные последствия?».

Список рекомендованной литературы

1, 3, 5, 6, 7, 8, 9, 16, 18, 20, 21, 22, 23, 24, 27, 32.

Тема 3. Процессуальный порядок определения статуса подозреваемого, организация и проведение допроса подозреваемого

Семинар – 1 час

Цель занятия: выработка профессиональных навыков по принятию процессуальных решений, составлению сопутствующих процессуальных документов; привитие навыков по использованию законодательных и иных нормативных актов в работе с доказательствами; привитие уважительного отношения к закону.

Вопросы занятия:

1. Понятие, значение допроса подозреваемого по уголовным делам в сфере компьютерной информации и высоких технологий.
2. Формы взаимодействия с допрашиваемым лицом, по ранее составленному плану допроса.
3. Процессуальные правила проведения допроса потерпевшего.
4. Каков порядок удостоверения личности допрашиваемого и порядок разъяснения процессуальных прав и обязанностей.
5. Какова структура и содержание протокола допроса подозреваемого.
6. Каков алгоритм проведения следственного действия допрос: этапы и характеристика?
7. На основании каких данных формируются задачи следственного действия допрос и вопросы, подлежащие выяснению?
8. Каким образом устанавливается психологический контакт с допрашиваемым лицом, и формулируются вопросы?

Задание: подготовить устный ответ.

Список рекомендованной литературы

1, 3, 6, 13, 17, 19, 20, 21, 22, 26, 34, 37.

Тема 3. Процессуальный порядок определения статуса потерпевшего, организация и проведение допроса потерпевшего

СРОП – 1 час

Вопросы для самоконтроля:

1. Преступления в сфере высоких информационных технологий .
2. Понятие и значение преступления в сфере высоких информационных технологий.
3. Направления преступной деятельности в информационной сфере и их классификация.

4. Основные обстоятельства, подлежащие установлению и доказыванию при расследовании преступлений в сфере высоких информационных технологий.

5. Общие условия производства досудебного расследования преступления в сфере высоких информационных технологий.

6. Правовое регулирование отношений в области компьютерной информации.

Методические рекомендации:

1. Изучить основную литературу.
2. Ознакомиться с дополнительной литературой.
3. Законспектировать основные положения нормативных актов, вопросы лекционных занятий и т.д.

Список рекомендованной литературы

1, 3, 6, 13, 17, 19, 20, 21, 22, 26, 31, 32.

Защита рефератов по темам:

1. Понятие и значение преступления в сфере высоких информационных технологий.

2. Направления преступной деятельности в информационной сфере и их классификация.

Форма проведения СРОП: письменная работа в тетради, устный ответ.

Тема 3. Процессуальный порядок определения статуса подозреваемого, организация и проведение допроса подозреваемого.

СРО – 11 часов

Самостоятельная работа обучающихся

1.Задания: обучающиеся по данной теме по указанию преподавателя изучают вопросы ее актуальности и значимости, спорные и нерешенные проблемы, пути и выходы решения в соответствии с уголовно-процессуальным законодательством Республики Казахстан. По рекомендации преподавателя обучающийся может изучить архивные материалы, статистические данные, справки и отчеты, статьи и другие источники. По выборке данного материала обучающийся составляет справки, отчеты, тезисы к докладу, реферату, статьи и т.д.

2.Форма проведения СРО: обучающиеся под руководством преподавателя обсуждают проблемы, связанные с организационно-распорядительной деятельностью начальника управления, отдела, отделения. Обсуждение докладов обучающихся, выбравших по данной теме письменную работу.

3.Методические рекомендации к выполнению: При подготовке к занятию необходимо опираться на ранее усвоенные знания и использовать

нормативные, теоретико-прикладные источники, а так же учебники и учебные пособия по теме занятия.

4. Рекомендуемая литература: теоретические (монографии, учебные пособия, практикумы) и нормативные источники, рекомендованные для подготовки к лекционным и семинарским занятиям.

Основная литература: 2,3,7. 22, 23, 24, 25, 26, 27.

Дополнительная литература: 24,25,26,30,31,32.

2.10 Методические рекомендации по изучению дисциплины «Расследование уголовных правонарушений связанных в сфере компьютерной информации и высоких технологий»

При изучении дисциплины «Расследование уголовных правонарушений связанных в сфере компьютерной информации и высоких технологий» обучение проходит по наиболее важным темам как: общая характеристика досудебного расследования в сфере компьютерной информации и высоких технологий, деятельность следователя по проверке законности и обоснованности повода к началу досудебного расследования в сфере компьютерной информации и высоких технологий, процессуальный порядок определения статуса потерпевшего, организация и проведение допроса потерпевшего и т.д.

Информацию теоретического характера по рассматриваемым темам можно получить на кафедре, воспользовавшись фондом электронных вариантов учебников, монографий, учебно-практических пособий, сборником нормативных актов МВД и Генеральной Прокуратуры Республики Казахстан, Нормативных постановлений Верховного суда Республики Казахстан.

Системное изучение уголовно-процессуального законодательства, а также теоретических основ по дисциплине в рамках подготовки к практическим занятиям способствует закреплению материала, полученного на лекционных занятиях.

Перечень и содержание видов самостоятельной работы по дисциплине:

1. Беглое прочтение (Skit) - прочитать заданный материал согласно программе обучения.

2. Подготовка обзора по теме (Review) - письменно написать краткий литературный обзор на 1-2 стр. по рекомендуемой теме с привлечением дополнительного материала из печати и информационных ресурсов Интернета.

3. Учебные конкретные ситуации - обучающимся предлагается множество простых и сложных ситуаций, по которым предстоит ответить на вопросы или написать свое видение проблемы; наиболее подготовленные обучающиеся могут написать свой кейс.

5. Групповой проект - в группе должно быть не более 4-5 человека, каждая группа должна разработать свой проект; например доклад на международную конференцию.

6. Индивидуальный проект - выполняют наиболее подготовленные обучающиеся по желанию; работа должна отличаться уникальностью, актуальностью темы, исследовательским характером; результаты проекта могут быть доложены на круглом столе, международной конференции.

7. Эссе - этюд, публицистики и др. жанры, дающие предварительное представление или общее представление о чем-либо. Подготовка эссе прививает следующие навыки обучающимся: критически оценивать, использовать в своей работе труды других авторов, вносить исправления в свою работу, готовить проект научной работы. Основной целью эссе является не донести слушателем авторской мысли, а показать его идею, свою собственную позицию.

Формы и содержание самостоятельной работы:

1. Помощь в выполнении домашних заданий:

- проверка и помощь в написании реферата, доклада, выбранного по списку или выданного преподавателем;
- помощь в составлении структурно-логических схем дисциплины;
- помощь в подготовке обзоров по проблемам основных институтов изучаемой дисциплины.

2. Обсуждение и проверка подготовленных курсантами материалов:

- ознакомление с литературным обзором по теме, выполненным успевающими курсантами;
- проверка того, как курсанты готовятся к презентации докладов по темам.

3. Проверка конспектов тетрадей, выполнения домашних заданий.

4. Проведение контроля знаний курсантов.

5. Выставление оценок по выполненным заданиям.

6. Индивидуальные консультации для пропустивших и неуспевающих обучающихся.

Курсант должен обладать важнейшими общеучебными способами работы:

I. Умения и навыки планирования учебной деятельности:

• осознание учебной задачи;
• постановка целей;
• выбор рационального и оптимального пути их достижения;
•определение последовательности и продолжительности этапов деятельности;
• построение модели (алгоритма) деятельности;
• планирование самостоятельной работы на уроке и дома;
• планирование на день, неделю, месяц.

II. Умения и навыки организации своей учебной деятельности:

• организация рабочего места - наличие и состояние учебных средств, их рациональное размещение, создание благоприятных гигиенических условий;
• организация режима работы;
• организация домашней самостоятельной работы;

• определение порядка и способов умственных действий.

III. Умения и навыки восприятия информации, работа с различными источниками информации (коммуникативные):

• чтение, работа с книгой, конспектирование;

• библиографический поиск, работа со справочниками, словарями;

• слушание речи, запись прослушанного;

• внимательное восприятие информации, управление вниманием;

• наблюдение;

• запоминание.

Особую группу образуют умения и навыки работы с компьютером, в том числе:

- работа в Интернете;
- работа с электронным учебником;
- работа с обучающей программой;
- работа с контролирующей программой;
- работа в условиях дистанционного обучения;
- телеконференции по электронной почте (off-line) или в оперативном режиме (on-line);
- электронные доски объявлений;
- электронные библиотеки.
- доступ к базам данных через электронную почту (off-line) или в оперативном режиме (on-line),
- телевидеоконференции.

Обучающиеся должны уметь самостоятельно работать с литературой учебного и специального характера, находить интересующие их проблемы и уметь их раскрывать.

2.11 Методические рекомендации по подготовке реферата

Основные требования к написанию рефератов. Структура реферата определяется целью и задачами исследования. Работа должна выполняться на основе сочетания хронологического и проблемного принципов, состоять из введения, двух или трех глав, заключения и списка использованных источников. Объем в зависимости от сложности и изученности темы, составляет 10-15 машинописных страниц. В итоге реферат должен представлять собой завершенный самостоятельный труд автора по выбранной теме с необходимыми выводами и рекомендациями.

Содержание рефератов. Реферат, как было указано выше, имеет свою структуру, которая устанавливается исходя из темы и проблемы ее исследования. Сложилась определенная система в написании.

Так, во введении надо дать краткое описание, обоснование основных вопросов темы, которые автор намерен изучить и раскрыть. Во введении обосновываются актуальность темы, степень ее разработанности и теоретическая и правовая базы работы, формулируются цель и задачи исследования, излагаются новизна, практическая значимость работы.

Введение отражает современное обоснование решаемых автором вопросов, видение автором путей их исследования и новизну.

В основной части реферата – это, как правило, два или три раздела (глав) в которых содержатся основные положения и данные, отражающие сущность и решение выполненной самостоятельной работы обучающегося. В этой части реферата содержание можно разделить на пункты и параграфы, каждый из которых должен иметь законченную информацию по конкретно поставленному вопросу. В целом содержание работы должно отражать всю совокупность проделанного научного анализа и обобщение событий и фактов, дипломатических или других, имеющих к исследуемой теме отношение законодательных, нормативных актов, инструктивных положений и литературных источников. Широкая документальная база и полнота объема литературы, по теме исследования обеспечат высокое качество и обоснованность в выводе заключения.

В заключении – подводятся итоги проделанной работы, краткие выводы и полученные результаты, рекомендации и практические предложения.

В конце следует привести список использованных источников.

Реферат должен носить самостоятельный характер. Допускается использование источников лишь в форме цитат с указанием автора, наименования работы, года, места издания и страницы. Избегайте простого переписывания в текст реферата материала рекомендованных учебных и специальных изданий, ибо это дает право рецензенту на отрицательное заключение (незачет). Лучший способ пройти этап контрольного задания - создать свой вариант исполнения, что обеспечивает гарантию успеха и оставит прочные знания по курсу.

Оформление рефератов. Реферат может быть набран на компьютере 14-м шрифтом с соблюдением общепринятых требований. При наборе текста надо соблюдать следующие параметры оставления полей: левое - 30 мм, правое - 10 мм, верхнее - 20 мм, нижнее - 20 мм. Нумерация сквозная в правом нижнем углу (все страницы, включая схемы, диаграммы, приложения нумеруются по порядку). Рекомендуется следующий порядок размещения:

- титульный лист;
- содержание;
- введение;
- разделы (главы) реферата;
- заключение;
- список использованных источников;
- приложения.

При необходимости графики и таблицы могут сопровождаться с пояснительными текстами и указаниями на источники и литературы, из которых использованы необходимые данные.

Если в тексте используются цитаты, цифровая и иная информация, то надо дать соответствующие библиографические сноски. Сноски концевые (в конце текстовой части реферата по мере их использования).

Составление списка (перечня) использованных источников и литературы, других научных работ рекомендуется осуществлять соответственно библиографическому описанию документа. В случае если использованы материалы с Интернета, то необходимо привести официальное название сайта.

Рекомендуется следующая последовательность самостоятельной работы над литературой:

1) ознакомление с учебной программой по курсу «Расследование уголовных правонарушений связанных в сфере компьютерной информации и высоких технологий»;

2) освоение настоящих «Методических указаний...»;

3) проработка рекомендуемой литературы.

Этот примерный алгоритм действий целесообразно применять при изучении каждой темы курса.

Самостоятельная работа обучающегося является составной частью учебного процесса и имеет большое значение в подготовке высококвалифицированных специалистов для органов внутренних дел, т.к. от усвоения материала и подготовки домашнего задания в часы самоподготовки зависит в целом уровень подготовленности слушателя. Изучение дисциплины «Расследование уголовных правонарушений связанных в сфере компьютерной информации и высоких технологий» не только на семинарских и практических занятиях, но и в часы самоподготовки, призвано завершить становление будущего специалиста, способного после окончания учебного заведения, в условиях минимальной адаптации, находясь на различных должностях, самостоятельно выполнять поставленные перед ним задачи.

В ходе занятий обучающиеся приобретают навыки составления процессуальных документов и деловых бумаг следователя, приобретают первоначальные навыки и умения расследования уголовных дел, тогда как в часы самоподготовки обучающиеся учатся анализировать ситуацию, принимать самостоятельно решения и составлять процессуальные документы расследования, которые должны отвечать требованиям закона, как по форме, так и по содержанию. И только на занятиях преподаватель определяет и оценивает уровень подготовленности к занятиям, насколько обучающийся усвоил пройденный материал и самостоятельно выполнил учебное задание в часы самоподготовки.

2.12 Тестовые задания для самоконтроля

1. В соответствии с Уголовно-процессуальным кодексом, началом досудебного расследования является:

а) постановление о возбуждении уголовного дела;

б) регистрация заявления, сообщения об уголовном правонарушении в Едином реестре досудебных расследований;

в) постановление о привлечении в качестве обвиняемого;

г) задержание подозреваемого;
д) первое неотложное следственное действие.

2. Поводами к началу досудебного расследования являются:
а) сообщения в СМИ или рапорт должностного лица;
б) заявление физического лица либо сообщение должностного лица об уголовном правонарушении;
в) наличие достаточных данных, указывающих на признаки уголовного правонарушения;
г) явка с повинной;
д) постановление о начале досудебного расследования.

3. При наличии в поступившем заявлении, сообщении сведений о признаках административного правонарушения либо дисциплинарного проступка, что должен осуществить орган уголовного преследования?
а) зарегистрировать такое сообщение и начать расследование ничего не предпринимать;
б) обращение в течение трех суток передать сопроводительным письмом в соответствующий уполномоченный государственный орган или должностному лицу;
в) внести представление в соответствующий уполномоченный орган или должностному лицу о привлечении лица к административной или дисциплинарной ответственности;
г) передать по подследственности в территориальный орган.

4. Возможно ли производство осмотра без участия понятых, с использованием научно-технических средств?
а) нет, это запрещено уголовно-процессуальным законом;
б) нет, это запрещено указанием Генерального прокурора РК;
в) да, кроме случаев осмотра жилого помещения;
г) нет, участие понятых обязательно во всех случаях;
д) да, если понятые не желают принимать участие в следственном действии.

5. На какой срок применяется мера процессуального принуждения - доставление:
а) 1 час;
б) 2 часа;
в) 3 часа;
г) 24 часа;
д) 12 часов.

6. Кем определяется порядок ведения Единого реестра досудебных расследований?
а) районным прокурором;
б) районным судьей;

в) Министром внутренних дел;
г) Генеральным Прокурором;
д) начальником Департамента внутренних дел.

7. В чем, состоит запрет на приближение:
а) в ограничении подозреваемого, обвиняемого, подсудимого разыскивать, преследовать, посещать потерпевших и иных лиц, участвующих в деле, в целях их защиты;
б) вести телефонные переговоры, общаться иными способами с потерпевшим и иными лицами, участвующими в деле, в целях их защиты;
в) участковый инспектор выносит мотивированное постановление о запрете на приближение;
г) в ограждении потерпевшего следователем от последующих угроз;
д) в ограничении доступа к сведениям о защищаемом лице.

8. В каких случаях назначается комплексная экспертиза?
а) если следователь сомневается в заключение эксперта;
б) для установления обстоятельства, имеющего значение для дела, где требуется различные познания;
в) если следователь планирует присутствовать при производстве экспертизы;
г) если для заключения необходимы исследования на основе различных отраслей знаний;
д) в случае расследования особо тяжкого преступления.

9. Вся информация о преступлениях и происшествиях (согласно Приказа ГП РК №89 от 19.09.2014 г.), в зависимости от ее содержания подразделяется на:
а) заявления, сообщения, сведения в средствах массовой информации;
б) заявления, сообщения, жалобы, обращения и непосредственные усмотрения органа уголовного преследования;
в) заявления, сообщения, телефонные звонки, оповещения охранной сигнализации;
г) заявления, сообщения и информация об уголовных правонарушениях в электронном формате;
д) сообщения и заявления в электронном формате.

10. В каких случаях лицо не может быть задержано по подозрению в совершении уголовного правонарушения?
а) если оно застигнуто при совершении преступления или непосредственно после его совершения;
б) если очевидцы, в том числе и потерпевшие, прямо укажут на данное лицо как на совершившее преступление;
в) если потерпевший в показаниях указывает на большую вероятность совершения преступления конкретным лицом;
г) если на подозреваемом или в его жилище обнаружены явные следы преступления;

д) если имеются данные, указывающие на то, что лицо совершило административное правонарушение.

11. Какие предметы не признаются вещественными доказательствами?
а) предметы, которые служили орудиями преступления;
б) предметы, которые сохранили на себе следы преступления;
в) предметы, которые были объектами преступных действий подозреваемого;
г) предметы личной гигиены;
д) предметы первой необходимости.

12. В каких случаях лицо признается подозреваемым?
а) с момента начала досудебного расследования;
б) с момента вынесения постановления о признании в качестве подозреваемого;
в) с момента совершения уголовного правонарушения;
г) с момента задержания в порядке ст. 131 УПК РК;
д) с момента вынесения постановления о квалификации деяния подозреваемого.

13. Какое условие не является основанием для признания протокола не допустимым в качестве доказательства?
а) составление протокола ненадлежащим субъектом;
б) нарушение порядка предусмотренного УПК РК;
в) наличие технических ошибок (описок, исправлений и т.п.) не ставящих под сомнение достоверность и законность следственного действия;
г) несоответствие времени производства следственного действия указанного в протоколе фактическому его содержанию;
д) наличие орфографических ошибок.

14. Какое лицо признается потерпевшим?
а) которому непосредственно уголовным правонарушением причинен моральный, физический или имущественный вред;
б) обращения в правоохранительные органы с заявлением о преступлении;
в) которому нанесен вред деянием, совершенным невменяемым;
г) в отношение которого вынесено соответствующее постановление;
д) если задержаны лица, совершившие преступление.

15. В каких случаях разрешается проверка обращения без регистрации в КУИ?
а) когда имеется реальная возможность примирить заявителя с нарушителем без регистрации обращения;
б) когда имеется возможность повлиять на нарушителя оперативными силами и средствами;
в) в случае отсутствия судебной перспективы материала;
г) когда очевидна невозможность раскрытия преступления;

д) проверка обращения без регистрации в КУИ запрещается.

16. В случае отсутствия доступа к информационной системе ЕРДР каким образом производится регистрация заявлений и сообщений?
а) путем обращения в центр обслуживания населения;
б) путем обращения в районный акимат;
в) путем регистрации на электронных носителях;
г) составляется рапорт должностного лица;
д) путем регистрации в бумажном журнале учета регистрации досудебных расследований в случае аварийных ситуаций.

17. Какое решение не может принять следователь в случае обращения заявителя с информацией об уголовном правонарушении?
а) о начале досудебного расследования;
б) о прерывании сроков досудебного расследования;
в) о передаче заявления или сообщения по подследственности;
г) о проведении неотложного следственного действия;
д) о прекращении расследования.

18. Какие условия предусмотрены для избрания меры пресечения «личное поручительство»?
а) письменное ходатайство обвиняемого;
б) дееспособность лица, в отношении которого применяется мера пресечения;
в) письменное ходатайство поручителей;
г) ходатайство близких родственников обвиняемого;
д) согласие лица, в отношении которого применяется мера пресечения.

19. Какие фактические данные не могут служить основанием для применения меры пресечения?
а) о том, что подозреваемый скроется от дознания, предварительного следствия или суда;
б) о том, что подозреваемый воспрепятствует установлению истины по делу;
в) о том, что подозреваемый не имеет постоянного места работы;
г) о том, что подозреваемый будет заниматься преступной деятельностью;
д) о том, что подозреваемый совершил уголовное правонарушение.

20. Что понимается под обнаружением доказательств?
а) изъятие предметов у физических и юридических лиц;
б) запечатление доказательств при помощи научно-технических средств;
в) действия по выявлению и сохранению сведений об обстоятельствах уголовного правонарушения;
г) результаты досмотра и личного обыска;
д) изъятие предметов из внутренней полости человека.

21. С какого момента объект (предмет) признается вещественным доказательством по уголовному делу?
а) с момента его обнаружения в процессе следственного действия;
б) с момента определения его относимости к уголовному делу;
в) с момента его приобщения к уголовному делу соответствующим постановлением;
г) с момента составления обвинительного акта;
д) с момента вынесения постановления о квалификации деяния подозреваемого.

22. Какие обстоятельства не могут быть предметом допроса свидетеля?
а) обстоятельства, которые предшествовали совершению уголовного правонарушения;
б) обстоятельства, характеризующие личность подозреваемого;
в) обстоятельства, уличающие близких родственников в совершении уголовного правонарушения;
г) обстоятельства, которые свидетель воспринимал лично;
д) обстоятельства, изобличающие дающего показания в совершении уголовного правонарушения.

23. Предметом залога может быть:
а) имущество, отчуждение которого не допускается вследствие прямого указания на это в законодательных актах;
б) требования, неразрывно связанные с личностью кредиторов, в частности, требования об алиментах, возмещение вреда жизни и здоровью;
в) любое имущество, в том числе и имущественные права (требования);
г) личные неимущественные блага и права за исключением случаев, установленных законодательными актами;
д) имущество учреждений, которое им передано на праве оперативного управления.

24. С какой целью производится осмотр места происшествия?
а) сбора максимального объема проверочного материала;
б) установления обстоятельств, имеющих значение для дела;
в) задержания преступника;
г) с целью обнаружения и выявления следов уголовного правонарушения, вещественных доказательства и иных материальных объектов, выяснения обстановки происшествия и установления обстоятельств, имеющих значение для дела;
д) составления протокола осмотра места происшествия.

25. Какие условия являются основанием для признания протокола не допустимым в качестве доказательства?
а) составление протокола ненадлежащим субъектом;
б) нарушение порядка предусмотренного УПК РК;

в) наличие технических ошибок (описок, исправлений и т.п.) не ставящих под сомнение достоверность и законность следственного действия;
г) несоответствие времени производства следственного действия указанного в протоколе фактическому его содержанию;
д) протокол не подписан участниками процессуального действия.

26. Какие цели задержания предусмотрены законом?
а) пресечение уголовного правонарушения;
б) изоляция преступника от общества;
в) для обеспечения производства по уголовному проступку;
г) предотвращение возможности общения подозреваемого с соучастниками;
д) разрешение вопроса о применении меры пресечения в виде «содержание под стражей».

27. Какой признак не характеризует предмет как вещественное доказательство?
а) предмет изъят с места происшествия;
б) предмет служил орудием уголовного правонарушения;
в) предмет сохранил на себе следы уголовного правонарушения;
г) предмет явился объектом преступных действий;
д) ценности, нажитые преступным путем.

28. Какие меры процессуального принуждения можно применить к свидетелю при его неявке к следователю?
а) избрать меру пресечения;
б) осуществить привод;
в) отобрать обязательство о явке;
г) наложить штраф;
д) начать в отношении свидетеля досудебное расследование.

29. Какие права разъясняются лицу должностным лицом органа уголовного преследования при задержании его по подозрению в совершении уголовного правонарушения?
а) право на приглашение защитника, право хранить молчание и то, что сказанное им может быть использовано против него в суде;
б) право на обжалование действий и решений органа уголовного преследования и суда;
в) право на обращение к прокурору;
г) право на встречу с независимым экспертом по правам человека;
д) право на приглашение следственного судьи.

30. В каких целях применяются иные меры процессуального принуждения?
а) в целях предупреждения девиантного поведения отдельных участников;
б) в целях обеспечения предусмотренного УПК РК порядка расследования;

в) в целях обеспечения бесконфликтного хода расследования уголовного дела;
г) в профилактических целях;
д) в целях безопасности участников уголовного процесса.

2.13 Критерии оценки знаний обучающихся:

Оценка знаний обучающихся проводится в течение всего семестра в результате проведения текущего, рейтингового и итогового видов контроля, оцениваемых в процентном содержании.

Текущий контроль – систематическая проверка знаний обучающихся по отдельным вопросам и темам, осуществляется в рамках семинарских занятий и СРОП в виде устных и тестовых опросов, оценки выполненных заданий по СРО и СРОП.

Рейтинговый контроль – проверка учебных достижений обучающихся по завершённым темам, разделам программы, проводимая в виде коллоквиумов и тестовых опросов.

Семестровый рейтинг определяется по сумме текущего и рейтингового контролей и максимально составляет 60%. В течение семестра проводится две аттестации. Итоговый контроль (экзамен) по дисциплине проводится в форме компьютерного тестирования.

Итоговая оценка по дисциплине выставляется по сумме баллов семестрового рейтинга и баллов, полученных на экзамене. Знания, умения и навыки обучающихся оцениваются по следующей системе:

Оценка по буквенной системе	Цифровой эквивалент баллов	Процентное содержание	Оценка по традиционной системе
A	4,0	95-100	Отлично
A-	3,67	90-94	Хорошо
B+	3,33	85-89	
B	3,0	80-84	
B-	2,67	75-79	
C+	2,33	70-74	удовлетворительно
C	2,0	65-69	
C-	1,67	60-64	
D-	1,33	55-59	
D	1,0	50-54	
F	0	0-49	неудовлетворительно

«А», «А-» («отлично») - если обучающийся глубоко и прочно усвоил весь программный материал, исчерпывающе, последовательно, грамотно и логически стройно его излагает, не затрудняется с ответом при видоизменении задания, свободно справляется с поставленными задачами,

показывает знания монографического материала, правильно обосновывает принятые решения, владеет разносторонними навыками и приемами выполнения практических работ, обнаруживает умение самостоятельно обобщать и излагать материал, не допуская ошибок;

«B+», «B», «B-» («хорошо») - если обучающийся твердо знает программный материал, грамотно и по существу излагает его, не допускает существенных неточностей в ответе на вопрос, может правильно применить теоретические положения и владеет необходимыми навыками при выполнении практических задач;

«C+», «C», «C-» («удовлетворительно») - если обучающийся усвоил только основной материал, но не знает отдельных деталей, допускает неточности;

«D+», «D» («удовлетворительно») - если обучающийся усвоил только основной материал допускает недостаточно правильные формулировки, нарушает последовательность в изложении программного материала и испытывает затруднения в выполнении практических заданий;

«F» («неудовлетворительно») - если обучающийся не знает значительной части программного материала 0%-30%;

если обучающийся допускает существенные ошибки 30%-40%;

если обучающийся не знает значительной части программного материала с большим затруднением выполняет практические работы 40%-49%.

Выбор оценки в амплитуде колебаний от A- до A, от B- до B+, от D до C+ определяется степенью соответствия знаний и умений обучающегося вышеописанным критериям.

2.14 Экзаменационные вопросы по дисциплине

1. Развитие уголовно-процессуального законодательства в свете Концепции правовой политики Республики Казахстан на период с 2010 до 2020г.
2. Процесс доказывания в разрезе Послания Президента Республики Казахстан-Лидера нации Нурсултана Назарбаева народу Казахстана «Стратегия «Казахстан-2050»: новый политический курс состоявшегося государства»
3. Теоретические основы медиации в уголовном процессе.
4. Теоретические основы производства негласных следственных действий.
5. Теоретические основы института реабилитации и возмещения вреда, причинённого незаконными действиями органа, ведущего уголовный процесс.
6. Практическая реализация ускоренного досудебного расследования.
7. Суд присяжных заседателей. История, развитие и его место в свете Концепции правовой политики Республики Казахстан на период с 2010 до 2020г.г.

8. Теоретические основы привлечения юридических лиц к уголовной ответственности: уголовно-процессуальные аспекты.

9. Упрощённые производства в досудебном производстве и судебных стадиях. Соотношение современного развития в разрезе Концепции правовой политики Республики Казахстан на период с 2010 до 2020г.г.

10. Несоответствия современного развития отдельных уголовно-процессуальных институтов в разрезе Концепции правовой политики Республики Казахстан на период с 2010 до 2020г.г.

11. Теоретические модели современного уголовного процесса Казахстана.

12. Процессуальный статус следователя на современном этапе.

13. Теория судебных доказательств. Понятие, виды и современное состояние. (на основе анализа нового УПК РК от 04.07.2014г)

14. Понятие доказательств. Источники доказательств.

15. Научные классификации мер процессуального принуждения.

16. Казахстанская классификация мер процессуального принуждения.

17. Процессуальная форма. Единство и дифференциация процессуальной формы.

18. Соблюдение прав человека и гражданина при избрании мер процессуального принуждения.

19. Использование электронных средств слежения при избрании мер процессуального принуждения. (на опыте стран СНГ и дальнего зарубежья, современного состояния в Республике Казахстан)

20. Теоретические проблемы применения мер процессуального принуждения.

21. Процессуальные особенности участия медиатора в уголовном процессе.

22. Понятие и виды процессуальных документов составляемых в ходе досудебного расследования преступлений в сфере компьютерной информации и высоких технологий.

23. Поводы к началу досудебного расследования преступлений в сфере компьютерной информации и высоких технологий.

24. Правила приема, регистрации заявлений и сообщений об уголовных правонарушениях, а также ведения ЕРДР

25. Понятие и виды следственных действий в досудебном расследовании преступлений в сфере компьютерной информации и высоких технологий.

26. Общие процессуальные правила производства следственных действий по УПК РК по преступлениям в сфере компьютерной информации и высоких технологий

27. Алгоритм проведения следственных действий: этапы и характеристика.

28. Понятие и сущность следственного осмотра по преступлениям в сфере компьютерной информации и высоких технологий Организационная деятельность следователя при производстве следственного осмотра.

29. Участники следственного осмотра и их процессуальное положение.

30. Действия следователя (дознавателя) на подготовительном этапе осмотра места происшествия.

31. Этапы осмотра места происшествия по преступлениям в сфере компьютерной информации и высоких технологий.

32. Порядок взаимодействия участников следственно-оперативной группы при производстве осмотра места происшествия.

33. Порядок обнаружения и изъятия следов преступления и иных материальных объектов при производстве осмотра места происшествия.

34. Деятельность следователя по организации проведения допроса по преступлениям в сфере компьютерной информации и высоких технологий.

35. Процессуальное закрепление результатов допроса участников по преступлениям в сфере компьютерной информации и высоких технологий.

36. Понятие, значение, порядок допроса. Процессуальный порядок допроса по преступлениям в сфере компьютерной информации и высоких технологий.

37. Решение организационных вопросов при назначении судебных экспертиз по преступлениям в сфере компьютерной информации и высоких технологий.

38. Использование судебных экспертиз в качестве доказательств по уголовному делу по преступлениям в сфере компьютерной информации и высоких технологий.

39. Собирание, проверка, исследование и оценка вещественных доказательств по преступлениям в сфере компьютерной информации и высоких технологий

40. Основания задержания подозреваемого по преступлениям в сфере компьютерной информации и высоких технологий.

41. Меры пресечения: понятие, классификация и основания для избрания.

42. Процессуальный порядок окончания расследования по преступлениям в сфере компьютерной информации и высоких технологий.

43. Может ли осмотр места происшествия производить дознаватель?

44. Возможно ли производство осмотра без участия понятых, с использованием технических средств фиксации хода и результатов?

45. Каков срок досудебного расследования?

46. В каком случае производится эксгумация трупа из места захоронения?

47. Досудебное производство – это производство по делу с начала досудебного расследования до направления?

48. При задержании лица по подозрению в совершении преступления изымаются ли следователем ценности и деньги, находящиеся при задержанном, если они не являются вещественными доказательствами по делу?

49. Какие объекты не могут быть признаны вещественными доказательствами по уголовным делам?

50. Сколько понятых (минимальное число) может присутствовать при производстве следственных действий при отсутствии научно-технических средств?

51. Какое из перечисленных действий не является процессуальным?

52. С какого момента предмет считается вещественным доказательством по уголовному делу?

53. Какая из указанных категорий лиц не подлежит дактилоскопическому учету в Комитете по правовой статистике и специальным учетам Генеральной прокуратуры РК?

54. Обязательно ли для органа дознания поручение следователя в связи с производством по уголовному делу?

55. Вправе ли следователь заниматься оперативно-розыскной деятельностью по расследуемому делу?

56. Кем определяется порядок ведения Единого реестра досудебных расследований?

2.15 Составитель: доцент кафедры досудебного расследования преступлений, майор полиции Кемпирова Ж.С.

Министерство внутренних дел Республики Казахстан

Карагандинская академия им. Баримбека Бейсенова

Юридический институт

Кафедра досудебного расследования преступлений

«Утверждаю»
Заместитель начальника академии
по учебной работе
д.ю.н., профессор
полковник полиции
_____ З.С. Токубаев

«_____»_____2018 г.

Рабочая учебная программа (SYLLABUS)
по дисциплине

RUPSSKIVT 4315 «Расследование уголовных правонарушений связанных в сфере компьютерной информации и высоких технологий»

Специальность: 5В030300 Правоохранительная деятельность

форма обучения – ФЗО
курс: 4 (н.2017) СЮР
количество кредитов: 1 (45 часов)
лекций: 4
семинарских занятий: 3
практических занятий: 2
СРОП: 1
СРОП: 35
форма контроля – экзамен

Караганда 2018

Рабочая учебная программа (SYLLABUS) по дисциплине «Расследование уголовных правонарушений связанных в сфере компьютерной информации и высоких технологий» для специальности 5В030300 «Правоохранительная деятельность».

Составитель: доцент кафедры досудебного расследования преступлений, майор полиции Кемпирова Ж.С.

Рассмотрен на заседании кафедры_____

«__»_____ 2018 г., протокол №__

Начальник кафедры
Досудебного расследования преступлений
полковник полиции Калиев А.К.

Утверждена на заседании УМС_____

«__»_____ 2018 г., протокол №__

2.1. Основная информация:

4. Шифр и название специальности	5В030300 «Правоохранительная деятельность»
2. Курс, семестр	4 курс (н.2017) СЮР
3. Цикл дисциплины	Компонент по выбору. RUPSSKIVT 4315
4. Количество кредитов	1
5. Место проведения занятий	Учебные аудитории, лекционный зал
6. Лекторы (Ф.И.О., должность, ученая степень, др. контактная информация)	Доцент кафедры досудебного расследования преступлений Ногайбаева Алтынай Сансызбаевна; старший преподаватель кафедры досудебного расследования преступлений Хасенов Ербол Амантаевич; контактный телефон – 30-34-03, внут.- 333, 307.
7.Преподаватели, ведущие остальные виды занятий (Ф.И.О., должность, ученая степень, др. контактная информация)	Преподаватели кафедры досудебного расследования преступлений.

2.2. Пререквизиты: Теория государства и права. Нормы права. Система права и ее структура. Толкование норм права. Правовые отношения. Правонарушения и юридическая ответственность. Правоохранительные органы: Прокуратура РК. Органы внутренних дел РК. Органы досудебного расследования в РК. Уголовное право РК. Часть общая: Понятие преступления. Состав преступления. Уголовная ответственность и ее основания. Субъект преступления. Обстоятельства, исключающие уголовную ответственность. Стадии преступления. Соучастие в преступлении. Понятие, цели, система и виды наказаний. Назначение наказания. Освобождение от уголовной ответственности и наказания. Отсрочка исполнения наказания. Погашение и снятие судимости. Принудительные меры медицинского характера. Уголовное право. Часть особенная. Все разделы.

2.3. Постреквизиты: «Досудебное расследовани», «Криминалистика», «Прокурорский надзор в РК», «Уголовный процесс», «Основы оперативно-розыскной деятельности», «Судебная риторика», «Основы судебной медицины и психиатрии».

2.4. Краткое описание дисциплины

Цель: подготовка обучающихся по специальности 5В030300 - «Правоохранительная деятельность», которые способны после окончания института выполнять поставленные перед правоохранительными органами задачи по предупреждению, раскрытию и расследованию уголовных правонарушений. Кроме того, изучение обучающимися данной дисциплины

способствует в дальнейшем развитие навыков в составлении процессуальных документов.

В процессе изучения данной учебной дисциплины обучающийся должен:

- закрепить имеющиеся теоретические знания и практические навыки с учетом происшедших изменений и дополнений в уголовном и уголовно-процессуальном законодательстве;

- выработать умение и навыки применения уголовно-процессуальных норм в штатных и нештатных ситуациях, связанных с расследованием уголовных дел по осуществлению взаимодействия с другими правоохранительными органами РК;

- закрепить убежденность в необходимости строжайшего соблюдения законности и недопустимости любого нарушения закона, чем бы оно, не мотивировалось; совершенствовать навыки по составлению организационно-распорядительных документов и деловых бумаг следователя, оформлять материалы уголовного дела и приложения к нему.

знать:

— нормы права, имеющие основополагающее значение для достижения задач уголовного судопроизводства;

— теоретические основы квалификации общеуголовных правонарушений;

— основы раскрытия и расследования уголовных правонарушений, отнесенных к подследственности органов досудебного расследования ОВД;

— основы взаимодействия с другими правоохранительными органами и с общественностью;

— основы форм и методов взаимодействия оперативных подразделений с другими службами в ходе предупреждения, раскрытия и расследования уголовных правонарушений;

— теоретические основы принятия процессуальных, тактических и организационных решений в ходе расследования;

— процессуальный порядок применения мер процессуального принуждения в отношении подозреваемых в совершении уголовных правонарушений;

— теоретические основы производства неотложных и первоначальных следственных действий;

— тактико-технические возможности криминалистической техники;

— общую характеристику оперативных и криминалистических учетов;

— перечень современных технико-криминалистических средств, методов и приемов фиксации, поиска, обнаружения, изъятия и исследования вещественных доказательств в целях раскрытия и расследования уголовных правонарушений;

уметь:

— правильно применять нормы права, имеющие основополагающие значения для достижения задач уголовного судопроизводства;

— принимать уголовно-процессуальные, тактические и организационные решения;

— оформлять и использовать сведения, полученные в процессе проведения оперативно- розыскных мероприятий;

— составлять статистические карточки и пользоваться оперативными и криминалистическими учетами;

— использовать технико-криминалистические средства, методы и приемы фиксации, поиска, обнаружения, изъятия и исследования вещественных доказательств в целях раскрытия и расследования уголовных правонарушений;

— разрабатывать и выдвигать следственные версии, обеспечивающие раскрытие уголовных правонарушений и установление виновных лиц;

— организовывать и проводить следственные действия в соответствии с уголовно- процессуальным законодательством;

— осуществлять взаимодействие со службами и подразделениями правоохранительных органов Республики Казахстан и других стран;

— обеспечивать реализацию прав и исполнение обязанностей участниками процесса, принимать меры к обеспечению безопасности;

— исчислять процессуальные сроки и решать вопросы об их продлении;

Дисциплина изучается обучающимися на 4 курсе. В конце обучающиеся сдают экзамен. Основными формами обучения являются лекции, семинарские и практические занятия, СРОП.

На занятиях для усвоения и закрепления навыков практической работы в сфере уголовного судопроизводства обучающиеся решают ситуационные задачи, составляют процессуальные документы.

Ожидаемые результаты: Изучение данной дисциплины способно привить умения и навыки проведения следственных действий, закрепления результатов, составления наиболее сложных процессуальных документов и деловых бумаг следователя. Приобретение данных навыков позволит в практической деятельности самостоятельно проводить расследование по уголовным делам.

2.5. График выполнения и сдачи заданий по дисциплине:

№	Виды работ	Цель и содержание задания	Ссылка на список рекомендованной	Форма контроля (согласно рейтинг-шкале)	Баллы (согласно рейтинг-шкале)	Форма отчетности	Сроки сдачи
1	2	3	4	5	6	7	8
2	1.Проверка конспектов. 2.Решение задач	Текущий контроль			0-100	Ответ Конс-пект	по расписанию

5.	1. Проверка конспектов 2. Опрос по теме 3.Решение задач	Текущий контроль			0-100	Ответ Конс-пект	по расписанию
6.	1. Проверка конспектов 2. Опрос по теме 3.Решение задач	Текущий контроль			0-100	Ответ Конс-пект Тест	по расписанию

2.6. Политика курса.

а) обязательное посещение всех аудиторных и внеаудиторных занятий СРОП согласно расписания.

б) регулярная подготовка к занятиям;

в) активность во время семинарских, практических и СРОП занятий

г) отработка в определенное преподавателем время пропущенных занятий;

д) соблюдение дисциплины.

Недопустимо:

а) опоздание и уход с занятий;

б) несвоевременная сдача заданий;

в) пользование сотовыми телефонами во время занятий, посторонние разговоры, жевание жевательной резинки;

г) обман и плагиат.

2.7. Список рекомендованной литературы

№ п/п	Автор, наименование	Год, место издания
1. Нормативные правовые акты		
1	Конституция РК принятая на республиканском референдуме 30 августа 1995 г. (с изменениями и дополнениями на 10.03.2017г.).	//http://online.zakon.kz.
2	Уголовный кодекс Республики Казахстан № 226-v-ЗРК от 03.07. 2014г. (с изменениями и дополнениями по состоянию на 09.01.2018 г.).	//http://online.zakon.kz.
3	Уголовно-процессуальный кодекс Республики Казахстан № 231-V-ЗРК от 04.07.2014г. (с изменениями и дополнениями по состоянию на 24.05.2018 г.).	//http://online.zakon.kz.
4	Закон республики казахстан от 23 апреля 2014 года № 199-v «об органах внутренних дел Республики Казахстан» (с изменениями и дополнениями по	//http://online.zakon.kz.

	состоянию на 24.05.2015 г.).	
5	Приказ Генерального прокурора Республики Казахстан от 22 сентября 2014 года №91 «Об утверждении Правил применения научно-технических средств фиксации хода и результатов следственных действий»	//http://online.zakon.kz.
6	Приказ Генерального Прокурора Республики Казахстан «Об утверждении правил приема и регистрации заявлений и сообщений об уголовных правонарушениях, а также ведения Единого реестра досудебных расследований» №89 от 19.09.2014г. с изм. и доп. от 10.08.2015 г. №99, 23.09.2016 №148.	//http://online.zakon.kz.
7	Приказ Генерального Прокурора Республики Казахстан «Об утверждении Положения о Департаменте по надзору за законностью досудебной стадии уголовного процесса ГП» № 125 от 09.10.2012г.	//http://online.zakon.kz.
8	Приказ Генерального Прокурора Республики Казахстан «Об усилении прокурорского надзора за соблюдением конституционных прав и свобод человека и гражданина в уголовном процессе» № 46 от 17.08.2006г.	//http://online.zakon.kz.
9	Инструкции «О порядке изъятия, учета, хранения, передачи и уничтожения вещественных доказательств, документов по уголовным делам, гражданским делам и делам об административных правонарушениях судом, органами прокуратуры, досудебного следствия, дознания и судебной экспертизы». Совместный приказ Министра юстиции Республики Казахстан от 12 ноября 1998 г. N 121, Генерального прокурора Республики Казахстан от 1 декабря 1998 года N 1043ца, Председателя КНБ Республики Казахстан от 8 декабря 1998 года N 73, Министра финансов Республики Казахстан от 22 декабря 1998 года N 598, Министра внутренних дел Республики Казахстан от 2 декабря 1998 года N 429, Министра государственных доходов Республики Казахстан от 28 декабря 1998 года N 111. Зарегистрирован Министерством юстиции Республики Казахстан 30.12.1998 г. N 658	//http://online.zakon.kz.
10	Закон Республики Казахстан от 30.03.1999 N 353-I ЗРК "О порядке и условиях содержания лиц в специальных учреждениях, обеспечивающих временную изоляцию от общества"	//http://online.zakon.kz.

11	Закон Республики Казахстан от 10 июля 1998 года № 279-I о наркотических средствах, психотропных веществах, прекурсорах и мерах противодействия их незаконному обороту и злоупотреблению ими (с изменениями и дополнениями по состоянию на 29.12.2014 г.)	//http://online.zakon.kz.
12	Нормативное Постановление Верховного суда РК от 20.04.2006 N 4 "О некоторых вопросах оценки доказательств по уголовным делам"	//http://online.zakon.kz.
13	Приказ Министра внутренних дел Республики Казахстан от 6 мая 2004 года № 256 О внесении изменений и дополнений в приказ Министра внутренних дел Республики Казахстан от 6 июля 2001 года № 543 «О мерах по совершенствованию деятельности следствия, дознания, оперативно-криминалистической службы органов внутренних дел Республики Казахстан»	//http://online.zakon.kz.
14	Закон Республики Казахстан «О судебно-экспертной деятельности в Республике Казахстан» (с изменениями и дополнениями по состоянию на 29.09.2014 г.)	//http://online.zakon.kz.
15	Приказ Генерального Прокурора Республики Казахстан от 02 мая 2018 года № 60 «О некоторых вопросах организации прокурорского надзора».	//http://online.zakon.kz.
2. Основная литература		
16	Назарбаев Н.А. «Новые возможности развития в условиях четвертой промышленной революции». Послание Президента Республики Казахстан народу Казахстана от 10 января 2018 года.	Официальный сайт Президента Республики Казахстан. //http://www.akorda.kz/
17	Капсалямов К.Ж. Уголовное преследование и способы собирания доказательств.	Астана, 2001.
18	Бекжанов А.А., Ташибаев К.У., Турсынов Е.Т. Производство дознания по УПК РК.	Караганда, 1998.
19	Сарсенбаев Т.Е., Хан А.Л. Уголовный процесс. Досудебное производство.	Астана, 2000.
20	Тяжина А.О., Ногайбаева А.С. Новеллы досудебного расследования по УПК Республики Казахстан: учебно-практическое пособие (краткий анализ в схемах)	Караганда, 2015.
21	Тяжина А.О., Ногайбаева А.С., Бейсенбаев А.Ж. Досудебное производство по уголовным делам: образцы процессуальных документов.	Караганда, 2014.
22	Кенжетаев Д.Т., Калиев А.К., Балтабаев Т.Н.	Караганда, 2014.

	Примерные образцы уголовно-процессуальных документов досудебного расследования.	
23	Громов В.И. Заключение эксперта как источник доказательства.	М.://Юстиция.1997. № 9
24	Шурухнов Н.Г. Тактика следственного осмотра и освидетельствования Криминалистика: Курс лекций.	Москва: Эксмо. 2006.
25	Журсимбаев С.К. Роль прокурора при отправлении уголовного правосудия.	Алматы, 2002 год.
	3. Дополнительная литература	
26	Руководство для следователей/ Под ред. Н.А. Селиванова В.А., Снеткова.	Москва, 1998 г.
27	Бахин В., Когамов М., Карпов Н. Допрос на предварительном следствии (уголовно – процессуальные и криминалистические вопросы): Монография. Изд. 2-е.	Алматы: Жеті жарғы, 2004. 192с.
28	Диков Д., Сейгер К., Фонстрох У. Компьютерные преступления	Москва, 1999 г.
29	Ляпунов Ю.И., Максимов В.С. Ответственность за компьютерные преступления	Москва,// Законность. 1997. № 1.
30	Бахарев Н.В. Очная ставка: уголовно процессуальные и криминалистические вопросы	Москва: Госюриздат1 983.
31	Гаврилов А.К. Следственные действия: (процессуальная характеристика, тактические и психологические особенности) А.К. Гаврилов, Б.П. Смагоринский.	Москва: ИКФ Экмос,1994 г.
32	Алиев Т.Т. Доказательства, понятие, свойства / Т.Т. Алиев, Н.А. Громов, А.И. Гришин // Закон и право.	А. - 2002 г. - №3.
33	Скоромников К.С. Расследование преступлений в сфере компьютерной информации // Руководство для следователей / Под ред. Н.А.Селиванова, В.А. Снеткова.	Москва, 1997.
34	Шуменова Р.Т. Система процессуальных гарантий обеспечения принципов уголовного судопроизводства. Монография.	Алматы, 2003 г. с.89
35	Бегалиев К. А Меры пресечения по УПК РК// Гос. и право.	Алматы, 2003 г.
36	Расследование неправомерного доступа к компьютерной информации. Научно-практической пособие / Под ред. Н.Г. Шурухнова.	Москва, 1999г.
37	Жалыбин С. М. Обеспечение прав человека при уголовном преследовании. - Правовая реформа в Казахстане.	Алматы – 2001г. № 1.

2.8. ТЕМАТИЧЕСКИЙ ПЛАН

по дисциплине «Расследование уголовных правонарушений, связанных в сфере компьютерной информации и высоких технологий» для преподавания обучающимся 4 курса СЮР (набор 2017 г.) факультета заочного обучения юридического института в 2018-2019 учебном году

Количество кредитов - 1 (45 часов)

№ п/п	Номер темы	Название темы	Кол-во кредитов (часов)	Аудиторные часы			СРОП		СРО
				лекции	семинарские занятия	практические занятия	аудиторные	внеаудиторны	
1	1	Общая характеристика досудебного расследования в сфере компьютерной информации и высоких технологий	15	1	1	1			12
2	2	Деятельность следователя по проверке законности и обоснованности повода к началу досудебного расследования в сфере компьютерной информации и высоких технологий	16	2	1	1			12
3	3	Процессуальный порядок определения статуса потерпевшего, организация и проведение допроса потерпевшего	14	1	1			1	11
Итого в семестре:			45	4	3	2		1	35

2.9. Планы занятий

Тема 1. Общая характеристика досудебного расследования в сфере компьютерной информации и высоких технологий

Лекция – 1 час

Цель занятия: выработка профессиональных навыков по принятию процессуальных решений, составлению сопутствующих процессуальных документов; привитие навыков по использованию законодательных и иных нормативных актов в работе с доказательствами; привитие уважительного отношения к закону.

План лекции

1. Понятие и значение преступления в сфере высоких информационных технологий.
2. Направления преступной деятельности в информационной сфере и их классификация.

Тезисы лекции:

Компьютерно-информационные технологии функционируют относительно давно, и их развитие происходит огромными темпами, что связано с большой заинтересованностью в этом широких слоев населения. Преступления, связанные с использованием компьютерной техники, - это лишь специализированная часть преступной деятельности в информационной сферы. К данной категории относятся и преступления, при совершении которых осуществляется неправомерный доступ к охраняемой законом компьютерной информации. В течение последних 15-20 лет по мере компьютеризации хозяйственно-управленческой и финансово коммерческой деятельности появились новые виды преступлений, которые стали называться компьютерными, исходя из терминологии зарубежной юридической практики. Первое преступление подобного типа в бывшем СССР было зарегистрировано в 1979 г. в городе Вильнюсе. Тогда ущерб государству составил около 80 тысяч рублей. Этот случай явился определенной отправной точкой в развитии и исследовании нового вида преступлений.

Только в последние годы появились работы по проблемам борьбы с компьютерной преступностью, в которых рассматриваются в основном уголовно-правовые и криминологические аспекты этого явления. Как нередко случалось уже ранее, например, ситуация с наркоманией или с организованной преступностью, борьба с этим социально опасным явлением началась лишь после того, как материальные потери от этого вида преступлений достигли существенных размеров и стали резко выделяться на общем фоне потерь от обычных видов обще уголовной преступности.

Для того чтобы четко определить суть проблемы, для любой науки вполне логичен подход, когда все исследователи конкретной предметной области организуют свое общение на основе единообразно понимаемых терминов и пытаются обеспечить некую стабильность понятий нотерминологического аппарата.

Так, А. В. Дулов к компьютерным преступлениям относит «различные преступления, совершаемые с помощью компьютеров, с нарушением их

деятельности». Нам кажется, подобное определение является довольно широким и содержащим существенную неточность: результатом компьютерного преступления не обязательно должно быть нарушение деятельности самих компьютеров. Общественно-опасные последствия могут наступать и при нормальном функционировании программно-аппаратных средств компьютера при условии неверных исходных данных, при ошибках оператора или программиста, при кражах машинного времени, неправомерном доступе и т. д.

Н. А. Селиванов относит к компьютерным преступлениям, преступления, предметом которых является компьютерная информация, либо средством совершения которых выступает электронно-вычислительная техника, используемая с целью совершения противоправного посягательства на иной объект. Опровергая данную точку зрения, В. В. Крылов считает, что подход, согласно которому в законодательстве следует отражать конкретные технические средства, себя не оправдывает и поэтому нецелесообразно принимать термин «компьютерные преступления» за основу для наименования в криминалистике всей совокупности преступлений в области информационных отношений. Компьютер, по его мнению, является лишь одной из разновидностей информационного оборудования и проблемами использования этого оборудования не исчерпывается совокупность отношений, связанных с обращением конфиденциальной документированной информации. В. В. Крылов предлагает рассматривать в качестве базового понятия «информационные преступления», исходя из того, что сложившаяся система правоотношений в области информационной деятельности позволяет абстрагироваться от конкретных технических средств. Он делает вывод, что преступления в области компьютерной информации, выделенные в отдельную главу УК, являются частью информационных преступлений, объединенных общим инструментом обработки информации — компьютером.

Ю.М. Батурин подразделяет объекты компьютерных атак натри категории сами компьютеры, объекты, которые могут быть атакованы с помощью компьютера как инструмента, объекты, для которых компьютер является окружением.

Представляется обоснованным не включать в состав объектов компьютерных преступлений первую категорию по данной классификации в случаях, когда компьютеры являются не более чем имуществом, абсолютно равнозначным любым другим материальным вещам, и не подлежат выделению в отдельную правовую категорию единственно по признаку их наименования.

Классической точки зрения о том, что рамки компьютерных преступлений можно ограничить использованием ПК в качестве инструмента (орудия) и предмета посягательства, придерживается и Н. Ф. Ахраменко, при этом указывает, что сам компьютер не может быть рассмотрен как предмет компьютерных преступлений, так как «предметом посягательств при их совершении является отнюдь не техника как таковая (ей ущерб, как правило,

не наносится), а информация, хранимая, обрабатываемая или передаваемая этой техникой. Определяя объект компьютерных посягательств, мы исходим из того, что преступления такого рода с гораздо большим основанием следует, отнести к информационным». На наш взгляд, предмет компьютерных преступлений следует еще больше расширить: помимо информации включить еще нормальное функционирование вычислительной техники и течение информационных процессов.

Несомненно, данный перечень мнений не является исчерпывающим, однако важно другое: необходимо различать преступления в сфере высоких информационных технологий и так называемые компьютерные преступления. К сожалению, последний термин настолько прочно вошел в обиход научных и практических работников, как в Казахстане, так и за рубежом, что стал уже традиционным, и некоторые авторы полагают, что вряд ли стоит его менять, «поскольку многие названия со временем приобретают условный характер».

Различие в терминологии указывает не только на обеспокоенность общества новой угрозой, но и на отсутствие полного понимания сути этой угрозы. Важно, что терминологическая неточность изложения закона или методологической рекомендации по его исполнению может повлечь неправильное его применение, а, следовательно, и негативные последствия.

Следует отметить, что общепризнанного определения преступления, совершаемого с ииспользованием или в отношении средств вычислительной техники, компьютерной информации, программного обеспечения, на сегодняшний день не имеется, вообще, а уголовное право иностранных государств охватывает этим понятием различные по своему характеру и степени общественной опасности виды противоправных деяний.

Наиболее распространенное определение — «преступление, совершенное с использованием компьютерной техники или направленное против безопасности компьютерной информации» — не отвечает потребностям науки и практики сегодняшнего дня и нуждается в уточнении.

К вопросу криминализации правонарушений в сфере высоких информационных технологий сегодня в мире существует три подхода.

Первый заключается в отнесении к преступлениям несанкционированного доступа в защищенные компьютерные системы, заражения вирусами, противоправного использования компьютерных систем и информации. Он характерен для таких стран, как Норвегия, Сингапур, Словакия, Филиппины, Южная Корея.

Второй подход заключается в признании компьютерными преступлениями лишь тех деяний, которые связаны с причинением ущерба имуществу и электронной обработке информации (Австрия, Дания, Швеция, Швейцария, Япония). Например, в законодательстве Австрии, Дании, предусматривается уголовная ответственность за неправомочное вмешательство в функционирование информационно-вычислительных систем.

Третий подход характерен для стран с высоким уровнем компьютеризации (США, Великобритания, Франция, Германия, Нидерланды) и развитой правовой базой. Он состоит в криминализации деяний, связанных не только с имущественным ущербом, но и с нарушением прав личности, с угрозой национальной безопасности и т. д. Так, из содержания норм уголовного права Великобритании следует, что его санкции применяются к «злоумышленникам, причинившим с помощью ПК ущерб или использовавшим информацию в своих целях». В 80-е годы системой уголовной юстиции ФРГ был предложен целый ряд уголовно-правовых определений исследуемой категории противоправных деяний. Уголовная полиция этой страны к преступлениям в сфере высоких технологий относит «все противоправные действия, при которых электронная обработка информации является орудием их совершения и(или) их объектом».

Для того чтобы понять, что же представляет собой «охраняемая законом компьютерная информация», мы приведем краткий перечень некоторых видов информации, охраняемых законодательством Республики Казахстан, которые одновременно подлежат защите — государственные секреты; служебная и коммерческая тайна; банковская тайна; нераскрытая информация; личная и семейная тайны, тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений; тайна усыновления (удочерения) ребенка; адвокатская тайна; тайна пенсионных накоплений получателя.

При этом информация — это сведения или данные, объективно отражающие различные стороны и элементы окружающего мира и деятельности человека на определенном этапе развития общества, представляющие для него какой-либо интерес, и материализованные в форме, удобной для использования, передачи, хранения и обработки (преобразования) человеком или автоматизированными средствами.

«Охраняемая законом компьютерная информация», как вид информации, представляет собой сведения, зафиксированные на машинном, магнитном носителе, представленные в форме набора состояний элементов ПК, иных электронных средств обработки, хранения и передачи информации.

Компьютерная техника и средства коммуникаций на территории Республики Казахстан используются в большей степени не как объекты посягательства (для сравнения, неправомерный доступ к компьютерной информации, хищение машинного времени, а также денежных средств посредством электронной транзакции — вот далеко не полный перечень преступлений, с которыми вынуждены бороться правоохранительные органы США, Канады, стран Европы и т. д.), а в большей степени как средства преступной деятельности. Причина — высокая латентность данного вида преступлений и слабо развитые, а иногда даже отсутствующие компьютерно-информационные сети. За рубежом, например, активно борются с проблемой латентности.

Еще одна из причин роста таких преступлений в Казахстане — это разрыв в уровнях развития информационного общества по сравнению с Западом, порождающий иногда абсурдные ситуации, нестыковки моральных, правовых стандартов и норм. Создаются условия для соблазна, искушения воспользоваться более удобной и дешевой формой обеспечения информацией. Взять, например, проблему сохранения интеллектуальной собственности. Лицензионные программы стоят очень дорого для массового потребителя, и нет моральных преград, пользоваться «взломанными» программами, которые во много раз дешевле.

Одним из новых направлений для преступной деятельности в информационной сфере является использование глобальных коммуникационных информационных систем с удаленным доступом к совместно используемым ресурсам сетей, таких как Интернет. В настоящее время Интернет, использующий в большинстве случаев телефонные линии, представляет собой глобальную систему обмена информационными потоками, объединяющую около 30000 мелких локальных сетей и более 30 миллионов пользователей, число которых постоянно растет. Вполне закономерно, что подобная информационная сеть, объединившая огромное число людей с возможностью подключения к ней любого человека, стала не только предметом преступного посягательства, но и очень эффективным средством совершения преступлений.

Используя Интернет в качестве среды для противоправной деятельности, преступники очень часто делают акцент на возможности, которые им дает сеть, обмена информацией, в том числе и криминального характера. Аналогичная ситуация складывается и при использовании компьютерных мини процессоров, составляющих основу современной мобильной или так называемой сотовой телефонной связи. Однако следует отметить, что большинство ее видов при эксплуатации позволяют оперировать лишь аудио и небольшими по объему частями текстовой информации, в то время как подключение этих устройств к цифровым каналам Интернет позволяет передавать не только аудио-, но и видеоинформацию, а также практически не ограниченные объемы текстовой и графической информации.

Другая черта сети Интернет, которая привлекает преступников, - возможность осуществлять в глобальных масштабах информационно психологическое воздействие на людей. Преступное сообщество весьма заинтересовано в распространении своих доктрин и учений, в формировании общественного мнения, благоприятного для укрепления позиций представителей преступного мира, и в дискредитации правоохранительных органов. При этом можно выделить следующие характерные особенности преступлений в сфере высоких информационных технологий: неоднородность объекта посягательства; выступление компьютерной информации, как в качестве объекта, так и в качестве средства преступления; многообразие предметов и средств

преступного посягательства; выступление компьютера либо в качестве предмета, либо в качестве средства совершения преступления.

С учетом особенностей совершения преступлений с использованием информационных технологий на сегодняшний день является актуальным целый комплекс юридических и технических проблем, связанных с: неадекватным состоянием национального законодательства (в уголовном законодательстве отсутствует соответствующая общественной опасности содеянного оценка действий, по своей сути являющихся преступлениями, но не нашедших разрешения; в уголовно-процессуальном законодательстве не определены процедуры в от ношении материальных объектов, не имеющих вещественных признаков — «электронные» доказательства, «электронные обыски и выемки» и т. п.); несформированностью структур правоохранительных органов, призванных бороться с данными видами преступлений, отсутствие оперативно розыскных методик по их предупреждению и раскрытию, судебно-следственной практики, по такого рода делам, специально обученного личного состава; крайне низкой оснащённостью правоохранительных органов специальными аппаратными и программными средствами, без которых эффективная борьба с этим новым видом преступлений практически невозможна; низкой профессиональной подготовкой сотрудников спецподразделений.

В связи с чем становится актуальным определение направленности совершенствования борьбы с «компьютерной» преступностью путем создания Концепции «Стратегия и тактика борьбы с преступностью в сфере высоких информационных технологий», а также внесения дополнений в уголовно процессуальное законодательство.

Существенную помощь в исследовании какого-либо предмета оказывает проведение классификации этого предмета или явления. Аналогично понятию преступлений в сфере высоких информационных технологий в литературе нет единого мнения о том, каким образом и по каким критериям классифицировать преступления в этой сфере. Одной из первых попыток было предложенное Ю. М. Батуриным разделение преступлений по способу их совершения: методы перехвата; методы несанкционированного доступа; методы манипуляции.

Определенный интерес представляет также предложенная В. А. Мещеряковым классификация, строящаяся на идеи не столько преступлений, сколько совокупности возможных противоправных посягательств в этой сфере.

1. Неправомерное завладение информацией или нарушение исключи тельного права ее использования:

-неправомерное завладение информацией как совокупностью сведений, документов (нарушение исключительного права владения);

-неправомерное завладение информацией как товаром;

-неправомерное завладение информацией как идеей (алгоритмом, методом решения задачи).

2. Неправомерная модификация информации:

-как товара с целью воспользоваться ее полезными свойствами (снятие защиты);

-как идеи, алгоритма и выдача за свою (подправка алгоритма);

-как совокупности фактов, сведений.

3. Разрушение информации:

-разрушение информации как товара;

-уничтожение информации.

4. Действие или бездействие по созданию (генерации) информации с заданными свойствами:

-распространение по телекоммуникационным каналам информационно вычислительных сетей информации, наносящей ущерб государству, обществу и личности;

-разработка и распространение компьютерных вирусов и прочих вредоносных программ для ПК;

- преступная халатность при разработке (эксплуатации) программного
обеспечения, алгоритма в нарушение установленных технических норм и правил.

5. Действия, направленные на создание препятствий пользования информацией законным пользователям:

-неправомерное использование ресурсов автоматизированных систем (памяти, машинного времени и т. п.);

-информационное «подавление» узлов телекоммуникационных систем (создание потока ложных вызовов).

Указанная классификация имеет ощутимое преимущество перед остальными — ее основанием являются не абстрактные юридические модели, а реальные правонарушения, совершаемые в настоящее время.

Наиболее удачной на тот период времени, по нашему мнению, является классификация, предложенная Марком Экенвайлером, в которой он выделяет три основные категории (с дальнейшей дифференциацией) в зависимости от способа использования компьютера при совершении преступлений:

1. Компьютер является объектом правонарушения, когда цель преступника — похитить информацию или нанести вред интересующей его системе:

-изъятие средств компьютерной техники с находящейся в ней информацией;

-хищение информации;

-хищение услуг (получение несанкционированного доступа к какой-то системе с целью безвозмездного пользования предоставляемыми ею услугами);

-повреждение системы. Данная группа объединяет преступления, совершаемых с целью разрушить или изменить данные, являющиеся важными для владельца или одного или многих пользователей системы — объекта несанкционированного доступа.

2. Компьютеры используются как средства, способствующие совершению преступления:

-как средство совершения традиционных преступлений (как правило, мошенничество);

-как средство атаки на другой компьютер, средство совершения иного компьютерного преступления.

3. Компьютер используется как запоминающее устройство (например, после взлома системы создается специальная директория для хранения файлов, содержащих программные средства преступника, пароли для других узлов, списки украденных номеров кредитных карточек и т. п.)

Предложенная классификация позволит систематизировать уголовно правовые аспекты определения видов преступлений в сфере высоких информационных технологий, а также определить способы совершения, конкретные приемы их применения, используемые при этом технические средства, методы подготовки и исполнения преступления и множество иных обстоятельств, имеющих следственно-оперативное значение при расследовании и раскрытии преступлений в сфере высоких информационных технологий.

Методические рекомендации:

4. Изучить основную литературу.
5. Ознакомиться с дополнительной литературой.
6. Законспектировать основные положения нормативных актов, вопросы лекционных занятий и т.д.

Список рекомендованной литературы

1, 3, 6, 13, 17, 19, 20, 21, 22, 26, 31, 32.

Тема 1. Общая характеристика досудебного расследования в сфере компьютерной информации и высоких технологий

Семинар – 1 час

Цель занятия: выработка профессиональных навыков по принятию процессуальных решений, составлению сопутствующих процессуальных документов; привитие навыков по использованию законодательных и иных нормативных актов в работе с доказательствами; привитие уважительного отношения к закону.

Вопросы занятия:

1. Преступления в сфере высоких информационных технологий .
2. Понятие и значение преступления в сфере высоких информационных технологий.
3. Направления преступной деятельности в информационной сфере и их классификация.

4. Основные обстоятельства, подлежащие установлению и доказыванию при расследовании преступлений в сфере высоких информационных технологий.

5. Общие условия производства досудебного расследования преступления в сфере высоких информационных технологий.

6. Правовое регулирование отношений в области компьютерной информации.

Задание: подготовить устный ответ.

Список рекомендованной литературы

1, 3, 6, 13, 17, 19, 20, 21, 22, 26, 34, 37.

Тема 1. Общая характеристика досудебного расследования в сфере компьютерной информации и высоких технологий

Практическое занятие – 1 час

Цель занятия: выработка профессиональных навыков по принятию процессуальных решений, составлению сопутствующих процессуальных документов; привитие навыков по использованию законодательных и иных нормативных актов в работе с доказательствами; привитие уважительного отношения к закону.

Вводная:

В УВД г. Энска поступило заявление от юриста торгового порта «Заря», о том, что после увольнения с должности ведущего инженера программиста Шамилова А.Н. была удалена с сервера вся бухгалтерская и финансовая информация, справочные и персональные сведения о судах, коммерческих партнерах и сотрудниках. Деятельность торгового порта в течение двух дней была парализована, поскольку предприятие оказалось неспособным выполнять свои обязательства по получению и отправки грузов.

В ходе оперативно-розыскных мероприятий было установлено, что гражданин Шамилов А.Н. из хулиганских побуждений уничтожил информацию, составляющую коммерческую тайну торгового порта, где он ранее работал. Используя сеть Интернет, через домашний компьютер он подключился к базе данных и удалил с сервера всю имеющуюся информацию.

Задание:

1. С учетом полученной информации необходимо дать анализ сложившейся ситуации.

2. Какое процессуальное решение необходимо принять в данной ситуации.

3. Составьте план проведения первоначальных следственных действий и оперативно-розыскных мероприятий.

4. С учетом полученной информации допросить лицо, сообщившее об уголовном правонарушении.

5. Проведите имитацию допроса подозреваемого лица Шамилова А.Н. и составьте соответствующий протокол.

Порядок контроля и оценки знаний:

1. Оценка правильности и содержательности ответов (использование УПК и норм. актов)

2. Оценка активного участия в дискуссии.

3. Качество составленных документов.

4. Качество проведения процессуальных действий.

Выступление с подготовленной презентацией в программе PoverPoint 2003-2007.

Нормативно правовые акты: 2,3,6.

Основная литература: 2,3,7.

Дополнительная литература: 24,25,26,30,31,32,33,35,36,37,38,39, 40.

Тема 1. Общая характеристика досудебного расследования в сфере компьютерной информации и высоких технологий

СРО – 12 часов

Защита рефератов по темам:

1. Деятельность правоохранительных органов, осуществляющих прием, регистрацию и разрешение сообщений о преступлениях в сфере компьютерной информации и высоких технологий.

2. Типичные следственные ситуации и планирование расследования преступлений

3. Возмещение вреда, причиненного преступлениями против собственности.

4. Новые методики исследования объектов, собранных в ходе расследования преступлений против собственности.

Самостоятельная работа обучающихся:

1. Задание: обучающиеся по данной теме по указанию преподавателя изучают вопросы ее актуальности и значимости, спорные и нерешенные проблемы, пути и выходы решения в соответствии с уголовно-процессуальным законодательством Республики Казахстан. По рекомендации преподавателя обучающиеся могут изучить архивные материалы, статистические данные, справки и отчеты, статьи и другие источники. По выборке данного материала обучающиеся составляют справки, отчеты, тезисы к докладу, реферату, статьи и т.д.

2. Форма проведения СРО: обучающиеся под руководством преподавателя обсуждают проблемы, связанные с организационно-

распорядительной деятельностью начальника управления, отдела, отделения. Обсуждение докладов обучающихся, выбравших по данной теме письменную работу.

3. Методические рекомендации к выполнению: при подготовке к занятию необходимо опираться на ранее усвоенные знания и использовать нормативные, теоретико-прикладные источники, а так же учебники и учебные пособия по теме занятия.

Основная литература: 2,3,7. 22, 23, 24, 25, 26, 27.

Дополнительная литература: 24,25,26,30,31,32, 36, 37, 38, 39, 40.

Тема 2. Деятельность следователя по проверке законности и обоснованности повода к началу досудебного расследования в сфере компьютерной информации и высоких технологий

Лекция – 1 час

Цель занятия: выработка профессиональных навыков по принятию процессуальных решений, составлению сопутствующих процессуальных документов; привитие навыков по использованию законодательных и иных нормативных актов в работе с доказательствами; привитие уважительного отношения к закону.

Вопросы лекции:

1. Следственные ситуации первоначального этапа расследования преступлений в сфере высоких информационных технологий в сфере компьютерной информации и высоких технологий.
2. Поводы к началу досудебного расследования в сфере компьютерной информации и высоких технологий?

Тезисы лекции:

Одна из особенностей преступлений в сфере высоких информационных технологий, как нами уже было отмечено, заключается в том, что они чрезвычайно латентны (около 90 %). Это связано с тем, что после совершения компьютерного преступления потерпевший обычно не выказывает особой заинтересованности в поимке преступника, а сам преступник, будучи пойман, всячески рекламирует свою деятельность (но это проявляется не во всех случаях). Возможные причины подобного поведения — жертва компьютерного преступления, как правило, совершенно убеждена, что затраты на его раскрытие (включая потери, понесенные в результате утраты, например, банком своей репутации) существенно превосходят уже причиненный ущерб, а сам преступник в результате огласки приобретает широкую известность в деловых и криминальных кругах.

Между тем раскрывать преступления, совершаемые в сфере высоких информационных технологий, сложно, т. к. нередко преступники прибегают к различным уловкам, маскируют свои преступные деяния многочисленными

объективными и субъективными причинами, которые действительно могут иметь место.

Как уже установлено, что определение основных направлений расследования и особенности тактики отдельных следственных действий зависят от характера исходных данных. Под исходной следственной ситуацией понимается объективно сложившаяся в первый период расследования его информационная среда, обстановка проведения и другие условия расследования, от которых зависит тактика и последовательность проведения первоначальных следственных действий, оперативно-розыскных и организационных мероприятий. По делам рассматриваемой категории можно выделить следующие исходные следственные ситуации:

1.Информация о причинах возникновения общественно опасных деяний, способе их совершения и личности правонарушителя отсутствует.

2.Имеются сведения о причинах возникновения преступления, способе его совершения, но нет сведений о личности преступника.

3.Известны причины возникновения преступления, способы его совершения и сокрытия, личность преступника и другие обстоятельства.

В первых двух следственных ситуациях обычно планируются и осуществляются следующие первоначальные следственные действия, оперативно розыскные и организационные мероприятия: допрос заявителя или лиц, на которых указано в исходной информации как на возможных свидетелей; решение вопроса о возможности задержания преступника с поличным и о необходимых в связи с этим мероприятиях; вызов необходимых специалистов для участия в осмотре места происшествия; осмотр места происшествия; проведение оперативно-розыскных мероприятий в целях установления причин совершения преступления, выявления лиц, виновных в его совершении, обнаружения следов и других вещественных доказательств; выемка и последующий осмотр средств электронно – вычислительной техники, предметов, материалов и документов (в т.ч. находящихся в электронной форме на машинных носителях информации), характеризующих производственную операцию, в ходе которой по имеющимся данным совершены преступные действия; допросы свидетелей (очевидцев); допросы подозреваемых (свидетелей), ответственных за данный участок работы, конкретную производственную операцию и защиту конфиденциальной информации; обыски на рабочих местах и по месту проживания подозреваемых; назначение программно-технической, радиотехнической, технической, бухгалтерской и иных экспертиз; дальнейшие действия, которые планируются с учетом дополнительной информации.

Для третьей следственной ситуации может быть предложена следующая программа расследования и действий следователя на первоначальном этапе:

- изучение поступивших материалов с позиций их полноты, соблюдения норм уголовно-процессуального законодательства и порядка

передачи в органы следствия. При необходимости принятие мер к получению недостающей информации;

-начало досудебного расследования;

-вызов необходимых специалистов для участия в осмотре места происшествия;

-осмотр места происшествия;

-личные обыски задержанных, их рабочих мест и места проживания;

-допрос подозреваемых;

-выемка и осмотр вещественных и письменных доказательств;

-изъятие и осмотр подлинных документов, удостоверяющих личность задержанных, а также документов, характеризующих те производственные операции, в процессе которых допущены нарушения и преступные действия (в т. ч. и тех документов, которые находятся в электронной форме на машинных носителях информации);

-допрос лиц, названных в документах, переданных в следственные органы, как допустивших нарушения, ответственных за работу (де нежные средства, материальные ценности, услуги и т. п.) по фактам установленных нарушений;

-истребование, а при необходимости производство выемки нормативных актов и документов, характеризующих порядок и организацию работы в данном подразделении (в т. ч. с конфиденциальной информацией, бланками строгой отчетности, использование СВТ ит. п.);

-допрос свидетелей, причастных к соответствующим производственным операциям или подозреваемых в связях с лицами, совершившими преступные действия;

-анализ полученной информации и решение вопроса о необходимости назначения экспертиз, проведения ревизии или проверки, в т. ч. повторной (по каким позициям, за какой период и с участием каких специалистов).

При выполнении вышеуказанных программ следует учитывать особенности методики расследования конкретного вида преступления, о совершении которого выдвинуты версии. Учитывая конкретные обстоятельства, следователем могут быть выдвинуты и проверены следующие общие версии:

1.Преступление совершено сотрудником данного учреждения либо лицом, имеющим свободный доступ к компьютерной технике.

2.Преступление совершено сторонним лицом, входящим в круг родственников, друзей, знакомых сотрудников учреждений.

3.Преступление совершено группой лиц по предварительному сговору или организованной группой с участием сотрудника данного учреждения либо лица, имеющего свободный доступ к компьютерной технике и в совершенстве владеющего навыками работы с ней.

4.Преступление совершено лицом или группой лиц, не связанных с деятельностью учреждения и не представляющих ценность компьютерной информации.

5.Преступление действительно имело место при тех обстоятельствах, которые вытекают из первичных материалов.

6.Ложное заявление о преступлении.

Приведенный перечень следственных версий является общим, и в зависимости от конкретной ситуации может быть расширен. При этом типичными частными версиями являются версии: о личности преступника (преступников); о способах совершения преступления; об обстоятельствах, при которых было совершено преступление; о размерах ущерба, причиненного преступлением.

Так, рассматривая главу 7 УК РК, можно отметить, что данная норма фактически предусматривает ответственность за совершение трех составов преступлений: неправомерный доступ к охраняемой законом компьютерной информации; создание, использование и распространение вредоносных программ для ПК; нарушение правил эксплуатации ПК, системы ПК или их сети. Рассмотрим особенности расследования данных преступлений более подробно.

Данную необходимость обуславливает дефицит криминалистических рекомендаций по методике и тактике расследования указанных составов преступлений, в связи с чем, представляется обоснованным предложить методические рекомендации и схемы расследования указанных преступлений, которые будет выглядеть следующим образом.

1. Первоначальный этап расследования неправомерного доступа к охраняемой законом компьютерной информации.

Признаками совершения указанного состава могут являться:

-появление в компьютере фальшивых или искаженных данных;

-не обновление в течение длительного времени в автоматизированной информационной системе кодов, паролей и других защитных средств;

-частые сбои в процессе работы компьютеров;

-участившиеся жалобы клиентов компьютерной системы или сети;

-осуществление сверхурочных работ без видимых на то причин;

-немотивированные отказы некоторых сотрудников, обслуживающих компьютерные системы или сети, от отпусков;

-неожиданное приобретение сотрудником домашнего дорогостоящего компьютера;

-чистые дискеты либо диски, принесенные на работу сотрудниками компьютерной системы под сомнительными предлогами;

-участившиеся случаи перезаписи отдельных данных без серьезных на то причин;

-чрезмерный интерес отдельных сотрудников к содержанию чужих распечаток (листингов), выходящих из принтеров.

При наличии указанных признаков либо иного сигнала о совершенном преступлении следует установить:

1.Факт неправомерного доступа к компьютерной информации.

2.Место несанкционированного проникновения в компьютерную систему или сеть.

3.Время несанкционированного доступа.

4.Надежность средств защиты компьютерной информации.

5.Способ совершения несанкционированного доступа.

6. Круг лиц, совершивших неправомерный доступ

7. Виновность и мотивы лиц, совершивших неправомерный доступ к компьютерной информации.

8.Наличие последствий преступления.

9.Наличие обстоятельств, способствовавших преступлению.

2. Первоначальный этап расследования создания, использования распространения вредоносных программ для ПК.

Признаков совершения данных преступлений нет. Как правило, обнаружить можно лишь их результаты — сбои в процессе работы компьютерной системы или сети, жалобы клиентов и т. п.

При расследовании создания вредоносных программ для ПК подлежат установлению следующие обстоятельства:

-факт создания вредоносной программы для ПК;

-способ создания вредоносной программы;

-факт использования и распространения вирусной программы;

-предназначение вредоносной программы и механизм действия;

-место, время создания, используемое для этого программное обеспечение и компьютерная техника;

-круг лиц, виновных в создании, использовании и распространении вирусных программ для ПК;

-цель и мотив создания программы;

-осведомленность лица, использовавшего программу, о ее вредоносных свойствах, наличие или отсутствие умысла на использование и распространение данной программы;

-характер и размер вреда, причиненного данным преступлением;

-наличие обстоятельств, способствовавших совершению расследуемого преступления.

Вредоносная программа, как правило, обнаруживается в момент, когда уже явно проявляются последствия ее применения. Вместе с тем она может быть обнаружена и на машинных носителях информации, в частности, путем изучения информации обложки компакт-диска. Кроме того, выявляется она также в процессе антивирусной проверки, производимой пользователем компьютерной системы перед началом работы на компьютере, особенно часто практикуемой при использовании чужих машинных носителей или получении электронной почты.

Наибольшую сложность для расследования представляет совершение преступления в условиях неочевидности. Здесь основными направлениями расследования должны быть:

- пресечение противоправной деятельности;

- выяснение механизма преступления и уточнение отдельных его обстоятельств;

- установление лица, распространяющего вредоносную программу;

- получение сведений о личности потерпевших;

- установление суммы материального ущерба;

-сбор доказательств о причастности установленного лица к каждым выявленным эпизодам преступной деятельности;

-выяснение причин и условий, способствовавших совершению преступления;

- получение характеризующего личность подозреваемого материала.

Наиболее распространенными условиями, способствовавшими совершению данного преступления, являются: использование не сертифицированного программного обеспечения; использование нелегальных копий программ для ПК; отсутствие резервных копий программ и системных файлов; отсутствие учета и контроля за доступом к компьютерным системам- использование компьютеров не по назначению (для компьютерных игр обучения посторонних, написания программ лицами, в обязанности которых это не входит); нерегулярное проведение антивирусной проверки компьютерной системы и машинных носителей, и др.

3. Первоначальный этап расследования нарушения правил эксплуатации ПК, системы ПК или их сети.

При расследовании нарушения правил эксплуатации ПК, системы ПК или их сети подлежат установлению следующие обстоятельства:

1) факт преступного нарушения правил эксплуатации ПК, системы ПК или их сети;

2) место и время совершения преступления;

3) характер информации, являющейся предметом посягательства;

4) способ и механизм нарушения правил эксплуатации ПК, системы ПК или их сети;

5) характер и размер ущерба, причиненного преступлением;

6) виновность лица;

7) обстоятельства, способствовавшие совершению преступления.

Наиболее распространенными поводами к началу досудебного расследования по указанным составам преступлений являются: сообщения должностных лиц организаций или их объединений (40%); заявления граждан (35%); непосредственное обнаружение органом дознания, следователем или прокурором сведений, указывающих на признаки преступления (20%); сообщения в средствах массовой информации и иные поводы (5 %).

По оценкам ведущих зарубежных и отечественных специалистов 90 % компьютерных преступлений остаются необнаруженными или о них не сообщается в правоохранительные органы по различным причинам.

Список рекомендованной литературы

1, 3, 5, 6, 7, 8, 13, 20, 21, 22,26, 32, 33.

Тема 2. Деятельность следователя по проверке законности и обоснованности повода к началу досудебного расследования в сфере компьютерной информации и высоких технологий

Лекция – 1 час

Цель занятия: выработка профессиональных навыков по принятию процессуальных решений, составлению сопутствующих процессуальных документов; привитие навыков по использованию законодательных и иных нормативных актов в работе с доказательствами; привитие уважительного отношения к закону.

Вопросы лекции:

1. Особенности проведения отдельных следственных действий на первоначальном этапе расследования преступлений в сфере высоких информационных технологий

Тезисы лекции:

Общее изучение сущности рассматриваемого вопроса предполагает анализ следующих следственных действий, чье проведение характерно для первоначального этапа расследования по делам о преступлениях, совершенных в сфере высоких информационных технологий:

По мнению Э. Мелик, целями следственных действий при расследовании данного вида преступлений могут являться:

- осмотр и изъятие компьютерной техники;
- поиск и изъятие информации и следов воздействия на нее непосредственно на носителях информации ПК и ее устройствах;
- поиск и изъятие информации и следов воздействия на нее вне ПК.

Полагаем, что указанные цели усекают перечень следственных действий, производство которых возможно при расследовании преступлений в сфере высоких информационных технологий, проводимых с целью установления обстоятельств, имеющих значение для дела. На этот счет думается, что необходимо расширить перечень указанных целей и дополнить их, где: целями следственных действий, проводимых при расследовании и раскрытии преступлений в сфере высоких информационных технологий, являются: установление и уточнение обстоятельств, происшедшего события (способ, место, время, личность совершившего преступное посягательство и пр.); выявление, фиксация, изъятие и оценка следов преступления (как традиционных криминалистических, так и нетрадиционных - информационных следов преступлений в сфере высоких технологий), различных вещественных доказательств; получение информации, необходимой для построения и проверки следственных версий и осуществления розыскной работы по делу; поиск и изъятие информации и следов воздействия на нее непосредственно на носителях информации ПК и ее устройствах; поиск и изъятие информации и

следов воздействия на нес вне ПК; обнаружение предметов и объектов преступлений; осмотр и изъятие компьютерной техники; установление лиц, способствующих совершению преступления; определение принадлежности компьютерной информации; проверка и оценка следственных версий; установление причин и условий, способствовавших совершению преступления; получение новых доказательств.

Таким образом, приступая к непосредственному исследованию особенностей проведения отдельных следственных действий при расследовании преступлении в сфере высоких информационных технологий (исходя из указанных целей), мы выделяем следующие виды следственных действий, чье рассмотрение будет осуществлено далее: осмотр (включая несколько его разновидностей), обыск и выемка, допрос, следственный эксперимент, предъявление для опознания, назначение экспертиз.

По своей сути, все перечисленные действия могут быть проведены как на первоначальном этапе расследования преступлений в сфере высоких информационных технологий, так и на последующем. Данный факт определяется конкретными условиями расследования преступления. Вместе с тем, исследование сущности установления события преступления и лица его совершившего свидетельствует о том, что успешность проведения перечисленных действий и определяет достижение задач, направленных на быстрое и полное раскрытие преступления, изобличение и привлечение к уголовной ответственности лиц, его совершивших.

Рассматривая следственные действия, производство которых осуществляется при расследовании преступлений указанной категории, еще раз отметим, что проводятся они в строгом соответствии с правилами, регламентированными действующим уголовно-процессуальным законодательством, но с учетом некоторых особенностей.

Следственный осмотр — это следственное действие, состоящее в непосредственном восприятии, анализе и фиксации следователем или лицом, проводящим дознание, различных материальных предметов и отдельных их элементов в целях обнаружения следов преступления и других вещественных доказательств, выяснения обстановки происшествия, а также иных обстоятельств, имеющих значение для дела. Цель осмотра места происшествия по делам указанной категории - установление конкретного СВТ, выступающего в качестве предмета и (или) орудия совершения преступления и имеющего следы преступной деятельности. При производстве следственного действия целесообразно использовать тактический прием «от центра - к периферии», где «центром» (отправной точкой осмотра места происшествия) являются СВТ, находящиеся на месте осмотра. Исследование специфики следственного осмотра производится, исходя из этапов его производства: подготовительного, рабочего, заключительного.

1. Подготовительный этап.

В процессе подготовки к проведению этого следственного действия, еще до выезда на место происшествия необходимо решить ряд

организационных вопросов, которые в последующем обеспечат качество проведения осмотра места происшествия.

Рассматриваемое следственное действие должно быть заблаговременно подготовлено и детально спланировано, необходимо предварительно провести следующую работу: с учетом сложившейся следственной ситуации, наметить круг лиц, участвующих в осмотре; определить последовательность действия лиц при осмотре места происшествия; пригласить соответствующих квалифицированных специалистов; подготовить соответствующую компьютерную технику и программное обеспечение, которые будут использоваться для считывания и хранения изъятой информации, при обнаружении изменений в компьютерной информации, исследовании полученной информации, обнаружении информационных следов преступления; перед началом осмотра разъяснить цели проведения следственного действия и задачи, стоящие перед специалистами, а также их права и обязанности; провести подбор и инструктаж понятых, в качестве которых целесообразнее привлекать лиц, обладающих минимально необходимыми знаниями в области СВТ и компьютерных технологий, разъяснить их права и обязанности.

2. Рабочий этап.

Прежде чем приступить к осмотру, следователь и участники следственно-оперативной группы должны знать и соблюдать общие правила обращения с вычислительной техникой и носителями информации. Несоблюдение этих правил может привести к потере важной для расследования информации и нанесению материального ущерба, вызванного этими действиями.

Общими правилами обращения с вычислительной техникой и носителями информации являются: все включения (выключения) компьютеров и других технических средств производятся только специалистом или под его руководством; применение средств криминалистической техники - магнитных искателей, ультрафиолетового осветителя, инфракрасного преобразователя, во избежание разрушения носителей информации и микросхем памяти ПК, должно быть согласовано со специалистом; необходимо исключить попадания мелких частиц и порошков на рабочие части компьютеров (разъемы, дисковод, вентилятор и др.); при работе с магнитными носителями информации запрещается прикасаться руками к рабочей поверхности дисков, подвергать их электромагнитному воздействию, сгибать диски, хранить без специальных конвертов (пакетов, коробок); диапазон допустимых температур при хранении и транспортировке должен варьироваться в температурных пределах от 0 до + 50 граду сов Цельсия; со всеми непонятными вопросами, затрагивающими терминологию, устройство и функционирование вычислительной техники необходимо обращаться только к специалисту.

На рабочей (исследовательской) стадии осмотра места происшествия каждый объект подлежит тщательному обследованию. В этот период времени важно установить - не содержится ли на компьютере информация,

которая может способствовать более плодотворному и целенаправленному осмотру (различные планы помещений, участков местности, пароли, коды доступа, шифры и т. п.). Для этого специалистом проводится экспресс-анализ компьютерной информации путем просмотра содержимого дисков. Интерес могут представлять файлы с текстовой или графической информацией. Следует обращать внимание не только на наличие (отсутствие) физических повреждений компьютерной техники, магнитных носителей и т. п., но и на состояние окон, дверей и запорных устройств на них.

3. Заключительный этап.

Изъятие средств компьютерной техники производится только в выключенном состоянии. При этом должны быть выполнены и отражены в протоколе следующие действия;

- установлено включенное состояние оборудования и зафиксирован порядок его отключения;

- описано точное местонахождение изымаемых предметов и их расположение относительно друг друга и окружающих предметов (с приложением необходимых схем и планов);

- описан порядок соединения между собой всех устройств с указанием особенностей соединения (цвет, количество, размеры, характерные индивидуальные признаки соединительных проводов, кабелей, шлейфов, разъемов, штекеров и их спецификация); - определено отсутствие либо наличие компьютерной сети, используемый канал (каналы) связи и телекоммуникаций. В последнем случае установлен тип связи, используемая аппаратура, абонентский номер, позывной либо рабочая частота;

- произведено разъединение (с соблюдением всех необходимых мер предосторожности) аппаратных частей (устройств) с одновременным опломбированием их технических входов и выходов;

- определен вид упаковки и транспортировки изъятых предметов.

Транспортировка и хранение компьютерной техники и информации должны осуществляться в условиях, исключающих ее повреждение, в том числе в результате воздействия метало детекторов, используемых для проверки багажа в аэропортах. Хранят компьютеры и их комплектующие в сухом, отапливаемом помещении. Следует удостовериться, что в нем нет грызунов, которые часто являются причиной неисправности аппаратуры. Учитывая нестандартность обстановки, в которой может производиться осмотр места происшествия, вопрос о возможности изъятия компьютерной техники и информации, способе упаковки, транспортировки и хранении изъятых объектов решается следователем в каждом конкретно случае совместно со специалистом. Процессуальный порядок изъятия объектов определяется общими требованиями Уголовно-процессуального кодекса.

Осмотр средств вычислительной техники (СВТ), участвовавших в преступлении, производят для достижения следующих целей:

- обнаружения следов, образовавшихся в результате происшествия или совершения преступления, и других вещественных доказательств для

установления, кем, с какой целью и при каких обстоятельствах было совершено преступление;

- выяснения обстановки происшествия для восстановления механизма совершения преступления;

- установления технического состояния СВТ.

Обыск, выемка.

Обыск - следственное действие, в процессе которого производится поиск и принудительное изъятие объектов, имеющих значение для правильного решения задач уголовного судопроизводства. Выемка — следственное действие, в процессе которого производится изъятие объектов, имеющих значение для правильного решения задач уголовного судопроизводства, в тех случаях, когда их местонахождение точно известно следователю.

Задачами обыска при расследовании преступлений в сфере высоких информационных технологий являются отыскание и изъятие:

1) орудий, используемых для совершения преступления в сфере компьютерной информации, в том числе носителей информации, примененных для копирования похищенной информации или содержащие программы «взлома» защиты компьютера, вредоносные программы, иные программы и файлы данных (например, библиотеки паролей и имен), использованные при совершении преступления;

2) компьютерной информации;

3) специальной литературы, посвященной вопросам компьютерной безопасности, эксплуатации ПК, создания вредоносных программ, неправомерного доступа к компьютерной информации, принципов и алгоритмов организации компьютерных сетей, программного обеспечения и пр.;

4) иных вещественных доказательств и документов, имеющих значение для дела;

5) разыскиваемого лица.

При производстве выемки следует придерживаться рассмотренных нами рекомендаций по осмотру, обыску с учетом процессуальной процедуры производства данного следственного действия.

Допрос. Допрос подозреваемого. При допросе лица в качестве подозреваемого в каждом конкретном случае, как минимум, необходимо получить ответы на следующие вопросы: «Где и кем (в какой должности) работал подозреваемый; к какой компьютерной информации имеет доступ; какие операции с информацией он имеет право проводить; какова его категория доступа к информации; умеет ли работать подозреваемый на компьютере, владеет ли он определенным программным обеспечением, каков уровень его квалификации; кто научил его работать с конкретным программным обеспечением; какие идентификационные коды и пароли закреплены за ним (в том числе при работе в компьютерной сети); к каким видам программного обеспечения имеет доступ подозреваемый; каков источник его происхождения; обнаруживались ли программы, источник

происхождения которых неизвестен; какие виды операций с компьютерной информацией данное лицо выполняло в исследуемое время; из какого источника или от кого конкретно подозреваемый узнал о содержании информации, к которой произвел неправомерный доступ; какой способ использовал подозреваемый для совершения неправомерного доступа к компьютерной информации; как подозреваемому удалось проникнуть в компьютерную систему (сеть); откуда подозреваемый мог узнать пароль (код) доступа к информации».

При установлении факта сбоев в работе средств компьютерной техники и устройств защиты информации в период работы данного лица в определенное время возможна постановка следующих вопросов: «Обнаруживал ли он сбои в работе программ, компьютерные вирусы и другие нарушения в нормальном функционировании программного обеспечения; обнаруживал ли подозреваемый случаи незаконного проникновения в свой компьютер, незаконного подключения к компьютерной сети; имеет ли он ограничения на допуск в помещения, где установлена компьютерная техника и какие именно; ознакомлен ли он с порядком работы с информацией, инструкциями о порядке проведения работ; не было ли случаев нарушения подозреваемым распорядка дня, порядка проведения работ, порядка доступа к компьютерной информации; не поступало ли к подозреваемому от других лиц предложений о передаче какой-либо компьютерной информации, программного обеспечения; неизвестны ли ему лица, проявлявшие интерес к получению идентификационных кодов и паролей».

Круг вопросов, подлежащих выяснению у подозреваемого, определяется конкретной следственной ситуацией, сложившейся по уголовному делу:

- при допросе подозреваемого в совершении создания вредоносных программ для ПК требуется установить уровень его профессиональной подготовленности как программиста, опыт работы по созданию программ конкретного класса на данном языке программирования, знание алгоритмов работы программ, подвергшихся воздействию;

- при расследовании преступлений, связанных с распространением вредоносных программ, особенно компьютерных вирусов, требуется выяснить: соблюдались ли требования противовирусной защиты, каков уровень владения соответствующими программами, каким образом был нарушен режим использования программных средств.

Кроме этого, необходимо установить конкретные факты несоблюдения режима доступа на объект, доступа к средствам вычислительной техники и программным средствам, способы преодоления программных и аппаратных средств защиты информации и другие обстоятельства, способные облегчить совершение преступления.

При допросе подозреваемого требуется выяснить все обстоятельства подготовки и совершения преступления, алгоритм функционирования

вредоносной программы, а также на какую информацию и как она воздействует, характер наступающих последствий, связанных с нарушением работы ПК, их системы или сети и несанкционированным уничтожением, блокированием, модификацией или копированием информации и какие действия по их преодолению могут быть наиболее эффективны.

В ходе допросов свидетелей выясняются следующие обстоятельства:

- на какой рабочей станции могли быть нарушены правила эксплуатации компьютерной сети и где она расположена;
- могли ли быть нарушены правила эксплуатации данной локальной сети на рабочей станции, расположенной в определенном месте (если нарушение правил произошло непосредственно на файловом сервере, то место нарушения этих правил может совпадать с местом наступления вредных последствий).

Основная литература: 2,3,7. 22, 23, 24, 25, 26, 27.
Дополнительная литература: 24,25,26,30,31,32.

Тема 2. Деятельность следователя по проверке законности и обоснованности повода к началу досудебного расследования в сфере компьютерной информации и высоких технологий

Семинар – 1 час

Цель занятия: выработка профессиональных навыков по принятию процессуальных решений, составлению сопутствующих процессуальных документов; привитие навыков по использованию законодательных и иных нормативных актов в работе с доказательствами; привитие уважительного отношения к закону.

Вопросы занятия:

1. Следственные ситуации первоначального этапа расследования преступлений в сфере высоких информационных технологий в сфере компьютерной информации и высоких технологий.
2. Поводы к началу досудебного расследования в сфере компьютерной информации и высоких технологий?
3. Особенности проведения отдельных следственных действий на первоначальном этапе расследования преступлений в сфере высоких информационных технологий

Задание: подготовить устный ответ.

Список рекомендованной литературы

1, 3, 6, 13, 17, 19, 20, 21, 22, 26, 34, 37.

Тема 2. Деятельность следователя по проверке законности и обоснованности повода к началу досудебного расследования в сфере компьютерной информации и высоких технологий

Практическое занятие – 1 час

Цель занятия: выработка профессиональных навыков по принятию процессуальных решений, составлению сопутствующих процессуальных документов; привитие навыков по использованию законодательных и иных нормативных актов в работе с доказательствами; привитие уважительного отношения к закону.

Вводная:

Согласно приказу №23 компании «Вымпел-Ком» г.Энск «О приеме работника на работу», Денисов А.Г. был принят на должность специалиста офиса обслуживания и продаж, и приступил к работе с 1 августа 2018г. Для работы в компьютерной программе, обеспечивающей удаленный доступ через программу «1С» к базе данных «Amdocs»,предназначенной для обслуживания абонентов данной компании Денисов А.Г. получил индивидуальный и конфиденциальный логин и пароль, составляющие его служебную учетную запись. В соответствии с должностной инструкцией Денисов А.Г. обязан был осуществлять обработку персональных данных физических лиц – абонентов компании «Вымпел-Ком», в том числе сбор, хранение, ввод, использование, изменение и уничтожение обрабатываемых персональных данных; обеспечивать конфиденциальность обрабатываемых персональных данных. Денисов А.Г. испытывая материальные трудности, действуя из корыстной заинтересованности с целью получения выгоды заинтересованности с целью получения выгоды имущественного характера для себя решил совершить неправомерный доступ к охраняемой компьютерной информации, содержащей персональные данные клиентов компании «ВымпелКом».

Денисов А.Г. был осведомлен о том, что сим-карта, применяемая в средствах мобильной связи в качестве идентификационного модуля абонента, содержит сведения о подключенных к абонентскому номеру услугах и установленных приложениях, в том числе предназначенных для осуществления операций приема, выдачи и перевода денежных средств, в который данный абонентский номер выступает в качестве идентификатора соответствующей учетной записи.

Задание:

1. С учетом полученной информации необходимо дать анализ сложившейся ситуации.
2. Какое процессуальное решение необходимо принять в данной ситуации.

3. Составьте план проведения первоначальных следственных действий и оперативно-розыскных мероприятий.

4. С учетом полученной информации допросить лицо, сообщившее об уголовном правонарушении.

5. С учетом полученной информации составьте план проверочных мероприятий, с целью чего заполните таблицу:

Установленные обстоятельства	Обстоятельства, требующие уточнения и дополнения	Необходимые действия

6. Определите структуру протокола осмотра места происшествия и процессуальный порядок его проведения, составьте протокол осмотра с учетом полученной вводной задания.

7. Составьте протокол осмотра вещественных доказательств (компьютер).

Порядок контроля и оценки знаний:

1. Оценка правильности и содержательности ответов (использование УПК и норм. актов)

2. Оценка активного участия в дискуссии.

3. Качество составленных документов.

4. Качество проведения процессуальных действий.

Выступление с подготовленной презентацией в программе PoverPoint 2003-2007.

Основная литература: 2,3,7.

Дополнительная литература: 24,25,26,30,31,32,33,35,36,37,38,39, 40.

Список рекомендованной литературы

1, 3, 6, 13, 17, 19, 20, 21, 22, 26, 31, 32.

Тема 2. Деятельность следователя по проверке законности и обоснованности повода к началу досудебного расследования в сфере компьютерной информации и высоких технологий

СРО – 12 часов

Методические рекомендации:

4. Изучить основную литературу.
5. Ознакомиться с дополнительной литературой.
6. Законспектировать основные положения нормативных актов, вопросы лекционных занятий и т.д.

Выполнить письменно ситуационные задачи и быть готовым доложить решения по ним.

Материал для самоконтроля

Тестовые задания для самоконтроля (раздаточный материал)

Самостоятельная работа обучающихся

1.Задания: обучающиеся по данной теме по указанию преподавателя изучают вопросы ее актуальности и значимости, спорные и нерешенные проблемы, пути и выходы решения в соответствии с уголовно-процессуальным законодательством Республики Казахстан. По рекомендации преподавателя обучающийся может изучить архивные материалы, статистические данные, справки и отчеты, статьи и другие источники. По выборке данного материала обучающийся составляет справки, отчеты, тезисы к докладу, реферату, статьи и т.д.

2.Форма проведения СРО: обучающиеся под руководством преподавателя обсуждают проблемы, связанные с организационно-распорядительной деятельностью начальника управления, отдела, отделения. Обсуждение докладов обучающихся, выбравших по данной теме письменную работу.

3.Методические рекомендации к выполнению: При подготовке к занятию необходимо опираться на ранее усвоенные знания и использовать нормативные, теоретико-прикладные источники, а так же учебники и учебные пособия по теме занятия.

4. Рекомендуемая литература: теоретические (монографии, учебные пособия, практикумы) и нормативные источники, рекомендованные для подготовки к лекционным и семинарским занятиям.

Список рекомендованной литературы

1, 3, 5, 6, 7, 8, 13, 20, 21, 22,26, 32, 33.

Тема 3. Процессуальный порядок определения статуса подозреваемого, организация и проведение допроса подозреваемого

Лекция – 1 час

Цель занятия: выработка профессиональных навыков по принятию процессуальных решений, составлению сопутствующих процессуальных документов; привитие навыков по использованию законодательных и иных нормативных актов в работе с доказательствами; привитие уважительного отношения к закону.

Вопросы лекции:

1. Особенности проведения допроса подозреваемого на первоначальном этапе расследования преступлений в сфере высоких информационных технологий

Тезисы лекции:

Допрос подозреваемого. При допросе лица в качестве подозреваемого в каждом конкретном случае, как минимум, необходимо получить ответы на

следующие вопросы: «Где и кем (в какой должности) работал подозреваемый; к какой компьютерной информации имеет доступ; какие операции с информацией он имеет право проводить; какова его категория доступа к информации; умеет ли работать подозреваемый на компьютере, владеет ли он определенным программным обеспечением, каков уровень его квалификации; кто научил его работать с конкретным программным обеспечением; какие идентификационные коды и пароли закреплены за ним (в том числе при работе в компьютерной сети); к каким видам программного обеспечения имеет доступ подозреваемый; каков источник его происхождения; обнаруживались ли программы, источник происхождения которых неизвестен; какие виды операций с компьютерной информацией данное лицо выполняло в исследуемое время; из какого источника или от кого конкретно подозреваемый узнал о содержании информации, к которой произвел неправомерный доступ; какой способ использовал подозреваемый для совершения неправомерного доступа к компьютерной информации; как подозреваемому удалось проникнуть в компьютерную систему (сеть); откуда подозреваемый мог узнать пароль (код) доступа к информации».

При установлении факта сбоев в работе средств компьютерной техники и устройств защиты информации в период работы данного лица в определенное время возможна постановка следующих вопросов: «Обнаруживал ли он сбои в работе программ, компьютерные вирусы и другие нарушения в нормальном функционировании программного обеспечения; обнаруживал ли подозреваемый случаи незаконного проникновения в свой компьютер, незаконного подключения к компьютерной сети; имеет ли он ограничения на допуск в помещения, где установлена компьютерная техника и какие именно; ознакомлен ли он с порядком работы с информацией, инструкциями о порядке проведения работ; не было ли случаев нарушения подозреваемым распорядка дня, порядка проведения работ, порядка доступа к компьютерной информации; не поступало ли к подозреваемому от других лиц предложений о передаче какой-либо компьютерной информации, программного обеспечения; неизвестны ли ему лица, проявлявшие интерес к получению идентификационных кодов и паролей».

Следует иметь в виду, что на первом допросе подозреваемый может попытаться объяснить факт неправомерного доступа к компьютерной информации некриминальными причинами (случайностью, стечением определенных обстоятельств, посторонним воздействием и т. п.). Может рассказывать о неправомерном доступе к компьютерной информации, как о факте, который совершился при отсутствии преступного умысла.

Для изобличения таких лиц хорошие результаты дает правильная реализация информации о преступной деятельности этого лица, полученной при проведении оперативно-розыскных мероприятий, а так же предъявление предметов и документов, принадлежащих подозреваемому и использовавшихся для неправомерного доступа к компьютерной информации. Умелое использование указанных сведений оказывает

определенное воздействие на допрашиваемого и позволяет получить правдивые показания на первом допросе.

Для успешного проведения допроса подозреваемого необходимо тщательно изучить все материалы дела, особенности личности подозреваемого, способы совершения преступления, доказательства, указывающие на виновность конкретного лица, и т. п. Ко времени привлечения лица в качестве подозреваемого следствие должно располагать двумя категориями доказательств. В первой из них предусматривается доказывание обстоятельств, свидетельствующих о том, что расследуемое событие (деяние) имело место, во второй — что это деяние совершено привлекаемым к уголовной ответственности лицом, и оно соответствует составу преступления, предусмотренного соответствующей статьей УК.

Как отмечает ряд авторов, допрос подозреваемого является одним из-важнейших, наиболее сложных и зачастую конфликтных следственных действий. Не преследуя цели рассмотрения тактики допроса подозреваемого в целом, отметим, что обвиняемые дают правдивые показания в тех случаях, когда убедятся, что расследованием установлен круг фактических данных. Поэтому обычно наиболее результативны приемы представления допрашиваемым собранных по делу доказательств и подробного изложения обстоятельств преступления без ссылки на источники.

Круг вопросов, подлежащих выяснению у подозреваемого, определяется конкретной следственной ситуацией, сложившейся по уголовному делу:

- при допросе подозреваемого в совершении создания вредоносных программ для ПК требуется установить уровень его профессиональной подготовленности как программиста, опыт работы по созданию программ конкретного класса на данном языке программирования, знание алгоритмов работы программ, подвергшихся воздействию;

- при расследовании преступлений, связанных с распространением вредоносных программ, особенно компьютерных вирусов, требуется выяснить: соблюдались ли требования противовирусной защиты, каков уровень владения соответствующими программами, каким образом был нарушен режим использования программных средств.

Кроме этого, необходимо установить конкретные факты несоблюдения режима доступа на объект, доступа к средствам вычислительной техники и программным средствам, способы преодоления программных и аппаратных средств защиты информации и другие обстоятельства, способные облегчить совершение преступления.

При допросе подозреваемого требуется выяснить все обстоятельства подготовки и совершения преступления, алгоритм функционирования вредоносной программы, а также на какую информацию и как она воздействует, характер наступающих последствий, связанных с нарушением работы ПК, их системы или сети и несанкционированным уничтожением,

блокированием, модификацией или копированием информации и какие действия по их преодолению могут быть наиболее эффективны.

В ходе допросов свидетелей выясняются следующие обстоятельства:

- на какой рабочей станции могли быть нарушены правила эксплуатации компьютерной сети и где она расположена;

- могли ли быть нарушены правила эксплуатации данной локальной сети на рабочей станции, расположенной в определенном месте (если нарушение правил произошло непосредственно на файловом сервере, то место нарушения этих правил может совпадать с местом наступления вредных последствий).

Время нарушения правил можно установить путем допроса свидетелей из числа лиц, участвующих в эксплуатации ПК. При этом могут быть заданы такие вопросы: «Каким образом в данной компьютерной системе фиксируются факты и время отклонения от установленных правил (порядка) эксплуатации ПК?». «Когда могло быть нарушено определенное правило эксплуатации ПК, после которого наступили известные вредные последствия?».

Список рекомендованной литературы

1, 3, 5, 6, 7, 8, 9, 16, 18, 20, 21, 22, 23, 24, 27, 32.

Тема 3. Процессуальный порядок определения статуса подозреваемого, организация и проведение допроса подозреваемого

Семинар – 1 час

Цель занятия: выработка профессиональных навыков по принятию процессуальных решений, составлению сопутствующих процессуальных документов; привитие навыков по использованию законодательных и иных нормативных актов в работе с доказательствами; привитие уважительного отношения к закону.

Вопросы занятия:

9. Понятие, значение допроса подозреваемого по уголовным делам в сфере компьютерной информации и высоких технологий.
10. Формы взаимодействия с допрашиваемым лицом, по ранее составленному плану допроса.
11. Процессуальные правила проведения допроса потерпевшего.
12. Каков порядок удостоверения личности допрашиваемого и порядок разъяснения процессуальных прав и обязанностей.
13. Какова структура и содержание протокола допроса подозреваемого.
14. Каков алгоритм проведения следственного действия допрос: этапы и характеристика?

15. На основании каких данных формируются задачи следственного действия допрос и вопросы, подлежащие выяснению?

16. Каким образом устанавливается психологический контакт с допрашиваемым лицом, и формулируются вопросы?

Задание: подготовить устный ответ.

Список рекомендованной литературы

1, 3, 6, 13, 17, 19, 20, 21, 22, 26, 34, 37.

Методические рекомендации:

1. Изучить основную литературу.
2. Ознакомиться с дополнительной литературой.
3. Законспектировать основные положения нормативных актов, вопросы лекции и т.д.
4. Выполнить письменно ситуационные задачи и быть готовым доложить решения по ним или решить тестовые задания.

Тема 3. Процессуальный порядок определения статуса потерпевшего, организация и проведение допроса потерпевшего

СРОП – 1 час

Вопросы для самоконтроля:

1. Преступления в сфере высоких информационных технологий .
2. Понятие и значение преступления в сфере высоких информационных технологий.
3. Направления преступной деятельности в информационной сфере и их классификация.
4. Основные обстоятельства, подлежащие установлению и доказыванию при расследовании преступлений в сфере высоких информационных технологий.
5. Общие условия производства досудебного расследования преступления в сфере высоких информационных технологий.
6. Правовое регулирование отношений в области компьютерной информации.

Методические рекомендации:

4. Изучить основную литературу.
5. Ознакомиться с дополнительной литературой.
6. Законспектировать основные положения нормативных актов, вопросы лекционных занятий и т.д.

Список рекомендованной литературы

1, 3, 6, 13, 17, 19, 20, 21, 22, 26, 31, 32.

Защита рефератов по темам:

1. Понятие и значение преступления в сфере высоких информационных технологий.

2. Направления преступной деятельности в информационной сфере и их классификация.

Тема 3. Процессуальный порядок определения статуса подозреваемого, организация и проведение допроса подозреваемого.

СРО – 11 часов

Самостоятельная работа обучающихся

1.Задания: обучающиеся по данной теме по указанию преподавателя изучают вопросы ее актуальности и значимости, спорные и нерешенные проблемы, пути и выходы решения в соответствии с уголовно-процессуальным законодательством Республики Казахстан. По рекомендации преподавателя обучающийся может изучить архивные материалы, статистические данные, справки и отчеты, статьи и другие источники. По выборке данного материала обучающийся составляет справки, отчеты, тезисы к докладу, реферату, статьи и т.д.

2.Форма проведения СРО: обучающиеся под руководством преподавателя обсуждают проблемы, связанные с организационно-распорядительной деятельностью начальника управления, отдела, отделения. Обсуждение докладов обучающихся, выбравших по данной теме письменную работу.

3.Методические рекомендации к выполнению: При подготовке к занятию необходимо опираться на ранее усвоенные знания и использовать нормативные, теоретико-прикладные источники, а так же учебники и учебные пособия по теме занятия.

4. Рекомендуемая литература: теоретические (монографии, учебные пособия, практикумы) и нормативные источники, рекомендованные для подготовки к лекционным и семинарским занятиям.

Основная литература: 2,3,7. 22, 23, 24, 25, 26, 27.

Дополнительная литература: 24,25,26,30,31,32.

2.10 Методические рекомендации по изучению дисциплины «Расследование уголовных правонарушений связанных в сфере компьютерной информации и высоких технологий»

При изучении дисциплины «Расследование уголовных правонарушений связанных в сфере компьютерной информации и высоких технологий» обучение проходит по наиболее важным темам как: общая характеристика досудебного расследования в сфере компьютерной информации и высоких технологий, деятельность следователя по проверке законности и обоснованности повода к началу досудебного расследования в сфере компьютерной информации и высоких технологий, процессуальный

порядок определения статуса потерпевшего, организация и проведение допроса потерпевшего и т.д.

Информацию теоретического характера по рассматриваемым темам можно получить на кафедре, воспользовавшись фондом электронных вариантов учебников, монографий, учебно-практических пособий, сборником нормативных актов МВД и Генеральной Прокуратуры Республики Казахстан, Нормативных постановлений Верховного суда Республики Казахстан.

Системное изучение уголовно-процессуального законодательства, а также теоретических основ по дисциплине в рамках подготовки к практическим занятиям способствует закреплению материала, полученного на лекционных занятиях.

Перечень и содержание видов самостоятельной работы по дисциплине:

1. Беглое прочтение (Skit) - прочитать заданный материал согласно программе обучения.

2. Подготовка обзора по теме (Review) - письменно написать краткий литературный обзор на 1-2 стр. по рекомендуемой теме с привлечением дополнительного материала из печати и информационных ресурсов Интернета.

3. Учебные конкретные ситуации - обучающимся предлагается множество простых и сложных ситуаций, по которым предстоит ответить на вопросы или написать свое видение проблемы; наиболее подготовленные обучающиеся могут написать свой кейс.

5. Групповой проект - в группе должно быть не более 4-5 человека, каждая группа должна разработать свой проект; например доклад на международную конференцию.

6. Индивидуальный проект - выполняют наиболее подготовленные обучающиеся по желанию; работа должна отличаться уникальностью, актуальностью темы, исследовательским характером; результаты проекта могут быть доложены на круглом столе, международной конференции.

7. Эссе - этюд, публицистики и др. жанры, дающие предварительное представление или общее представление о чем-либо. Подготовка эссе прививает следующие навыки обучающимся: критически оценивать, использовать в своей работе труды других авторов, вносить исправления в свою работу, готовить проект научной работы. Основной целью эссе является не донести слушателем авторской мысли, а показать его идею, свою собственную позицию.

Формы и содержание самостоятельной работы:

1. Помощь в выполнении домашних заданий:

- проверка и помощь в написании реферата, доклада, выбранного по списку или выданного преподавателем;

- помощь в составлении структурно-логических схем дисциплины;

- помощь в подготовке обзоров по проблемам основных институтов изучаемой дисциплины.

2. Обсуждение и проверка подготовленных курсантами материалов:

- ознакомление с литературным обзором по теме, выполненным успевающими курсантами;

- проверка того, как курсанты готовятся к презентации докладов по темам.

3. Проверка конспектов тетрадей, выполнения домашних заданий.

4. Проведение контроля знаний курсантов.

5. Выставление оценок по выполненным заданиям.

6. Индивидуальные консультации для пропустивших и неуспевающих обучающихся.

Курсант должен обладать важнейшими общеучебными способами работы:

I. Умения и навыки планирования учебной деятельности:

• осознание учебной задачи;

• постановка целей;

• выбор рационального и оптимального пути их достижения;

•определение последовательности и продолжительности этапов деятельности;

• построение модели (алгоритма) деятельности;

• планирование самостоятельной работы на уроке и дома;

• планирование на день, неделю, месяц.

II. Умения и навыки организации своей учебной деятельности:

• организация рабочего места - наличие и состояние учебных средств, их рациональное размещение, создание благоприятных гигиенических условий;

• организация режима работы;

• организация домашней самостоятельной работы;

• определение порядка и способов умственных действий.

III. Умения и навыки восприятия информации, работа с различными источниками информации (коммуникативные):

• чтение, работа с книгой, конспектирование;

• библиографический поиск, работа со справочниками, словарями;

• слушание речи, запись прослушанного;

• внимательное восприятие информации, управление вниманием;

• наблюдение;

• запоминание.

Особую группу образуют умения и навыки работы с компьютером, в том числе:

- работа в Интернете;

- работа с электронным учебником;

- работа с обучающей программой;

- работа с контролирующей программой;

- работа в условиях дистанционного обучения;

- телеконференции по электронной почте (off-line) или в оперативном режиме (on-line);

- электронные доски объявлений;

- электронные библиотеки.

- доступ к базам данных через электронную почту (off-line) или в оперативном режиме (on-line),

- телевидеоконференции.

Обучающиеся должны уметь самостоятельно работать с литературой учебного и специального характера, находить интересующие их проблемы и уметь их раскрывать.

2.11 Методические рекомендации по подготовке реферата

Основные требования к написанию рефератов. Структура реферата определяется целью и задачами исследования. Работа должна выполняться на основе сочетания хронологического и проблемного принципов, состоять из введения, двух или трех глав, заключения и списка использованных источников. Объем в зависимости от сложности и изученности темы, составляет 10-15 машинописных страниц. В итоге реферат должен представлять собой завершенный самостоятельный труд автора по выбранной теме с необходимыми выводами и рекомендациями.

Содержание рефератов. Реферат, как было указано выше, имеет свою структуру, которая устанавливается исходя из темы и проблемы ее исследования. Сложилась определенная система в написании.

Так, во введении надо дать краткое описание, обоснование основных вопросов темы, которые автор намерен изучить и раскрыть. Во введении обосновываются актуальность темы, степень ее разработанности и теоретическая и правовая базы работы, формулируются цель и задачи исследования, излагаются новизна, практическая значимость работы. Введение отражает современное обоснование решаемых автором вопросов, видение автором путей их исследования и новизну.

В основной части реферата – это, как правило, два или три раздела (глав) в которых содержатся основные положения и данные, отражающие сущность и решение выполненной самостоятельной работы обучающегося. В этой части реферата содержание можно разделить на пункты и параграфы, каждый из которых должен иметь законченную информацию по конкретно поставленному вопросу. В целом содержание работы должно отражать всю совокупность проделанного научного анализа и обобщение событий и фактов, дипломатических или других, имеющих к исследуемой теме отношение законодательных, нормативных актов, инструктивных положений и литературных источников. Широкая документальная база и полнота объема литературы, по теме исследования обеспечат высокое качество и обоснованность в выводе заключения.

В заключении – подводятся итоги проделанной работы, краткие выводы и полученные результаты, рекомендации и практические предложения.

В конце следует привести список использованных источников.

Реферат должен носить самостоятельный характер. Допускается использование источников лишь в форме цитат с указанием автора,

наименования работы, года, места издания и страницы. Избегайте простого переписывания в текст реферата материала рекомендованных учебных и специальных изданий, ибо это дает право рецензенту на отрицательное заключение (незачет). Лучший способ пройти этап контрольного задания - создать свой вариант исполнения, что обеспечивает гарантию успеха и оставит прочные знания по курсу.

Оформление рефератов. Реферат может быть набран на компьютере 14-м шрифтом с соблюдением общепринятых требований. При наборе текста надо соблюдать следующие параметры оставления полей: левое - 30 мм, правое - 10 мм, верхнее - 20 мм, нижнее - 20 мм. Нумерация сквозная в правом нижнем углу (все страницы, включая схемы, диаграммы, приложения нумеруются по порядку). Рекомендуется следующий порядок размещения:

- титульный лист;
- содержание;
- введение;
- разделы (главы) реферата;
- заключение;
- список использованных источников;
- приложения.

При необходимости графики и таблицы могут сопровождаться с пояснительными текстами и указаниями на источники и литературы, из которых использованы необходимые данные.

Если в тексте используются цитаты, цифровая и иная информация, то надо дать соответствующие библиографические сноски. Сноски концевые (в конце текстовой части реферата по мере их использования).

Составление списка (перечня) использованных источников и литературы, других научных работ рекомендуется осуществлять соответственно библиографическому описанию документа. В случае если использованы материалы с Интернета, то необходимо привести официальное название сайта.

Рекомендуется следующая последовательность самостоятельной работы над литературой:

1) ознакомление с учебной программой по курсу «Расследование уголовных правонарушений связанных в сфере компьютерной информации и высоких технологий»;

2) освоение настоящих «Методических указаний...»;

3) проработка рекомендуемой литературы.

Этот примерный алгоритм действий целесообразно применять при изучении каждой темы курса.

Самостоятельная работа обучающегося является составной частью учебного процесса и имеет большое значение в подготовке высококвалифицированных специалистов для органов внутренних дел, т.к. от усвоения материала и подготовки домашнего задания в часы самоподготовки зависит в целом уровень подготовленности слушателя. Изучение дисциплины «Расследование уголовных правонарушений связанных в сфере

компьютерной информации и высоких технологий» не только на семинарских и практических занятиях, но и в часы самоподготовки, призвано завершить становление будущего специалиста, способного после окончания учебного заведения, в условиях минимальной адаптации, находясь на различных должностях, самостоятельно выполнять поставленные перед ним задачи.

В ходе занятий обучающиеся приобретают навыки составления процессуальных документов и деловых бумаг следователя, приобретают первоначальные навыки и умения расследования уголовных дел, тогда как в часы самоподготовки обучающиеся учатся анализировать ситуацию, принимать самостоятельно решения и составлять процессуальные документы расследования, которые должны отвечать требованиям закона, как по форме, так и по содержанию. И только на занятиях преподаватель определяет и оценивает уровень подготовленности к занятиям, насколько обучающийся усвоил пройденный материал и самостоятельно выполнил учебное задание в часы самоподготовки.

2.12 Тестовые задания для самоконтроля

1. В соответствии с Уголовно-процессуальным кодексом, началом досудебного расследования является:
а) постановление о возбуждении уголовного дела;
б) регистрация заявления, сообщения об уголовном правонарушении в Едином реестре досудебных расследований;
в) постановление о привлечении в качестве обвиняемого;
г) задержание подозреваемого;
д) первое неотложное следственное действие.

2. Поводами к началу досудебного расследования являются:
а) сообщения в СМИ или рапорт должностного лица;
б) заявление физического лица либо сообщение должностного лица об уголовном правонарушении;
в) наличие достаточных данных, указывающих на признаки уголовного правонарушения;
г) явка с повинной;
д) постановление о начале досудебного расследования.

3. При наличии в поступившем заявлении, сообщении сведений о признаках административного правонарушения либо дисциплинарного проступка, что должен осуществить орган уголовного преследования?
а) зарегистрировать такое сообщение и начать расследование ничего не предпринимать;
б) обращение в течение трех суток передать сопроводительным письмом в соответствующий уполномоченный государственный орган или должностному лицу;

в) внести представление в соответствующий уполномоченный орган или должностному лицу о привлечении лица к административной или дисциплинарной ответственности;
г) передать по подследственности в территориальный орган.

4. Возможно ли производство осмотра без участия понятых, с использованием научно-технических средств?
а) нет, это запрещено уголовно-процессуальным законом;
б) нет, это запрещено указанием Генерального прокурора РК;
в) да, кроме случаев осмотра жилого помещения;
г) нет, участие понятых обязательно во всех случаях;
д) да, если понятые не желают принимать участие в следственном действии.

5. На какой срок применяется мера процессуального принуждения - доставление:
а) 1 час;
б) 2 часа;
в) 3 часа;
г) 24 часа;
д) 12 часов.

6. Кем определяется порядок ведения Единого реестра досудебных расследований?
а) районным прокурором;
б) районным судьей;
в) Министром внутренних дел;
г) Генеральным Прокурором;
д) начальником Департамента внутренних дел.

7. В чем, состоит запрет на приближение:
а) в ограничении подозреваемого, обвиняемого, подсудимого разыскивать, преследовать, посещать потерпевших и иных лиц, участвующих в деле, в целях их защиты;
б) вести телефонные переговоры, общаться иными способами с потерпевшим и иными лицами, участвующими в деле, в целях их защиты;
в) участковый инспектор выносит мотивированное постановление о запрете на приближение;
г) в ограждении потерпевшего следователем от последующих угроз;
д) в ограничении доступа к сведениям о защищаемом лице.

8. В каких случаях назначается комплексная экспертиза?
а) если следователь сомневается в заключение эксперта;
б) для установления обстоятельства, имеющего значение для дела, где требуется различные познания;
в) если следователь планирует присутствовать при производстве экспертизы;

г) если для заключения необходимы исследования на основе различных отраслей знаний;
д) в случае расследования особо тяжкого преступления.

9. Вся информация о преступлениях и происшествиях (согласно Приказа ГП РК №89 от 19.09.2014 г.), в зависимости от ее содержания подразделяется на:
а) заявления, сообщения, сведения в средствах массовой информации;
б) заявления, сообщения, жалобы, обращения и непосредственные усмотрения органа уголовного преследования;
в) заявления, сообщения, телефонные звонки, оповещения охранной сигнализации;
г) заявления, сообщения и информация об уголовных правонарушениях в электронном формате;
д) сообщения и заявления в электронном формате.

10. В каких случаях лицо не может быть задержано по подозрению в совершении уголовного правонарушения?
а) если оно застигнуто при совершении преступления или непосредственно после его совершения;
б) если очевидцы, в том числе и потерпевшие, прямо укажут на данное лицо как на совершившее преступление;
в) если потерпевший в показаниях указывает на большую вероятность совершения преступления конкретным лицом;
г) если на подозреваемом или в его жилище обнаружены явные следы преступления;
д) если имеются данные, указывающие на то, что лицо совершило административное правонарушение.

11. Какие предметы не признаются вещественными доказательствами?
а) предметы, которые служили орудиями преступления;
б) предметы, которые сохранили на себе следы преступления;
в) предметы, которые были объектами преступных действий подозреваемого;
г) предметы личной гигиены;
д) предметы первой необходимости.

12. В каких случаях лицо признается подозреваемым?
а) с момента начала досудебного расследования;
б) с момента вынесения постановления о признании в качестве подозреваемого;
в) с момента совершения уголовного правонарушения;
г) с момента задержания в порядке ст. 131 УПК РК;
д) с момента вынесения постановления о квалификации деяния подозреваемого.

13. Какое условие не является основанием для признания протокола не допустимым в качестве доказательства?
а) составление протокола ненадлежащим субъектом;
б) нарушение порядка предусмотренного УПК РК;
в) наличие технических ошибок (описок, исправлений и т.п.) не ставящих под сомнение достоверность и законность следственного действия;
г) несоответствие времени производства следственного действия указанного в протоколе фактическому его содержанию;
д) наличие орфографических ошибок.

14. Какое лицо признается потерпевшим?
а) которому непосредственно уголовным правонарушением причинен моральный, физический или имущественный вред;
б) обращения в правоохранительные органы с заявлением о преступлении;
в) которому нанесен вред деянием, совершенным невменяемым;
г) в отношение которого вынесено соответствующее постановление;
д) если задержаны лица, совершившие преступление.

15. В каких случаях разрешается проверка обращения без регистрации в КУИ?
а) когда имеется реальная возможность примирить заявителя с нарушителем без регистрации обращения;
б) когда имеется возможность повлиять на нарушителя оперативными силами и средствами;
в) в случае отсутствия судебной перспективы материала;
г) когда очевидна невозможность раскрытия преступления;
д) проверка обращения без регистрации в КУИ запрещается.

16. В случае отсутствия доступа к информационной системе ЕРДР каким образом производится регистрация заявлений и сообщений?
а) путем обращения в центр обслуживания населения;
б) путем обращения в районный акимат;
в) путем регистрации на электронных носителях;
г) составляется рапорт должностного лица;
д) путем регистрации в бумажном журнале учета регистрации досудебных расследований в случае аварийных ситуаций.

17. Какое решение не может принять следователь в случае обращения заявителя с информацией об уголовном правонарушении?
а) о начале досудебного расследования;
б) о прерывании сроков досудебного расследования;
в) о передаче заявления или сообщения по подследственности;
г) о проведении неотложного следственного действия;
д) о прекращении расследования.

18. Какие условия предусмотрены для избрания меры пресечения «личное поручительство»?
а) письменное ходатайство обвиняемого;
б) дееспособность лица, в отношении которого применяется мера пресечения;
в) письменное ходатайство поручителей;
г) ходатайство близких родственников обвиняемого;
д) согласие лица, в отношении которого применяется мера пресечения.

19. Какие фактические данные не могут служить основанием для применения меры пресечения?
а) о том, что подозреваемый скроется от дознания, предварительного следствия или суда;
б) о том, что подозреваемый воспрепятствует установлению истины по делу;
в) о том, что подозреваемый не имеет постоянного места работы;
г) о том, что подозреваемый будет заниматься преступной деятельностью;
д) о том, что подозреваемый совершил уголовное правонарушение.

20. Что понимается под обнаружением доказательств?
а) изъятие предметов у физических и юридических лиц;
б) запечатление доказательств при помощи научно-технических средств;
в) действия по выявлению и сохранению сведений об обстоятельствах уголовного правонарушения;
г) результаты досмотра и личного обыска;
д) изъятие предметов из внутренней полости человека.

21. С какого момента объект (предмет) признается вещественным доказательством по уголовному делу?
а) с момента его обнаружения в процессе следственного действия;
б) с момента определения его относимости к уголовному делу;
в) с момента его приобщения к уголовному делу соответствующим постановлением;
г) с момента составления обвинительного акта;
д) с момента вынесения постановления о квалификации деяния подозреваемого.

22. Какие обстоятельства не могут быть предметом допроса свидетеля?
а) обстоятельства, которые предшествовали совершению уголовного правонарушения;
б) обстоятельства, характеризующие личность подозреваемого;
в) обстоятельства, уличающие близких родственников в совершении уголовного правонарушения;
г) обстоятельства, которые свидетель воспринимал лично;
д) обстоятельства, изобличающие дающего показания в совершении уголовного правонарушения.

23. Предметом залога может быть:
а) имущество, отчуждение которого не допускается вследствие прямого указания на это в законодательных актах;
б) требования, неразрывно связанные с личностью кредиторов, в частности, требования об алиментах, возмещение вреда жизни и здоровью;
в) любое имущество, в том числе и имущественные права (требования);
г) личные неимущественные блага и права за исключением случаев, установленных законодательными актами;
д) имущество учреждений, которое им передано на праве оперативного управления.

24. С какой целью производится осмотр места происшествия?
а) сбора максимального объема проверочного материала;
б) установления обстоятельств, имеющих значение для дела;
в) задержания преступника;
г) с целью обнаружения и выявления следов уголовного правонарушения, вещественных доказательства и иных материальных объектов, выяснения обстановки происшествия и установления обстоятельств, имеющих значение для дела;
д) составления протокола осмотра места происшествия.

25. Какие условия являются основанием для признания протокола не допустимым в качестве доказательства?
а) составление протокола ненадлежащим субъектом;
б) нарушение порядка предусмотренного УПК РК;
в) наличие технических ошибок (описок, исправлений и т.п.) не ставящих под сомнение достоверность и законность следственного действия;
г) несоответствие времени производства следственного действия указанного в протоколе фактическому его содержанию;
д) протокол не подписан участниками процессуального действия.

26. Какие цели задержания предусмотрены законом?
а) пресечение уголовного правонарушения;
б) изоляция преступника от общества;
в) для обеспечения производства по уголовному проступку;
г) предотвращение возможности общения подозреваемого с соучастниками;
д) разрешение вопроса о применении меры пресечения в виде «содержание под стражей».

27. Какой признак не характеризует предмет как вещественное доказательство?
а) предмет изъят с места происшествия;
б) предмет служил орудием уголовного правонарушения;
в) предмет сохранил на себе следы уголовного правонарушения;

г) предмет явился объектом преступных действий;
д) ценности, нажитые преступным путем.

28. Какие меры процессуального принуждения можно применить к свидетелю при его неявке к следователю?
а) избрать меру пресечения;
б) осуществить привод;
в) отобрать обязательство о явке;
г) наложить штраф;
д) начать в отношении свидетеля досудебное расследование.

29. Какие права разъясняются лицу должностным лицом органа уголовного преследования при задержании его по подозрению в совершении уголовного правонарушения?
а) право на приглашение защитника, право хранить молчание и то, что сказанное им может быть использовано против него в суде;
б) право на обжалование действий и решений органа уголовного преследования и суда;
в) право на обращение к прокурору;
г) право на встречу с независимым экспертом по правам человека;
д) право на приглашение следственного судьи.

30. В каких целях применяются иные меры процессуального принуждения?
а) в целях предупреждения девиантного поведения отдельных участников;
б) в целях обеспечения предусмотренного УПК РК порядка расследования;
в) в целях обеспечения бесконфликтного хода расследования уголовного дела;
г) в профилактических целях;
д) в целях безопасности участников уголовного процесса.

2.13 Критерии оценки знаний обучающихся:

Оценка знаний обучающихся проводится в течение всего семестра в результате проведения текущего, рейтингового и итогового видов контроля, оцениваемых в процентном содержании.

Текущий контроль – систематическая проверка знаний обучающихся по отдельным вопросам и темам, осуществляется в рамках семинарских занятий и СРОП в виде устных и тестовых опросов, оценки выполненных заданий по СРО и СРОП.

Рейтинговый контроль – проверка учебных достижений обучающихся по завершённым темам, разделам программы, проводимая в виде коллоквиумов и тестовых опросов.

Семестровый рейтинг определяется по сумме текущего и рейтингового контролей и максимально составляет 60%. В течение семестра проводится две аттестации. Итоговый контроль (экзамен) по дисциплине проводится в форме компьютерного тестирования.

Итоговая оценка по дисциплине выставляется по сумме баллов семестрового рейтинга и баллов, полученных на экзамене. Знания, умения и навыки обучающихся оцениваются по следующей системе:

Оценка по буквенной системе	Цифровой эквивалент баллов	Процентное содержание	Оценка по традиционной системе
A	4,0	95-100	Отлично
A-	3,67	90-94	Хорошо
B+	3,33	85-89	
B	3,0	80-84	
B-	2,67	75-79	
C+	2,33	70-74	удовлетворительно
C	2,0	65-69	
C-	1,67	60-64	
D-	1,33	55-59	
D	1,0	50-54	
F	0	0-49	неудовлетворительно

«A», «A-» («отлично») - если обучающийся глубоко и прочно усвоил весь программный материал, исчерпывающе, последовательно, грамотно и логически стройно его излагает, не затрудняется с ответом при видоизменении задания, свободно справляется с поставленными задачами, показывает знания монографического материала, правильно обосновывает принятые решения, владеет разносторонними навыками и приемами выполнения практических работ, обнаруживает умение самостоятельно обобщать и излагать материал, не допуская ошибок;

«B+», «B», «B-» («хорошо») - если обучающийся твердо знает программный материал, грамотно и по существу излагает его, не допускает существенных неточностей в ответе на вопрос, может правильно применить теоретические положения и владеет необходимыми навыками при выполнении практических задач;

«C+», «C», «C-» («удовлетворительно») - если обучающийся усвоил только основной материал, но не знает отдельных деталей, допускает неточности;

«D+», «D» («удовлетворительно») - если обучающийся усвоил только основной материал допускает недостаточно правильные формулировки, нарушает последовательность в изложении программного материала и испытывает затруднения в выполнении практических заданий;

«F» («неудовлетворительно») - если обучающийся не знает значительной части программного материала 0%-30%;

если обучающийся допускает существенные ошибки 30%-40%;

если обучающийся не знает значительной части программного материала с большим затруднением выполняет практические работы 40%-49%.

Выбор оценки в амплитуде колебаний от A- до A, от B- до B+, от D до C+ определяется степенью соответствия знаний и умений обучающегося вышеописанным критериям.

2.14 Экзаменационные вопросы по дисциплине

57. Развитие уголовно-процессуального законодательства в свете Концепции правовой политики Республики Казахстан на период с 2010 до 2020г.
58. Процесс доказывания в разрезе Послания Президента Республики Казахстан-Лидера нации Нурсултана Назарбаева народу Казахстана «Стратегия «Казахстан-2050»: новый политический курс состоявшегося государства»
59. Теоретические основы медиации в уголовном процессе.
60. Теоретические основы производства негласных следственных действий.
61. Теоретические основы института реабилитации и возмещения вреда, причинённого незаконными действиями органа, ведущего уголовный процесс.
62. Практическая реализация ускоренного досудебного расследования.
63. Суд присяжных заседателей. История, развитие и его место в свете Концепции правовой политики Республики Казахстан на период с 2010 до 2020г.г.
64. Теоретические основы привлечения юридических лиц к уголовной ответственности: уголовно-процессуальные аспекты.
65. Упрощённые производства в досудебном производстве и судебных стадиях. Соотношение современного развития в разрезе Концепции правовой политики Республики Казахстан на период с 2010 до 2020г.г.
66. Несоответствия современного развития отдельных уголовно-процессуальных институтов в разрезе Концепции правовой политики Республики Казахстан на период с 2010 до 2020г.г.
67. Теоретические модели современного уголовного процесса Казахстана.
68. Процессуальный статус следователя на современном этапе.
69. Теория судебных доказательств. Понятие, виды и современное состояние. (на основе анализа нового УПК РК от 04.07.2014г)
70. Понятие доказательств. Источники доказательств.
71. Научные классификации мер процессуального принуждения.
72. Казахстанская классификация мер процессуального принуждения.
73. Процессуальная форма. Единство и дифференциация процессуальной формы.
74. Соблюдение прав человека и гражданина при избрании мер процессуального принуждения.

75. Использование электронных средств слежения при избрании мер процессуального принуждения. (на опыте стран СНГ и дальнего зарубежья, современного состояния в Республике Казахстан)

76. Теоретические проблемы применения мер процессуального принуждения.

77. Процессуальные особенности участия медиатора в уголовном процессе.

78. Понятие и виды процессуальных документов составляемых в ходе досудебного расследования преступлений в сфере компьютерной информации и высоких технологий.

79. Поводы к началу досудебного расследования преступлений в сфере компьютерной информации и высоких технологий.

80. Правила приема, регистрации заявлений и сообщений об уголовных правонарушениях, а также ведения ЕРДР

81. Понятие и виды следственных действий в досудебном расследовании преступлений в сфере компьютерной информации и высоких технологий.

82. Общие процессуальные правила производства следственных действий по УПК РК по преступлениям в сфере компьютерной информации и высоких технологий

83. Алгоритм проведения следственных действий: этапы и характеристика.

84. Понятие и сущность следственного осмотра по преступлениям в сфере компьютерной информации и высоких технологий Организационная деятельность следователя при производстве следственного осмотра.

85. Участники следственного осмотра и их процессуальное положение.

86. Действия следователя (дознавателя) на подготовительном этапе осмотра места происшествия.

87. Этапы осмотра места происшествия по преступлениям в сфере компьютерной информации и высоких технологий.

88. Порядок взаимодействия участников следственно-оперативной группы при производстве осмотра места происшествия.

89. Порядок обнаружения и изъятия следов преступления и иных материальных объектов при производстве осмотра места происшествия.

90. Деятельность следователя по организации проведения допроса по преступлениям в сфере компьютерной информации и высоких технологий.

91. Процессуальное закрепление результатов допроса участников по преступлениям в сфере компьютерной информации и высоких технологий.

92. Понятие, значение, порядок допроса. Процессуальный порядок допроса по преступлениям в сфере компьютерной информации и высоких технологий.

93. Решение организационных вопросов при назначении судебных экспертиз по преступлениям в сфере компьютерной информации и высоких технологий.

94. Использование судебных экспертиз в качестве доказательств по уголовному делу по преступлениям в сфере компьютерной информации и высоких технологий.

95. Собирание, проверка, исследование и оценка вещественных доказательств по преступлениям в сфере компьютерной информации и высоких технологий

96. Основания задержания подозреваемого по преступлениям в сфере компьютерной информации и высоких технологий.

97. Меры пресечения: понятие, классификация и основания для избрания.

98. Процессуальный порядок окончания расследования по преступлениям в сфере компьютерной информации и высоких технологий.

99. Может ли осмотр места происшествия производить дознаватель?

100. Возможно ли производство осмотра без участия понятых, с использованием технических средств фиксации хода и результатов?

101. Каков срок досудебного расследования?

102. Досудебное производство – это производство по делу с начала досудебного расследования до направления?

103. При задержании лица по подозрению в совершении преступления изымаются ли следователем ценности и деньги, находящиеся при задержанном, если они не являются вещественными доказательствами по делу?

104. Какие объекты не могут быть признаны вещественными доказательствами по уголовным делам?

105. Сколько понятых (минимальное число) может присутствовать при производстве следственных действий при отсутствии научно-технических средств?

106. С какого момента предмет считается вещественным доказательством по уголовному делу?

107. Какая из указанных категорий лиц не подлежит дактилоскопическому учету в Комитете по правовой статистике и специальным учетам Генеральной прокуратуры РК?

108. Обязательно ли для органа дознания поручение следователя в связи с производством по уголовному делу?

109. Вправе ли следователь заниматься оперативно-розыскной деятельностью по расследуемому делу?

110. Кем определяется порядок ведения Единого реестра досудебных расследований?

2.15 Составитель: доцент кафедры досудебного расследования преступлений, майор полиции Кемпирова Ж.С.

ТЕМАТИКА ПИСЬМЕННЫХ РАБОТ ПО ДИСЦИПЛИНЕ И МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ИХ ВЫПОЛНЕНИЮ

1. Понятие и виды процессуальных документов составляемых в ходе досудебного расследования преступлений **в сфере компьютерной информации** и высоких технологий.
2. Поводы к началу досудебного расследования преступлений **в сфере компьютерной информации** и высоких технологий.
3. Правила приема, регистрации заявлений и сообщений об уголовных правонарушениях, а также ведения ЕРДР
4. Понятие и виды следственных действий в досудебном расследовании преступлений **в сфере компьютерной информации** и высоких технологий.
5. Общие процессуальные правила производства следственных действий по УПК РК по преступлениям **в сфере компьютерной информации** и высоких технологий
6. Алгоритм проведения следственных действий: этапы и характеристика.
7. Понятие и сущность следственного осмотра по преступлениям **в сфере компьютерной информации** и высоких технологий Организационная деятельность следователя при производстве следственного осмотра.
8. Участники следственного осмотра и их процессуальное положение.
9. Действия следователя (дознавателя) на подготовительном этапе осмотра места происшествия.
10. Этапы осмотра места происшествия по преступлениям **в сфере компьютерной информации** и высоких технологий.
11. Порядок взаимодействия участников следственно-оперативной группы при производстве осмотра места происшествия.
12. Порядок обнаружения и изъятия следов преступления и иных материальных объектов при производстве осмотра места происшествия.
13. Деятельность следователя по организации проведения допроса по преступлениям **в сфере компьютерной информации** и высоких технологий.
14. Процессуальное закрепление результатов допроса участников по преступлениям **в сфере компьютерной информации** и высоких технологий.
15. Понятие, значение, порядок допроса. Процессуальный порядок допроса по преступлениям **в сфере компьютерной информации** и высоких технологий.
16. Решение организационных вопросов при назначении судебных экспертиз по преступлениям **в сфере компьютерной информации** и высоких технологий.
17. Использование судебных экспертиз в качестве доказательств по уголовному делу по преступлениям **в сфере компьютерной информации** и высоких технологий.
18. Собирание, проверка, исследование и оценка вещественных доказательств по преступлениям **в сфере компьютерной информации** и высоких технологий
19. Основания задержания подозреваемого по преступлениям **в сфере компьютерной информации** и высоких технологий.
20. Меры пресечения: понятие, классификация и основания для избрания.
21. Процессуальный порядок окончания расследования по преступлениям **в сфере компьютерной информации** и высоких технологий.

МВД РЕСПУБЛИКИ КАЗАХСТАН
КАРАГАНДИНСКАЯ АКАДЕМИЯ МВД РК им. Б.БЕЙСЕНОВА
ЮРИДИЧЕСКИЙ ИНСТИТУТ

КАФЕДРА ДОСУДЕБНОГО РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

к выполнению письменных работ
по дисциплине RUPSSKIVT 4315
«Расследование уголовных правонарушений, связанных
в сфере компьютерной информации и высоких технологий»

Специальность: 5В030300 Правоохранительная деятельность

Караганда 2018

Рассмотрены и рекомендованы к утверждению на заседании кафедры досудебного расследования преступлений

протокол №___ от «___» _____ 20__ г.

Рассмотрен на заседании кафедры досудебного расследования преступлений «__» _____ 2018 г., Протокол №____

Начальник кафедры досудебного
расследования преступлений
к.ю.н., полковник полиции Калиев А. К.

Утверждены на заседании УМС «__» _____ 2018 г. Протокол №____

Составитель: доцент кафедры досудебного расследования преступлений, майор полиции Кемпирова Ж.С.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Особую роль в процессе повышения качества высшего образования играет организация самостоятельной работы обучающихся. Развитие навыков самостоятельной работы – одна из современных тенденций высшего образования, которая связана со многими факторами, начиная от необходимости развития творческих способностей личности, ее компетенций, и заканчивая скоростью увеличения объема научной информации в современном мире.

В рамках данного процесса важен методический компонент, который предоставляет обучающемуся необходимые инструменты, рекомендации, правила и алгоритмы действий, как для самостоятельного исследования учебных вопросов, так и надлежащего им выполнения индивидуальных письменных работ.

Одной из основных форм самостоятельной работы обучающихся является выполнение ими письменных работ. Поэтому неотъемлемым элементом учебно-методического обеспечения учебного процесса являются методические указания к выполнению письменных работ по изучаемым дисциплинам. Которые дают обучающимся (и, прежде всего, обучающимся заочных форм обучения) возможность правильно и квалифицированно подготовить письменную работу, соблюдая при этом все стандарты их оформления.

Данные методические указания к выполнению и подготовке письменных работ по дисциплине «Расследование уголовных правонарушений, связанных в сфере компьютерной информации и высоких технологий» предназначены для обучающихся по специальности: 5В030300 «Правоохранительная деятельность» очной и заочных форм обучения.

В них указываются все необходимые требования, касающиеся:

- организации подготовки и написания письменной работы,
- их содержания и объема;
- порядка их оформления.

Кроме того, методические указания включают:

- указания на цели и задачи выполнения письменной работы;
- информационные материалы для подготовки к выполнению письменных работ.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ К ВЫПОЛНЕНИЮ ПИСЬМЕННЫХ РАБОТ

1. Цели и задачи выполнения письменной работы

Письменную работу по дисциплине «Расследование уголовных правонарушений, связанных в сфере компьютерной информации и высоких технологий» обучающиеся выполняют в соответствии с учебным планом специальности 5В030300 «Правоохранительная деятельность».

Письменная работа является звеном, связующим теоретическую подготовку студента с практикой работы по специальности и представляет собой форму контроля за усвоением программного материала.

Письменная работа должна быть выполнена на основе глубокого изучения действующего законодательства, международных стандартов, научных разработок по теме работы. Выполнение работы требует от обучающегося не только знаний общей и специальной литературы по теме, но и умения проводить аналитические исследования, увязывать вопросы теории с юридической практикой, делать обобщения, выводы и предложения по совершенствованию законодательства, как в целом, так и по отдельным направлениям досудебного расследования.

Общими требованиями письменной работы являются:

- четкость и последовательность изложения материала;
- краткость и ясность формулировок;
- конкретность изложения результатов и выводов.

Целями письменной работы являются:

- закрепление, углубление и проверка теоретических знаний, полученных при изучении дисциплины;

- усвоение элементов её системы, знания закономерностей структуры и механизма преступления, возникновения информации о нём и его участниках, организации, планировании и деятельности по раскрытию, расследованию и предупреждению преступлений;

- выработка системы знаний, умений и навыков по использованию методов, приемов и средств, обеспечения профессиональной деятельности;

- вырабатывание профессионального мышления о расследуемых событиях;

- развитие способности выделения элементов структуры преступления и механизма образования информации её собирания и использования;

- развитие анализа и оценки следственных ситуаций и принятия решений по ним;

- обучение выдвижению версий, выбору форм, методов и направлений тактического воздействия;

- подготовка к грамотному применению в условиях складывающихся следственных ситуаций рекомендаций методики расследования и предупреждения преступлений;

- формирование у обучающегося способности к непрерывному самообразованию и личностной и профессиональной самореализации в сфере профессиональной деятельности.

2. Организация подготовки и написания письменной работы

При выборе темы обучающийся должен руководствоваться примерным перечнем тем письменных работ по дисциплине ежегодно утверждающимся на заседании кафедры. Обучающийся имеет право предложить свою тему обосновав ее целесообразность по согласованию с преподавателем кафедры. Недопустимо выполнение письменной работы на одинаковую тему несколькими обучающимися.

Написание письменной работы осуществляется самостоятельно. Обучающийся уточняет круг вопросов, подлежащих изучению, составляет план письменной работы, определяет структуру работы, сроки выполнения ее этапов, определяет необходимую литературу[1].

Логически обусловленная последовательность выполнения письменной работы может быть следующей:

1. Формирование замысла (осмысление темы, задания).

2. Поиск и отбор материалов (правовых источников, отечественной и зарубежной литературы по теме письменной работы), их изучение, обработка.

При изучении литературы рекомендуется выписывать наиболее важную информацию и фиксировать собственные мысли или критические замечания по ранее изученным материалам. Выписки из литературных источников следует делать в виде цитат, которые берутся в кавычки. После каждой цитаты должна быть ссылка на автора и источник информации с указанием страницы.

3. Группировка и систематизация материалов (составление плана).

4. Теоретическое исследование по теме письменной работы.

5. Практическая часть письменной работы.

6. Написание текста.

7. Оформление письменной работы в соответствии с предъявляемыми требованиями.

Письменная работа должна быть сдана на проверку в соответствии со сроками, установленными графиком учебного процесса. Проверка работы осуществляется преподавателем.

---

[1] Кузнецов, И.Н. Подготовка и оформление рефератов, курсовых и дипломных работ / И.Н. Кузнецов. – Минск: ООО «Сэр-Вит», 2000. – С. 105-106.

3. Структура, содержание и объем письменной работы

Структура письменной работы должна способствовать раскрытию избранной темы и отдельных ее вопросов.

Структурными элементами письменной работы являются:

- титульный лист;
- содержание;
- введение;
- основная часть;
- заключение;
- список использованных источников;
- приложение.

Все части письменной работы должны быть изложены в строгой логической последовательности и взаимосвязи.

Содержание работы рекомендуется иллюстрировать схемами, таблицами, диаграммами, графиками, фотографиями, рисунками и т д.

Объем основной части письменной работы составляет 10-15 страниц печатного текста.

Титульный лист **является первой страницей письменной работы. Номер страницы на титульном листе не проставляют.**

В *содержании* последовательно перечисляют все заголовки письменной работы: введение, номера и заголовки рассматриваемых вопросов, заключение, список использованных источников и приложения с указанием номера страницы, на которой помещен каждый заголовок.

Введение **– вступительная, начальная часть письменной работы. Во введении обосновывается выбор темы, определяется ее актуальность, формулируется проблема и круг вопросов, необходимых для ее решения; определяется цель работы с ее расчленением на взаимосвязанный комплекс задач, подлежащих решению; указывается предмет и объект исследования; описываются используемые методы исследования и литературные источники.**

Общий объем введения не должен превышать 1,5 страницы машинописного текста.

Основная часть **письменной работы делится на разделы. Дальнейшее Разделы должны быть соразмерны, как по структурному делению, так и по объему. Как правило,**

письменная работа содержит 3 раздела. Основная часть письменной работы включает в себя:

- общетеоретический и методологический характер;

- аналитический характер;

- изучение и анализ материала;

- предложения по разработке или дальнейшему совершенствованию конкретных теоретических концепций или частных теорий, отдельных направлений, законодательства регламентирующего уголовно-процессуальную деятельность, её организацию и структуру.

Заключение **составляет 1,5 страницы, в котором логически и последовательно излагаются теоретические и практические выводы и предложения, которые сделал обучающийся в результате исследования. Они должны быть краткими и четкими, дающими полное представление о содержании, значимости, обоснованности и эффективности разработок.**

Тезисная форма их изложения должна отражать основные выводы по теории вопроса, по проведенному анализу и всем предлагаемым направлениям любого из аспектов изученной проблемы с оценкой их эффективности по конкретному объекту исследования.

Все предложения и рекомендации должны носить конкретный характер, позволяющие определить место автора в решении проблемы.

Список использованных источников **должен содержать перечень источников информации, на которые в письменной работе приводятся ссылки. Он должен включать все изученные источники, располагаемые в алфавитном порядке.**

В *приложениях* следует размещать вспомогательный иллюстративный или справочный материал, необходимый для более целостного и полного восприятия письменной работы, оценки ее научной и практической значимости.

К приложениям могут относиться:

- ✓ **рисунки, схемы, графики, материалы правовой статистики;**
- ✓ **тексты различных нормативно-правовых актов и**

служебных документов;

- ✓ **таблицы вспомогательных цифровых данных;**
- ✓ **иллюстрации вспомогательного характера.**

4. Оформление письменной работы

Оформление письменной работы: объем основного текста должен составлять 12-14 страниц, шрифт основного текста Times New Roman, размер шрифта основного текста 14 пт, межстрочный интервал одинарный, отступ первой строки абзаца1,25 см, выравнивание текста по ширине, автоматическая расстановка переносов включена, нумерация страниц внизу посередине, поля слева и справа – по2 см, снизу и сверху – по2,5 см.

На все источники должны присутствовать ссылки в тексте реферата. Литература оформляется в соответствии с требованиями ВАК.

5. Информационные материалы для подготовки письменных работ

1. Андреев, Б.В. Расследование преступлений в сфере компьютерной информации / Б.В. Андреев, П.Н. Пак, В.П. Хорст. – М. : Юрлитинформ, 2001. – 148 с.
2. Астапкин, С.М., Расследование хищений государственного имущества / С.М. Астапкин, Л.П. Дубровицкая. – М., 1990. – 123 с.
3. Баев, О.Я. Тактика следственных действий: учебное пособие /О.Я. Баев. - Воронеж: Изд-во Воронеж, ун-та, 1992. - 205 с.
4. Басецкий, И. И. Организованная преступность: моногр. / И.И. Басецкий, Н.А. Легенченко. - 2-е изд., испр. и доп. - Мн.: Академия МВД Республики Беларусь. 2002. - 551 с.
5. Басецкий, И.И. Коррупция: теория и практика противодействия: моногр., И.И. Басецкий, А.В. Башан: под общ. ред И.И. Басецкого. - Мн.: Акад. МВД Респ. Беларусь,2005. -461 с.
6. Баландюк, В.Н.Экологические преступления / В.Н. Баландюк. – Омск, 1998. – 123 с.
7. Бертовский, Л.В. Выявление и расследование экономических преступлений / Л.В. Бертовский. – М.: Экзамен, 2003. – 255 с.
8. Биленчук, П.Д. Компьютерные преступления: Социально-правовые и криминолого-криминалистические аспекты: Учеб. пособие / П.Д. Биленчук, М.А. Зубань. – Киев : Укр. акад. внутр. дел, 1994. – 71 с.
9. Вехов, В.Б. Расследование компьютерных преступлений в странах СНГ : монография / В.Б.Вехов, В.А.Голубев; под ред. Б.П.Смагоринского. – Волгоград : ВА МВД России, 2004. – 304 с.

10. Вехов, В.Б. Тактические особенности расследования преступлений в сфере компьютерной информации : Науч.-практ. пособие / В.Б.Вехов, В.В.Попова, Д.А.Илюшин. – Самара : [Офорт], 2003. – 184 с.

11. Волеводз, А.Г. Противодействие компьютерным преступлениям/ А.Г.Волеводз. – М. Юрлитинформ, 2002. – 123 с.

12. Волженкин, Б.Е. Преступления в сфере экономической деятельности : (Экономические преступления) / Б.В. Волженкин. – СПб., 2002. – 123 с.

13. Гросс, Г. Руководство для следователей / Г. Грос. - Вып. 1. - Смоленск: Типо-Литовская Ф.В. Зельдовичъ, 1895. - 980 с.

14. Газизов, В.А., Видеозапись и ее использование при раскрытии и расследовании преступлений: учеб. пособие / В.А. Газизов, А.Г. Филиппов. – М.: Щит, 1998. – 283 с.

15. Галахов, С.С. Криминальные взрывы. Основы оперативно–розыскной деятельности по борьбе с преступлениями террористического характера / С.С. Галахов. – М.: Экзамен, 2002. – 288 с.

16. Галезник, М.В. Методика расследования криминальных взрывов: лекция / М.В. Галезник; М-во внутр. дел Респ. Беларусь, Акад. МВД, каф. криминалистики. – Минск: Акад. МВД Респ. Беларусь, 2007. – 39 с.

17. Гурев, М.С. Убийства на «разборках»: методика расследования / М.С. Гурев. – СПб.: Питер, 2001. – 282 с.

18. Дубровин, И.С. ДНК–анализ в международных информационно–поисковых системах // Закон и право (РФ). – 2007. – № 5. – С. 78–79.

19. Еникеев, М.И. Следственные действия: психология, тактика, технология: учеб. пособие / М.И. Еникеев, В.А. Образцов, В.Е. Эминов. - М.: ТК Велби. Изд-во Проспект, 2007. - 216 с.

20. Егоров, В.П. Осмотр места происшествия на железнодорожном транспорте: практ. пособие / В.П. Егоров. – Минск: Молодежное науч. об-во, 2001. – 165 с.

21. Ермолович, В.Ф. Построение и проверка версий / В.Ф. Ермолович, М.В. Ермолович; под ред. И.И. Басецкого. – Минск: Амалфея, 2000. – 176 с.

22. Ерохина, Л.Д. Торговля женщинами в целях сексуальной эксплуатации. Теория и практика борьбы / Л.Д. Ерохина, Ю.М. Буряк. : Владивосток : Изд-во Дальневосточного ун-та, 2001. – 196 с.

23. Женило, В.Р. Компьютерная фоноскопия / В.Р.Женило. – М. : Акад. МВД России, 1995. – 208 с.

24. Ищенко, Е.П. Криминалистика: Учебник / Е.П. Ищенко. А.А. Топорков; под ред. Е.П. Ищенко. - М.: Юридическая фирма «КОНТРАКТ»: ИНФРА-М. 2007. - 748 с.

25. Иванов, Э.А. Отмывание денег и правовое регулирование борьбы с ними / Э.А. Иванов. – М., 1999. – 123 с.

26. Исютин-Федотков, Д.В. Образцы для сравнительного исследования в уголовном процессе и криминалистике: учеб. пособие / Д.В. Исютин-Федотков; под ред. Г.Н.Мухина. – Минск: Акад. МВД Респ. Беларусь, 2005. – 101 с.

27. Калиев А.К., Кондратьев И.В., Хасенов Е.А. Досудебное расследование уголовных правонарушений (убийство). Учебно-практическое

пособие (под общей редакцией д.ю.н., профессора Токубаева З.С.) Караганда 2015 г.

28. Каныгин, В.И. Расследование преступлений против личности и собственности: курс лекций /В.И. Каныгин, А.Ф., Лубин, Д.О. Серебров, С.П. Сереброва. - СПб.: Питер. 2008. - 272 с.

29. Кенжетаев Д.Т., Калиев А.К., Балтабаев Т.Н. Примерные образцы уголовно-процессуальных документов досудебного расследования, Караганда, 2014.

30. Криминалистика: информационные технологии доказывания. Учебник для вузов / А.И. Баянов [и др.]; под ред. В.Я. Колдина. - М.: Зерцало-М. 2007. - 752 с.

31. Кауфман, Л.Д. Преступления в сфере экономической деятельности / Л.Д. Кауфман, С.В. Максимов; – М., 1997. – 123 с.

32. Клейменов, М.П. Деятельность органов внутренних дел по борьбе с вымогательством / М.П.Клейменов, О.В.Дмитриев; – Омск: Ом. высш. шк. МВД Рос. Федерации, 1995 – 123 с.

33. Климова, Е.И. Методика расследования фальшивомонетничества / Е.И. Климова, Мн., 1999. – 123 с.

34. Козлов, В.Е. Компьютерные преступления: криминалистическая характеристика и осмотр места происшествия /В.Е.Козлов. – Минск: Акад. МВД Респ. Беларусь, 2001. – 123 с.

35. Лепёхин, А.Н. Расследование преступлений против информационной безопасности: теоретико-правовые и прикладные аспекты: монография / А.Н. Лепёхин. - Минск: Тесей. 2007.- 176 с.

36. Лавров, В.П. Расследование преступлений по «горячим следам»: Учебное пособие. / В.П. Лавров, В.Е. Сидоров - М., 1989. – 123 с.

37. Лагун, Н.И. Особенности расследования уголовных дел о выманивании кредита и дотаций: учеб. пособие / Н.И. Лагун. – Минск: Акад. МВД Респ. Беларусь, 2005. – 93 с.

38. Лившиц, Е.М. Тактика следственных действий /Е. М. Лившиц, Р.С. Белкин. - М.: Новый Юристь, 1997. - 176 с.

39. Логвин, В.М. Взаимодействие следователей и оперативных работников органов внутренних дел при расследовании преступлений (правовые и организационные аспекты): Монография. / В.М. Логвин, В.П. Шиенок – Мнинск: Академия МВД РБ, 2002. – 223 с.

40. Настольная книга следователя. Тактические приемы проведения осмотра места происшествия и допросов при расследовании преступлений различной категории: научно-методическое пособие /А.И. Дворкин [и др.]; под ред.А.И. Дворкина. - М.: Издательство «Экзамен», 2006. - 637 с.

41. Осмотр места происшествия: Практикум /А.Е. Гучок, И.А. Мороз. - Мн.: БГУ. 2003. -75 с.

42. Осмотр места происшествия по делам о насильственной смерти: пособие для следователей / И.С. Андреев [и др.]; под ред. А.В. Дулова, Н.И. Порубова. - Мн.: НИИПККиСЭ, 1995. - 364 с.

43. Осмотр трупа на месте его обнаружения: практическое руководство /Э.П. Александров [и др.]; под ред. В.А. Матышева. - СПб.: Лань, 1997. - 283 с.

44. Расследование неправомерного доступа к компьютерной информации: науч.-практич. пособие / Н.Г. Шурухнов [и др.]; под ред. Н.Г. Шурухнова. - М.: Щит-М, 1999. - 253 с.

45. Руководство для следователей по ОМП: учебно-практическое пособие / А.В. Головинов, С. И. Данилова, Л.С. Корнева [и др.]: под ред. И.А. Попова, Г.В. Костылевской, Н.Е. Муженской [и др.]. - М.: Проспект. 2011. – 440 с.

46. Толеубекова Б.Х. Компьютерная преступность: вчера, сегодня, завтра. Караганда, 1995.

47. Тяжина А.О., Ногайбаева А.С. Новеллы досудебного расследования по УПК Республики Казахстан. Учебно-практическое пособие (краткий анализ в схемах). Караганда, 2015.

48. Тяжина А.О., Ногайбаева А.С., Бейсенбаев А.Ж. Досудебное производство по уголовным делам: образцы процессуальных документов, Караганда, 2014.

МАТЕРИАЛЫ ПО КОНТРОЛЮ И ОЦЕНКЕ УЧЕБНЫХ ДОСТИЖЕНИЙ ОБУЧАЮЩИХСЯ (ТЕСТОВЫЕ ЗАДАНИЯ ДЛЯ САМОКОНТРОЛЯ, ТЕМАТИКА ПИСЬМЕННЫХ РАБОТ, ПЕРЕЧЕНЬ ЭКЗАМЕНАЦИОННЫХ ВОПРОСОВ И ВОПРОСОВ ДЛЯ РУБЕЖНОГО КОНТРОЛЯ)

ТЕСТОВЫЕ ЗАДАНИЯ ДЛЯ САМОКОНТРОЛЯ:

1. В соответствии с Уголовно-процессуальным кодексом, началом досудебного расследования является:

а) постановление о возбуждении уголовного дела;

б) регистрация заявления, сообщения об уголовном правонарушении в Едином реестре досудебных расследований;

в) постановление о привлечении в качестве обвиняемого;

г) задержание подозреваемого;

д) первое неотложное следственное действие.

2. Поводами к началу досудебного расследования являются:

а) сообщения в СМИ или рапорт должностного лица;

б) заявление физического лица либо сообщение должностного лица об уголовном правонарушении;

в) наличие достаточных данных, указывающих на признаки уголовного правонарушения;

г) явка с повинной;

д) постановление о начале досудебного расследования.

3. При наличии в поступившем заявлении, сообщении сведений о признаках административного правонарушения либо дисциплинарного проступка, что должен осуществить орган уголовного преследования?

а) зарегистрировать такое сообщение и начать расследование ничего не предпринимать;

б) обращение в течение трех суток передать сопроводительным письмом в соответствующий уполномоченный государственный орган или должностному лицу;

в) внести представление в соответствующий уполномоченный орган или должностному лицу о привлечении лица к административной или дисциплинарной ответственности;

г) передать по подследственности в территориальный орган.

4. Возможно ли производство осмотра без участия понятых, с использованием научно-технических средств?

а) нет, это запрещено уголовно-процессуальным законом;

б) нет, это запрещено указанием Генерального прокурора РК;

в) да, кроме случаев осмотра жилого помещения;

г) нет, участие понятых обязательно во всех случаях;

д) да, если понятые не желают принимать участие в следственном действии.

5. На какой срок применяется мера процессуального принуждения - доставление:

а) 1 час;

б) 2 часа;

в) 3 часа;

г) 24 часа;

д) 12 часов.

6. Кем определяется порядок ведения Единого реестра досудебных расследований?

а) районным прокурором;

б) районным судьей;

в) Министром внутренних дел;

г) Генеральным Прокурором;

д) начальником Департамента внутренних дел.

7. В чем, состоит запрет на приближение:

а) в ограничении подозреваемого, обвиняемого, подсудимого разыскивать, преследовать, посещать потерпевших и иных лиц, участвующих в деле, в целях их защиты;

б) вести телефонные переговоры, общаться иными способами с потерпевшим и иными лицами, участвующими в деле, в целях их защиты;

в) участковый инспектор выносит мотивированное постановление о запрете на приближение;

г) в ограждении потерпевшего следователем от последующих угроз;

д) в ограничении доступа к сведениям о защищаемом лице.

8. В каких случаях назначается комплексная экспертиза?

а) если следователь сомневается в заключение эксперта;

б) для установления обстоятельства, имеющего значение для дела, где требуется различные познания;

в) если следователь планирует присутствовать при производстве экспертизы;

г) если для заключения необходимы исследования на основе различных отраслей знаний;

д) в случае расследования особо тяжкого преступления.

9. Вся информация о преступлениях и происшествиях (согласно Приказа ГП РК №89 от 19.09.2014 г.), в зависимости от ее содержания подразделяется на:

а) заявления, сообщения, сведения в средствах массовой информации;

б) заявления, сообщения, жалобы, обращения и непосредственные усмотрения органа уголовного преследования;

в) заявления, сообщения, телефонные звонки, оповещения охранной сигнализации;

г) заявления, сообщения и информация об уголовных правонарушениях в электронном формате;

д) сообщения и заявления в электронном формате.

10. В каких случаях лицо не может быть задержано по подозрению в совершении уголовного правонарушения?

а) если оно застигнуто при совершении преступления или непосредственно после его совершения;

б) если очевидцы, в том числе и потерпевшие, прямо укажут на данное лицо как на совершившее преступление;

в) если потерпевший в показаниях указывает на большую вероятность совершения преступления конкретным лицом;

г) если на подозреваемом или в его жилище обнаружены явные следы преступления;

д) если имеются данные, указывающие на то, что лицо совершило административное правонарушение.

11. Какие предметы не признаются вещественными доказательствами?

а) предметы, которые служили орудиями преступления;

б) предметы, которые сохранили на себе следы преступления;

в) предметы, которые были объектами преступных действий подозреваемого;

г) предметы личной гигиены;

д) предметы первой необходимости.

12. В каких случаях лицо признается подозреваемым?

а) с момента начала досудебного расследования;

б) с момента вынесения постановления о признании в качестве подозреваемого;

в) с момента совершения уголовного правонарушения;

г) с момента задержания в порядке ст. 131 УПК РК;

д) с момента вынесения постановления о квалификации деяния подозреваемого.

13. Какое условие не является основанием для признания протокола не допустимым в качестве доказательства?

а) составление протокола ненадлежащим субъектом;

б) нарушение порядка предусмотренного УПК РК;

в) наличие технических ошибок (описок, исправлений и т.п.) не ставящих под сомнение достоверность и законность следственного действия;

г) несоответствие времени производства следственного действия указанного в протоколе фактическому его содержанию;

д) наличие орфографических ошибок.

14. Какое лицо признается потерпевшим?

а) которому непосредственно уголовным правонарушением причинен моральный, физический или имущественный вред;

б) обращения в правоохранительные органы с заявлением о преступлении;

в) которому нанесен вред деянием, совершенным невменяемым;

г) в отношение которого вынесено соответствующее постановление;

д) если задержаны лица, совершившие преступление.

15. В каких случаях разрешается проверка обращения без регистрации в КУИ?

а) когда имеется реальная возможность примирить заявителя с нарушителем без регистрации обращения;

б) когда имеется возможность повлиять на нарушителя оперативными силами и средствами;

в) в случае отсутствия судебной перспективы материала;

г) когда очевидна невозможность раскрытия преступления;

д) проверка обращения без регистрации в КУИ запрещается.

16. В случае отсутствия доступа к информационной системе ЕРДР каким образом производится регистрация заявлений и сообщений?

а) путем обращения в центр обслуживания населения;

б) путем обращения в районный акимат;

в) путем регистрации на электронных носителях;

г) составляется рапорт должностного лица;

д) путем регистрации в бумажном журнале учета регистрации досудебных расследований в случае аварийных ситуаций.

17. Какое решение не может принять следователь в случае обращения заявителя с информацией об уголовном правонарушении?

а) о начале досудебного расследования;

б) о прерывании сроков досудебного расследования;

в) о передаче заявления или сообщения по подследственности;

г) о проведении неотложного следственного действия;

д) о прекращении расследования.

18. Какие условия предусмотрены для избрания меры пресечения «личное поручительство»?

а) письменное ходатайство обвиняемого;

б) дееспособность лица, в отношении которого применяется мера пресечения;

в) письменное ходатайство поручителей;

г) ходатайство близких родственников обвиняемого;

д) согласие лица, в отношении которого применяется мера пресечения.

19. Какие фактические данные не могут служить основанием для применения меры пресечения?

а) о том, что подозреваемый скроется от дознания, предварительного следствия или суда;

б) о том, что подозреваемый воспрепятствует установлению истины по делу;

в) о том, что подозреваемый не имеет постоянного места работы;

г) о том, что подозреваемый будет заниматься преступной деятельностью;

д) о том, что подозреваемый совершил уголовное правонарушение.

20. Что понимается под обнаружением доказательств?

а) изъятие предметов у физических и юридических лиц;

б) запечатление доказательств при помощи научно-технических средств;

в) действия по выявлению и сохранению сведений об обстоятельствах уголовного правонарушения;

г) результаты досмотра и личного обыска;

д) изъятие предметов из внутренней полости человека.

21. С какого момента объект (предмет) признается вещественным доказательством по уголовному делу?

а) с момента его обнаружения в процессе следственного действия;

б) с момента определения его относимости к уголовному делу;

в) с момента его приобщения к уголовному делу соответствующим постановлением;

г) с момента составления обвинительного акта;

д) с момента вынесения постановления о квалификации деяния подозреваемого.

22. Какие обстоятельства не могут быть предметом допроса свидетеля?

а) обстоятельства, которые предшествовали совершению уголовного правонарушения;

б) обстоятельства, характеризующие личность подозреваемого;

в) обстоятельства, уличающие близких родственников в совершении уголовного правонарушения;

г) обстоятельства, которые свидетель воспринимал лично;

д) обстоятельства, изобличающие дающего показания в совершении уголовного правонарушения.

23. Предметом залога может быть:

а) имущество, отчуждение которого не допускается вследствие прямого указания на это в законодательных актах;

б) требования, неразрывно связанные с личностью кредиторов, в частности, требования об алиментах, возмещение вреда жизни и здоровью;

в) любое имущество, в том числе и имущественные права (требования);

г) личные неимущественные блага и права за исключением случаев, установленных законодательными актами;

д) имущество учреждений, которое им передано на праве оперативного управления.

24. С какой целью производится осмотр места происшествия?

а) сбора максимального объема проверочного материала;

б) установления обстоятельств, имеющих значение для дела;

в) задержания преступника;

г) с целью обнаружения и выявления следов уголовного правонарушения, вещественных доказательства и иных материальных объектов, выяснения обстановки происшествия и установления обстоятельств, имеющих значение для дела;

д) составления протокола осмотра места происшествия.

25. Какие условия являются основанием для признания протокола не допустимым в качестве доказательства?

а) составление протокола ненадлежащим субъектом;

б) нарушение порядка предусмотренного УПК РК;

в) наличие технических ошибок (описок, исправлений и т.п.) не ставящих под сомнение достоверность и законность следственного действия;

г) несоответствие времени производства следственного действия указанного в протоколе фактическому его содержанию;

д) протокол не подписан участниками процессуального действия.

26. Какие цели задержания предусмотрены законом?

а) пресечение уголовного правонарушения;

б) изоляция преступника от общества;

в) для обеспечения производства по уголовному проступку;

г) предотвращение возможности общения подозреваемого с соучастниками;

д) разрешение вопроса о применении меры пресечения в виде «содержание под стражей».

27. Какой признак не характеризует предмет как вещественное доказательство?

а) предмет изъят с места происшествия;

б) предмет служил орудием уголовного правонарушения;

в) предмет сохранил на себе следы уголовного правонарушения;

г) предмет явился объектом преступных действий;

д) ценности, нажитые преступным путем.

28. Какие меры процессуального принуждения можно применить к свидетелю при его неявке к следователю?

а) избрать меру пресечения;

б) осуществить привод;

в) отобрать обязательство о явке;

г) наложить штраф;

д) начать в отношении свидетеля досудебное расследование.

29. Какие права разъясняются лицу должностным лицом органа уголовного преследования при задержании его по подозрению в совершении уголовного правонарушения?

а) право на приглашение защитника, право хранить молчание и то, что сказанное им может быть использовано против него в суде;

б) право на обжалование действий и решений органа уголовного преследования и суда;

в) право на обращение к прокурору;

г) право на встречу с независимым экспертом по правам человека;

д) право на приглашение следственного судьи.

30. В каких целях применяются иные меры процессуального принуждения?

а) в целях предупреждения девиантного поведения отдельных участников;

б) в целях обеспечения предусмотренного УПК РК порядка расследования;

в) в целях обеспечения бесконфликтного хода расследования уголовного дела;

г) в профилактических целях;

д) в целях безопасности участников уголовного процесса.

ТЕМАТИКА ПИСЬМЕННЫХ РАБОТ:

1. Деятельность правоохранительных органов, осуществляющих прием, регистрацию и разрешение сообщений о преступлениях в сфере компьютерной информации и высоких технологий.
2. Зарубежный опыт расследования уголовных правонарушений в сфере компьютерной информации и высоких технологий.
3. Использование достижений науки и техники, в том числе компьютерных технологий, в расследовании преступлений против личности и собственности.
4. Взаимодействие участников расследования преступления – право или обязанность.
5. Взаимодействие правоохранительных органов в борьбе с

преступлениями в сфере компьютерной информации и высоких технологий.

6. Следственная и судебная практика организации и осуществления взаимодействия органов предварительного следствия различных ведомств при расследовании уголовных правонарушений в сфере компьютерной информации и высоких технологий.

7. Заключение эксперта – личное мнение специалиста или коллективный труд.

8. Новые методики исследования объектов, собранных в ходе расследования уголовных правонарушений в сфере компьютерной информации и высоких технологий.

9. Чьи интересы защищает адвокат: клиента или правосудия?

10. Следственная и судебная практика рассмотрения в органах внутренних дел сообщений о причинении тяжкого вреда здоровью.

11. Обеспечение прав и законных интересов лица, задержанного по подозрению в совершении преступления.

12. Можно ли привлечь к уголовной ответственности иностранного гражданина?

13. Следственная и судебная практика производства следственных действий по судебному решению.

14. Рассмотрение ходатайств, заявленных участниками уголовного судопроизводства в ходе досудебного расследования.

15. Обстоятельства, способствующие совершению уголовных правонарушений в сфере компьютерной информации и высоких технологий.

16. Следственная и судебная практика назначения и производства судебных экспертиз по уголовным делам о причинении тяжкого вреда здоровью.

17. Обеспечение прав и законных интересов лица, задержанного по подозрению в совершении преступления.

18. Вещественные доказательства – немые свидетели преступления.

19. Новые методики исследования объектов, собранных в ходе расследования преступлений против половой неприкосновенности.

20. Конкуренция интересов свидетелей по стороны обвинения и свидетелей со стороны защиты.

21. Деятельность правоохранительных органов, осуществляющих прием, регистрацию и разрешение сообщений о преступлениях против собственности.

22. Взаимодействие правоохранительных органов в борьбе с преступлениями против собственности.

23. Возмещение вреда, причиненного преступлениями против собственности.

24. Новые методики исследования объектов, собранных в ходе расследования уголовных правонарушений в сфере компьютерной информации и высоких технологий.

25. Вещественные доказательства – немые свидетели преступления.

26. Использование вещественных доказательств в уголовном и

гражданском судопроизводстве.

27. Использование достижений науки и техники, в том числе компьютерных технологий, в расследовании преступлений против личности и собственности.

28. Общая характеристика убийств.

29. Особенности производства следственных действий при расследовании уголовных правонарушений в сфере компьютерной информации и высоких технологий.

30. Особенности расследования заказных убийств.

31. Особенности расследования убийств, при расчленении трупа.

32. Типичные следственные ситуации при расследовании убийств

33. Общая характеристика уголовного правонарушения причинение вреда здоровью в досудебном расследовании.

34. Особенности проведения следственных действий при расследовании преступления причинение вреда здоровью.

35. Понятие, общий порядок и виды осмотра, при расследовании уголовных дел связанных с причинением вреда здоровью.

36. Тактика допроса свидетелей и потерпевших (допрос в условиях бесконфликтной ситуации), при расследовании уголовных дел связанных с причинением вреда здоровью.

37. Тактика допроса подозреваемых (допрос в условиях конфликтной ситуации), при расследовании уголовных дел связанных с причинением вреда здоровью.

38. Фиксация хода и результатов осмотра.

39. Основания для прекращения уголовного дела, зарегистрированного по факту разбоя.

40. Обвинительный акт и обвинительное заключение – общие и отличительные черты.

41. Стилистика обвинительного заключения о разбое и грабеже.

42. *Общие вопросы расследования мошенничества в досудебном производстве.*

43. *Порядок производство следственных действий при расследовании мошенничества.*

44. *Особенности тактики первоначальных следственных действий.*

45. *Способы совершения и сокрытия мошенничества в отношении физических лиц.*

46. Следственная и судебная практика рассмотрения в органах внутренних дел сообщений о факте вымогательства.

47. Возмещение вреда, причиненного преступлениями против собственности.

48. Понятие, признаки и история развития вымогательства по уголовно-процессуальному праву.

49. Вымогательство в отечественном уголовном законодательстве.

50. Особенности квалификации деяния подозреваемого по делам о вымогательстве.

ПЕРЕЧЕНЬ ЭКЗАМЕНАЦИОННЫХ ВОПРОСОВ И ВОПРОСОВ ДЛЯ РУБЕЖНОГО КОНТРОЛЯ:

1. Понятие и виды процессуальных документов составляемых в ходе досудебного расследования преступлений в сфере компьютерной информации и высоких технологий.
2. Поводы к началу досудебного расследования преступлений в сфере компьютерной информации и высоких технологий.
3. Правила приема, регистрации заявлений и сообщений об уголовных правонарушениях, а также ведения ЕРДР
4. Понятие и виды следственных действий в досудебном расследовании преступлений в сфере компьютерной информации и высоких технологий.
5. Общие процессуальные правила производства следственных действий по УПК РК по преступлениям в сфере компьютерной информации и высоких технологий
6. Алгоритм проведения следственных действий: этапы и характеристика.
7. Понятие и сущность следственного осмотра по преступлениям в сфере компьютерной информации и высоких технологий Организационная деятельность следователя при производстве следственного осмотра.
8. Участники следственного осмотра и их процессуальное положение.
9. Действия следователя (дознавателя) на подготовительном этапе осмотра места происшествия.
10. Этапы осмотра места происшествия по преступлениям в сфере компьютерной информации и высоких технологий.
11. Порядок взаимодействия участников следственно-оперативной группы при производстве осмотра места происшествия.
12. Порядок обнаружения и изъятия следов преступления и иных материальных объектов при производстве осмотра места происшествия.
13. Деятельность следователя по организации проведения допроса по преступлениям в сфере компьютерной информации и высоких технологий.
14. Процессуальное закрепление результатов допроса участников по преступлениям в сфере компьютерной информации и высоких технологий.
15. Понятие, значение, порядок допроса. Процессуальный порядок допроса по преступлениям в сфере компьютерной информации и высоких технологий.
16. Решение организационных вопросов при назначении судебных экспертиз по преступлениям в сфере компьютерной информации и высоких технологий.
17. Использование судебных экспертиз в качестве доказательств по уголовному делу по преступлениям в сфере компьютерной информации и высоких технологий.
18. Собирание, проверка, исследование и оценка вещественных доказательств по преступлениям в сфере компьютерной информации и высоких технологий
19. Основания задержания подозреваемого по преступлениям в сфере компьютерной информации и высоких технологий.

20. Меры пресечения: понятие, классификация и основания для избрания.
21. Процессуальный порядок окончания расследования по преступлениям в сфере компьютерной информации и высоких технологий.
22. Следственная и судебная практика рассмотрения в органах внутренних дел сообщений о причинении тяжкого вреда здоровью.
23. Обеспечение прав и законных интересов лица, задержанного по подозрению в совершении преступления.
24. Можно ли привлечь к уголовной ответственности иностранного гражданина?
25. Следственная и судебная практика производства следственных действий по судебному решению.
26. Рассмотрение ходатайств, заявленных участниками уголовного судопроизводства в ходе досудебного расследования.
27. Обстоятельства, способствующие совершению преступления против личности.
28. Виды следственного осмотра по объему?
29. Виды следственного осмотра по последовательности проведения?
30. На какие стадии подразделяется подготовительный этап осмотра места происшествия?
31. На какие стадии подразделяется рабочий этап осмотра места происшествия?
32. На какие стадии подразделяется рабочий этап осмотра трупа?
33. Действия заключительного этапа осмотра места происшествия?
34. К числу первоначальных следственных действий при расследовании уголовных дел об убийстве в условиях следственной ситуации, характеризующейся обнаружением неопознанного трупа или его частей, относится?
35. Какой из тактических приемов осмотра места происшествия целесообразно применять при обнаружении трупа?
36. Концентрический способ осмотра места происшествия - это осмотр?
37. Освидетельствование – это…?
38. Виды основных способов осмотра места происшествия?
39. Что служит началом досудебного расследования?
40. Каким документом оформляется устное заявление?
41. Явка с повинной – это?
42. Какие существуют формы досудебного расследования?
43. Кто несет ответственность за своевременную доставку специалиста к месту проведения следственного действия и обратно?
44. Каким языком может пользоваться заявитель при обращении в орган уголовного преследования?
45. На каком языке дается ответ о принятом решении по заявлению о преступлении?
46. В какой орган невозможно обращение гражданина с информацией о подготавливаемом преступлении?

47. Какое действие не входит в обязанность органа досудебного расследования после регистрации устной информации о преступлении в КУИ и ЕРДР, если деяние совершено на территории обслуживания другого органа?

48. Сколько раз учитывается преступление при поступлении нескольких заявлений, сообщений, жалоб и иной информации по одному и тому же факту?

49. В случае отсутствия доступа к информационной системе ЕРДР каким образом производится регистрация заявлений и сообщений?

50. Каким документом оформляется изъятие трупа из жилого помещения?

51. Чье участие в наружном осмотре трупа человека на месте его обнаружения является обязательным?

52. Что входит в понятие предмета доказывания по уголовному делу?

53. Что понимается под пределами доказывания по уголовному делу?

54. Что понимается под обнаружением доказательств?

55. Какие действия следователя понимаются как исследование доказательств?

56. В каком случае труп человека при осмотре подлежит обязательному дактилоскопированию?

57. Что понимается под относимостью доказательства при его оценке?

58. Что понимается под допустимостью доказательства при его оценке?

59. Что понимается под достоверностью доказательства по уголовному делу при его оценке?

60. В каком случае после осмотра трупа человека производство судебно-медицинской экспертизы необязательно?

61. В каком случае производится эксгумация трупа из места захоронения?

62. С какого момента объект (предмет) признается вещественным доказательством по уголовному делу?

63. С какой целью производится осмотр места происшествия?

64. Какие условия являются основанием для признания протокола не допустимым в качестве доказательства?

65. Какие следственные действия не вправе производить лицо, осуществляющее досудебное производство при ускоренном досудебном расследовании?

66. Установление, каких обстоятельств возможно без назначения экспертизы?

67. По каким уголовным правонарушениям начальник ОВД обязан выезжать на место происшествия лично?

68. Какой признак не характеризует предмет как вещественное доказательство?

69. В каком случае работник органа дознания обязан провести осмотр места происшествия?

70. Что не охватывается содержанием понятия вреда здоровью?

71. Осмотр производится с целью?

72. Какие сведения не выясняет эксперт для внесения в протокол осмотра трупа в процессе осмотра трупа на месте его обнаружения?

73. Рабочий этап следственного осмотра включает в себя?

74. Может ли следователь, дознаватель одновременно опрашивать несколько лиц, вызванных по одному делу?

75. В случае необходимости производства следственных действий в другом районе, кто вправе их производить?

76. Что не может являться доказательством по уголовному делу?

77. При осуществлении надзора за законностью при расследовании, прокурор не вправе?

78. Какие предварительные суждения не может высказывать эксперт на месте происшествия по окончании наружного осмотра трупа и изучения обстановки?

79. В каких случаях допускается принудительное получение образцов у потерпевшего?

80. Планирование должно осуществляться при соблюдении следующих принципов (укажите неверный вариант) ?

81. Сроки, установленные УПК РК, исчисляются?

82. В каких случаях следователь вправе лично получить образцы?

83. Какие действия с объектами допускаются при производстве экспертизы?

84. На кого не распространяются требования о возможности присутствия при производстве исследований, сопровождающихся обнажением, лица того же пола?

85. Что указывается в постановлениях, выносимых в ходе досудебного расследования?

86. Вправе ли начальник следственного отдела осуществлять досудебное расследование?

87. В каких случаях допускается проведение следственного эксперимента?

88. Изъятые в ходе судопроизводства наркотические средства в опечатанном виде хранятся?

89. Какие из целей не охватывает проверка и уточнение показаний на месте?

90. Какой вид планов не охватывается процессуальной деятельностью дознавателя?

91. Какие фактические данные признаются допустимыми в качестве доказательств?

92. Эксперт – это?

93. Что означает принцип динамичности планирования?

94. Что означает принцип реальности планирования?

95. Какие обстоятельства не подлежат доказыванию по уголовному делу?

96. Что понимается под частной версией?

97. Какая цель не преследуется следователем при составлении плана расследования по конкретному уголовному делу?

98. Какие действия следователя не входят в организацию планирования?

99. По какому принципу специализации структурных подразделений или работников строится деятельность Оперативно-криминалистических подразделений?

100. Что означает принцип публичности?

101. С какой целью организуется дежурство работников Оперативно-криминалистического подразделения в составе следственно-оперативных групп?

102. На каком автотранспорте осуществляется выезд работника Оперативно-криминалистического подразделения на место происшествия и возвращение его к месту службы?

103. Может ли производится следственный эксперимент, если при этом унижается честь и достоинство потерпевшего?

104. Кто несет ответственность за своевременную доставку специалиста к месту проведения следственного действия?

105. Может ли быть привлечен для участия в осмотре места происшествия специалист другого отдела внутренних дел?

106. В каком процессуальном документе необходимо отразить факт применения кинолога с служебной собакой, обнаруживших наркотики на месте происшествия?

107. Вправе ли следователь назначить экспертизу до регистрации уголовного правонарушения в ЕРДР?

108. Допустимо ли в уголовном процессе использование результатов прослушивания телефонных переговоров?

109. Какие предметы не могут являться вещественными доказательствами?

110. Что не может являться доказательствами по уголовному делу?

111. Что не относится к уголовно-процессуальным документам?

112. Иную информацию о преступлениях составляют?

113. Куда сдаются вещественные доказательства подвергающиеся быстрой порче?

114. Каким образом определяется достоверность доказательства?

115. Какое из доказательств может быть признано недопустимым?

116. На должности следователя назначаются лица?

117. Следственные подразделения не подчиняются?

118. Непосредственное руководство и контроль за деятельностью следователей осуществляют?

119. Осмотр вещественных доказательств производится?

120. При осмотре предметов и документов составляется?

121. В каких случаях производится повторный осмотр?

122. В каком случае производится эксгумация трупа из места захоронения?

123. Рабочий этап следственного осмотра включает в себя?

124. С какого момента предмет считается вещественным доказательством по уголовному делу?

125. В каком случае труп человека при осмотре подлежит обязательному фотографированию?

126. С какой целью производится осмотр места убийства?

127. С какой целью производится осмотр места обнаружения трупа?

128. В каком случае работник органа дознания вправе провести осмотр места происшествия?

129. Осмотр производится с целью?

130. В каких случаях при проведении следственных действий обязательно участие понятых?

131. Каким документом оформляется изъятие трупа из жилого помещения?

132. В каком случае, при осмотре трупа человека, участие врача – специалиста в области судебной медицины не обязательно?

133. В каком случае производится эксгумация трупа из места захоронения?

134. Кто не может принимать участия в осмотре места совершения убийства?

135. Какой документ направляется одновременно с трупом в морг?

136. В каком случае производство осмотра возможно без участия понятых?

137. Какое обязательное действие следователя не влечет за собой факт изъятия вещественных доказательств?

МВД РЕСПУБЛИКИ КАЗАХСТАН
КАРАГАНДИНСКАЯ АКАДЕМИЯ МВД РК
им. БАРИМБЕКА БЕЙСЕНОВА
ЮРИДИЧЕСКИЙ ИНСТИТУТ

КАФЕДРА ДОСУДЕБНОГО РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ

ЛЕКЦИЯ

Тема №1 Общая характеристика досудебного расследования в сфере компьютерной информации и высоких технологий

Лекцию подготовил:
доцент кафедры досудебного расследования преступлений Карагандинской академии МВД РК им. Б. Бейсенова
майор полиции Кемпирова Ж.С.

Лекция обсуждена и одобрена на заседании кафедры досудебного расследования преступлений «___» _____ 2018 года Протокол №___.

Караганда – 2018 г.

Тема: Общая характеристика досудебного расследования в сфере компьютерной информации и высоких технологий

Вид занятия: Лекция Время - 1 час.

План лекции:

Введение

1. Понятие и значение преступления в сфере высоких информационных технологий.

2. Направления преступной деятельности в информационной сфере и их классификация.

Заключение

Цели занятия**:**

Методическая - подготовка и чтение лекции, выбор средств, обеспечивающих наглядное и полное усвоение дидактического содержания лекции.

Дидактическая - доведение до курсантов определенного комплекса учебной информации, определенного блока знаний на уровне и в объеме, предусмотренном программой и тематическим планом по вопросам организации и проведения следственных осмотров. Доведение материала с использованием методических и технических средств обучения, которые обеспечивают его усвоение.

Воспитательная - выработка психологической установки на возможность осознания, усвоения воспринимаемых научных знаний и понимания значения их реализации через соответствующие практические умения в будущей деятельности при проведении досудебного расследования.

Литература:

1. Аверьянова Т.В. Задачи компьютерно-технической экспертизы // Информатизация правоохранительных систем: Тезисы докладов междун. конф. В 2-х ч. М., 1998. 4.2.

2. Батурин Ю.М., Жодзишский А.М. Компьютерные правонарушения: криминализация, квалификация, раскрытие // Сов. государство и право, 1990. № 12. С.86-94.

3. Гортинский А.В., Пархоменко А.Н. Некоторые рекомендации по организации и проведению следственных действий при расследовании преступлений, совершенных с использованием печатающих средств персональных компьютеров // Материалы семинара: «Вопросы квалификации и расследования некоторых преступлений в сфере экономики». Саратов, 1998. 15-18 дек. С. 184-187.

4. КЕНЖЕТАЕВ Д.Т., КАЛИЕВ А.К., БАЛТАБАЕВ Т.Н. ПРИМЕРНЫЕ ОБРАЗЦЫ УГОЛОВНО-ПРОЦЕССУАЛЬНЫХ ДОКУМЕНТОВ ДОСУДЕБНОГО РАССЛЕДОВАНИЯ, КАРАГАНДА, 2014.

5. КРЫЛОВ В.В. ИНФОРМАЦИЯ КАК ЭЛЕМЕНТ КРИМИНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ // ВЕСТНИК МОСК. УН-ТА. СЕР. 11. ПРАВО. - М., 1998. - № 4. - С. 50-64.

6. РОССИНСКАЯ Е.Р ПРЕДМЕТ И ПРАКТИЧЕСКИЕ ПРИЛОЖЕНИЯ КОМПЬЮТЕРНО-ТЕХНИЧЕСКОЙ ЭКСПЕРТИЗЫ //ИНФОРМАТИЗАЦИЯ ПРАВООХРАНИТЕЛЬНЫХ СИСТЕМ: ТЕЗИСЫ ДОКЛАДОВ МЕЖДУНАР.КОНФ. В 2-Х Ч. М., 1998. Ч. 2.

7. Скоромников К.С. Расследование преступлений в сфере компьютерной информации // Руководство для следователей / Под ред. Н.А.Селиванова, В.А. Снеткова. М., 1997.

8. Толеубекова Б.Х. Компьютерная преступность: вчера, сегодня, завтра. Караганда, 1995.

9. ТЯЖИНА А.О., НОГАЙБАЕВА А.С. НОВЕЛЛЫ ДОСУДЕБНОГО РАССЛЕДОВАНИЯ ПО УПК РЕСПУБЛИКИ КАЗАХСТАН. УЧЕБНО-ПРАКТИЧЕСКОЕ ПОСОБИЕ (КРАТКИЙ АНАЛИЗ В СХЕМАХ). КАРАГАНДА, 2015.

10. ТЯЖИНА А.О., НОГАЙБАЕВА А.С., БЕЙСЕНБАЕВ А.Ж. ДОСУДЕБНОЕ ПРОИЗВОДСТВО ПО УГОЛОВНЫМ ДЕЛАМ: ОБРАЗЦЫ ПРОЦЕССУАЛЬНЫХ ДОКУМЕНТОВ, КАРАГАНДА, 2014.

11. Шурухнов Н.Г. Тактика следственного осмотра и освидетельствования Криминалистика: Курс лекций. М.: Эксмо. 2006.

Нормативные акты:

1. **Конституция Республики Казахстан** *(принята на республиканском референдуме 30 августа 1995 года), (с* изменениями и дополнениями *по состоянию на 10.03.2017 г.).*

2. Уголовно-процессуальный кодекс Республики Казахстан № 231-V-ЗРК *(с* изменениями и дополнениями *по состоянию на 09.01.2018 г.)*

3. Уголовный кодекс Республики Казахстан № 226-V-ЗРК *(с* изменениями и дополнениями *по состоянию на 09.01.2018 г.)*

4. Приказ Генерального Прокурора Республики Казахстан «Об утверждении правил приема и регистрации заявлений и сообщений об уголовных правонарушениях, а также ведения Единого реестра досудебных расследований» №89 от 19.09.2014г. с изм. и доп. от 10.08.2015 г. №99, 23.09.2016 №148.

5. Приказ Генерального прокурора Республики Казахстан от 22 сентября 2014 года №91 «Об утверждении Правил применения научно-технических средств фиксации хода и результатов следственных действий».

6. **Закон Республики Казахстан от 11.01.2007 N 217-III «Об информатизации».**

Введение

Развитие и совершенствование правового регулирования общественных отношений, повышение его эффективности – одна из важнейших задач, стоящих перед юридической наукой. Актуальность проблемы совершенствования правового регулирования приобретают в наши дни в связи с интенсивным развитием современного информационного общества и высоких технологий.

Во всем мире информационные технологии и Интернет прочно входят в повседневную жизнь. Несмотря на то, что преобладающее большинство операций в Интернете осуществляется в законных целях, всемирная сеть все чаще используется для претворения в жизнь мошеннических схем.

В таких государствах, как США, Великобритания, Япония, Канада, Германия правительства давно осознали характер угрозы, исходящей от компьютерных преступлений, и создали эффективную систему законодательства и правоохранительных органов для борьбы с ними. Борьба с такого рода преступлениями базируется на понимании необходимости

тесного взаимодействия и сотрудничества на всех уровнях государственной власти и частного сектора экономики.

Глубокое исследование проблем компьютерных технологий невозможно без привлечения специалистов различных отраслей знаний - кибернетики, математики, информатики, радиотехники, электроники, связи и т.п. Труднее всего специалистам юридической науки, поскольку необходимо как дать своевременную и должную уголовно-правовую оценку существующим правонарушениям в сфере компьютерной информации, так и подготовить нормы закона к появлению новых форм компьютерной преступности. Одновременно важно не только профессионально сформулировать уголовный закон, но и продумать механизм его реализации.

В уголовно-правовой науке до последнего времени не уделялось серьезного внимания исследуемой проблематике. Именно поэтому важно уделить внимание расследованию преступлений данной категории уголовных дел, что позволит совершенствовать Уголовный кодекс РК, который должен обеспечивать безопасность общества, государства и гражданина в сфере информационных отношений.

Объектами посягательств могут быть сами технические средства (компьютеры и периферия) как материальные объекты, программное обеспечение, базы данных и информация, как таковая. А сами преступления, где применяются компьютерные технологии, чрезвычайно многогранны и сложны, например, это может быть: перехват конфиденциальных сигналов пейджинговых и сотовых станций, подделка кредитных карт, несанкционированный доступ к информации, ввод в программное обеспечение «логических бомб», которые частично или полностью выводят из строя компьютерную систему, разработка и распространение компьютерных вирусов, хищение компьютерной информации и многое другое.

Одним из наиболее распространенных видов компьютерных посягательств является неправомерный доступ к компьютерной информации. Такие преступления чаще посягают на охраняемую законом информацию и совершаются с умыслом на добычу и неправомерное использование ее в корыстных целях. У данного вида компьютерных преступлений большой потенциал в виду того, что информация растущими темпами приобретает характер основного ресурса человеческой деятельности и опасность неправомерного доступа к ней трудно переоценить.

1. Понятие и значение преступления в сфере высоких информационных технологий.

Отсутствие четкого определения компьютерной преступности, единого понимания сущности этого явления значительно затрудняют определение задач правоприменительных органов в выработке единой стратегии борьбы с ней.

В настоящее время существуют два основных течения научной мысли. Одна часть исследователей относит к компьютерным преступлениям действия, в которых компьютер является либо объектом, либо орудием посягательств. В этом случае кража компьютера тоже является компьютерным преступлением. Другая часть исследователей утверждает, что объектом посягательства является информация, обрабатываемая в компьютерной системе, а компьютер служит орудием посягательства. Надо сказать, что законодательство многих стран, в том числе и в Казахстане, стало развиваться именно по этому пути.

Новое уголовное законодательство включает в себя ряд неизвестных ранее составов преступлений, среди которых есть нормы, направленные на защиту компьютерной информации. Необходимость установления уголовной ответственности за причинение вреда в связи с использованием именно компьютерной информации вызвана возрастающим значением и широким применением ЭВМ во многих сферах деятельности и наряду с этим повышенной уязвимостью компьютерной информации по сравнению, скажем, с информацией, зафиксированной на бумаге и хранящейся в сейфе.

Итак, компьютерные преступления – это преступления, совершенные с использованием компьютерной информации. При этом компьютерная информация является предметом и (или) средством совершения преступления.

По свидетельству специалистов, наиболее привлекательным сектором экономики практически любой страны является ее кредитно-финансовая система. Наиболее распространенным в этой области являются компьютерные преступления, совершаемые путем несанкционированного доступа к банковским базам данных посредством телекоммуникационных сетей.

Следует отметить, что одним из новых направлений для преступной деятельности в информационной сфере является использование глобальных коммуникационных информационных систем с удаленным доступом к совместно используемым ресурсам сетей, таких как Интернет (International Network - международная система связи). В настоящее время Интернет, использующая в большинстве случаев телефонные линии, представляет собой глобальную систему обмена информационными потоками. Вполне закономерно, что подобная информационная сеть, объединившая огромное число людей с возможностью подключения к ней любого человека, стала не только предметом преступного посягательства, но и очень эффективным средством совершения преступлений.

Используя Интернет в качестве среды для противоправной деятельности, преступники очень часто делают акцент на возможности, которые им дает сеть, обмена информацией, в том числе и криминального характера. Аналогичная ситуация складывается и при использовании компьютерных минипроцессоров, составляющих основу современной мобильной или так называемой сотовой телефонной связи. Однако следует отметить, что большинство ее видов при эксплуатации позволяют

оперировать лишь аудио и небольшими по объему частями текстовой информации, в то время как подключение этих устройств к цифровым каналам Интернет позволяет передавать не только аудио, но и видео, а также практически не ограниченные объемы текстовой и графической информации.

Другая черта сети Интернет, которая привлекает преступников, - возможность осуществлять в глобальных масштабах информационно-психологическое воздействие на людей.

Наиболее распространенными преступлениями с использованием компьютерной техники являются: компьютерное пиратство, компьютерное мошенничество, распространение вредоносных (вирусных) программ и компьютерный саботаж. К компьютерному пиратству относят, прежде всего, деятельность «хакеров» - неправомерный доступ к компьютерной информации с помощью подбора паролей, кодов, шифров, взломов электронных замков и т.п. Когда результатом подобной деятельности являются модификация информации и утечка денежных средств - она превращается в компьютерное мошенничество. Второй вид компьютерного пиратства - незаконное копирование, тиражирование и сбыт компьютерных программ. Подобная деятельность нарушает авторские права создателей и разработчиков программ, причиняет материальный ущерб им и законным владельцам компьютерных программ. К тому же страдают пользователи программного продукта, так как качество копий уступает качеству оригинала.

Затрагивая проблему компьютерного пиратства, представляет интерес тот факт, что для зарубежного законодательства очевидна следующая тенденция: составы собственно компьютерных преступлений (действия против только охраняемой компьютерной информации) либо просто отсутствуют, либо существуют наряду с традиционными составами (мошенничество, выдача государственной тайны, собирание и распространение персональных данных). Последние либо предусматривают самостоятельный состав, который выступает как специальный по отношению к общему (тому же мошенничеству), либо находятся в той же статье в качестве квалифицированного состава.

Большинство компьютерных преступлений - это проявления профессиональной и организованной преступности, нередко носящей групповой транснациональный характер. Причем часто в состав группы входит непосредственный работник кредитной организации или иной компании, которая впоследствии оказывается пострадавшей (по некоторым оценкам, при хищениях с использованием компьютерных средств до 80% таких деяний совершались «изнутри»).

Транснациональный характер компьютерной преступности, быстрые темпы ее распространения обусловливают неизбежность объединения сил и средств многих государств по противостоянию этому явлению. В настоящее время создается острая необходимость разработки международно-правовой базы предотвращения инцидентов, связанных с обменом информацией, борьбы против «информационного терроризма», разработки комплекса мер

международного характера, предотвращающих деструктивное использование средств воздействия на национальные и глобальные информационные ресурсы.

Родовым объектом компьютерных преступлений является общественная безопасность. В качестве дополнительных объектов в ряде случаев могут выступать права и интересы граждан в сфере обеспечения личной, семейной, врачебной и т.п. тайны, интересы собственности, защищенность государственной, банковской тайны и т.п.

Видовым объектом преступлений является совокупность общественных отношений, обеспечивающих состояние защищенности процессов создания, сбора, хранения, передачи и использования компьютерной информации, в которых правомерно участвуют собственники, владельцы и пользователи информации (информационная безопасность).

Большей частью преступления в сфере компьютерной информации могут совершаться только путем действия - неправомерный доступ к компьютерной информации или создание либо использование вредоносных программ для ЭВМ. Однако нарушение установленных правил эксплуатации ЭВМ, системы ЭВМ или их сети возможно и путем бездействия - в виде невыполнения обязательных предписаний таких правил.

Неправомерный доступ к компьютерной информации и нарушение установленных правил эксплуатации ЭВМ, системы ЭВМ или их сети сформулированы как преступления с материальным составом, а создание либо использование вредоносных программ для ЭВМ - с формальным. В качестве последствий указываются: уничтожение, модификация, блокирование либо копирование информации, нарушение работы ЭВМ или системы ЭВМ, причинение существенного вреда и т.п.

Временем совершения компьютерного преступления является момент нажатия клавиши клавиатуры компьютера или кнопки «мыши», отсылающей последнюю компьютерную команду, независимо от того, в какое время наступили опасные последствия.

Значительно сложнее обстоит дело с определением места совершения преступления. Поскольку большое количество компьютерных преступлений совершается в компьютерных сетях, объединяющих несколько регионов или стран, лидирующее место среди которых занимает всемирная компьютерная сеть Интернет, постольку место совершения деяния и место наступления последствий могут отделять многие километры, таможенные и государственные границы.

Уголовный кодекс РК не содержит нормы, определяющей место совершения преступления, поэтому им может быть место как совершения деяния, так и наступления последствий, либо то место, в котором деяние окончено либо пресечено.

Если применить по аналогии норму о времени совершения преступления, то местом его совершения надлежит считать место отдачи последней компьютерной команды, однако принцип законности запрещает применение уголовного закона по аналогии. Следует также учитывать, что

преступления с материальными составами считаются оконченными с момента наступления таких последствий. Общественную опасность преступления определяет не само деяние, а тот вред, который оно причинило или могло причинить. Поэтому место наступления последствий может быть определяющим.

Термин «компьютерные преступления» впервые использован в американской, а затем и другой зарубежной литературе в начале 60-х годов, когда стали известны первые случаи совершения преступлений с использованием ЭВМ. Первый специальный закон о компьютерных правонарушениях был принят в штате Флорида США, в соответствии с которым модификация, уничтожение, несанкционированный доступ или изъятие компьютерных данных, программ или сопутствующей документации, те же действия, совершенные с целью хищения какой-либо собственности признавалась фелонией . Затем практически во всех штатах США вступило в действие специальное законодательство о компьютерных правонарушениях. В первой половине 80-х годов наряду с этим было разработано федеральное законодательство, посвященное регулированию данной проблемы (Comprehensive crime control act of 1984). С принятием федерального законодательства правовая охрана компьютерных систем строилась на основе запрещения несанкционированного доступа и получения информации определенного рода.

Не смотря на наличие достаточно устоявшейся законодательной базы, среди ученых нет пока ни общепринятого понятия компьютерных преступлений и обоснованной их классификации, ни их криминалистической характеристики, как нет и достаточно научно разработанных методик их предотвращения, раскрытия и расследования. Одна часть исследователей относит к компьютерным правонарушениям действия, в которых компьютер является объектом либо орудием посягательства. Эта точка зрения отражена в докладе министерства здравоохранения США, в котором кража самих компьютеров рассматривается как один из способов совершения компьютерных правонарушений. Другие исследователи относят к этому виду преступлений только неправомерные действия в сфере автоматизированной обработки информации. Они выделяют то главное в компьютерных преступлениях, что позволяет считать их отдельным видом преступлений, характеризующихся общностью способов, орудий, объектов посягательства: объектом посягательства является информация, обрабатываемая в системе, а компьютер служит орудием посягательства. По этому пути стало развиваться и законодательство, в частности, США.

Некоторые ученые разделяют понятия компьютерных преступлений и преступлений, совершенных с использованием вычислительной техники, считая, что это далеко не одно и тоже. Такая градация свойственна научной мысли тех стран, где компьютеризация находится на ранних стадиях развития. Мы согласны с ней в том, что первая формула требует категориальных признаков, вторая предполагает рассмотрение компьютеров только как орудий совершения иных, известных уголовному праву, категорий преступлений. «Этот феномен носит временный характер. Тенденция к изменению точки зрения начнет проявляться вместе с расширением спектра преступного применения ЭВМ и увеличением наносимого ущерба.

Использование компьютерной техники в преступных целях может осуществляться в следующих формах:

- использование программных продуктов в качестве объекта преступления (незаконное копирование, причинение ущерба применением разрушающих программ - вирусов);

- использование программных продуктов в качестве инструмента совершения преступления (несанкционированное проникновение в компьютерную систему, искажения и подлоги информации);

- объектом совершения преступления являются технические средства ЭВМ (кража компьютера, незаконное использование машинного времени);

- использование технических средств ЭВМ как средства совершения преступления (внесение изменений в информационную базу, изготовление с помощью печатной базы ЭВМ фальшивых документов).

Как уже ранее отмечалось, среди дел, традиционно рассматриваемых судами, все чаще появляются такие, которые вытекают из информационных правоотношений или связаны с последними. Естественно требуется выработать адекватные средства правильного разрешения таких дел, исследования и доказывания фактических обстоятельств, входящих в предмет изучения.

При всей емкости действующих норм доказательственного права, их способности удовлетворительно обслуживать все новые и новые общественные потребности за счет заложенного в них запаса прочности, с одной стороны, и гибкости судебной практики - с другой, происшедшие под влиянием научно-технического прогресса изменения настолько велики, что требуют дальнейшего развития процессуального законодательства в направлении расширения границ допустимости доказательств; расширения круга традиционных следственных действий, появление дополнительных гарантий при их производстве.

Совокупность понятий, используемых в той или иной науке, образует ее понятийный аппарат, который правомерно рассматривать как теоретический костяк данной науки. Но эту роль понятийный аппарат выполняет лишь тогда, когда образующие его понятия взаимосвязаны, причем взаимосвязь их настолько существенна, что изменение содержания и объема одного из них влечет за собой уточнение другого или даже логической структуры данной науки.

Каждая наука оперирует своим понятийным аппаратом, формирование которого во многом предопределяется характером и природой самой науки, ее предметом и объектами исследования.

Исследуя проблему собирания и использования компьютерной информации при расследовании преступлений мы таким образом попытались вторгнуться в еще не познанную в полной мере криминалистикой сферу, законы которой диктуются различными областями научных знаний. Решение указанной проблемы, а это видно из ее постановки, лежит во взаимосвязи проявлений общих закономерностей взаимодействия криминалистики, уголовного права, уголовного процесса, кибернетики, математики, информатики и других наук. Исходя из этого в результате ее взаимодействия с указанными науками (применительно к нашей проблематике) не могут не появляться элементы их языка. «Практика показывает, - что использование средств и методов математики, в частности ее языка, приводит к тому, что понятия, которые применяются для описания хода и результатов исследования, приобретают более определенный характер, степень их подтверждения увеличивается, а систематическая связь суждений в пределах структуры научных высказываний улучшается».

Одним из ключевых понятий, как нам представляется, является понятие «компьютерной информации».

Вплоть до середины XX века термин «информация» и в обиходе и в научной литературе обычно употреблялся в смысле сообщения, осведомления кого-либо о чем-либо или, что близко к этому, в смысле сведений, передаваемых одними людьми другим людям. С развитием технических средств передачи, восприятия и в особенности анализа различного рода сведений, а также с зарождением информатики и кибернетики – наук, внесших весомый вклад в реализацию проблемы обмена сведениями не только между людьми, но и между человеком и машиной (в частности, ЭВМ) - понятие «информация» стало объектом специального и разностороннего исследования. Это привело к формированию целого «семейства» теорий информации и к самым различным определениям самого понятия «информация».

В философском плане информацию можно определить как отражение разнообразия, существующего в материальном мире. Отражение, как одно из универсальных свойств материи, заключается в воспроизведении особенностей одного объекта в другом в результате их взаимодействия. Информация – это не просто сообщение, сведения из книг и других источников, а то новое, что познается из них человеком и используется им. «Познать механизм отображения можно лишь путем анализа философской категории движения материи, в частности такой ее формы, как взаимодействие одного материального образования с другим. Результатом их взаимодействия и являются отображения, а данные, образующие их содержание - информацией»

Развитие информационных технологий заставляет интенсивно совершенствовать законодательную базу, вводя понятия, ранее применявшиеся в кибернетике и информатике.

Закон Республики Казахстан от 11.01.2007 N 217-III "Об информатизации" определяет термины «информатизация», «документированная информация», «информационные процессы», «информационная система», «средства обеспечения автоматизированных информационных систем» и др. Данная терминология позволяет нам с позиции юридических наук определить виды и источники компьютерной информации, используемые при расследований преступлений. Поэтому, говоря о компьютерной информации как о полноправном объекте изучения доказательственного права мы не можем рассматривать ее в отрыве от понимания принципов работы компьютера, технологии обработки данных с помощью ЭВМ, форм существования и преставления информации при ее машинной обработке и др.

В процессе работы компьютер осуществляет: ввод информации извне; преобразование; вывод в виде, доступном для восприятия человеком.

Процесс получения информации компьютером называют кратко «ввод», а выдачу ее пользователю - «вывод». Эти процессы настолько важны, что для их реализации предложено наибольшее количество разнообразных устройств (на которых мы остановимся ниже). Ввод и вывод это две стороны одного процесса обмена информации, причем без одной из них не бывает другой. Поэтому когда говорят не о преобразовании данных, а об их передаче компьютеру для вычислений и получения итоговых результатов, применяется термин «ввод\вывод».

Ввод информации в компьютер осуществляется специализированными устройствами - как стандартными (т.е. входящими в состав базовой системы

компьютера), так и нестандартными. Стандартными устройствами ввода в ЭВМ являются клавиатура и накопители - на гибких магнитных дисках (НГМД) и/или на жестких магнитных дисках (НЖМД). К нестандартным устройствам можно отнести мышь, модем, дигитайзер, сканер, аналого-цифровой преобразователь и др.

Блок устройств вывода информации позволяет пользователю получить результаты работы компьютера в привычном для него виде. Устройства вывода (также, как и ввода) могут быть стандартными и нестандартными. К стандартным устройствам вывода относятся монитор (дисплей) и накопители на жестких и гибких дисках. К нестандартным - принтер, модем, плоттер (графопостроитель) и др.

Для долговременного и надежного хранения данных создано множество устройств: магнитные и магнитооптические дисковые накопители, накопители на магнитной ленте и др. У внешних запоминающих устройств есть несколько главных преимущества перед оперативной памятью (мы рассматриваем эти преимущества с точки зрения сохранности следов преступления):

- хранение данных не требует бесперебойного обеспечения энергией;
- объемы информации могут быть чрезвычайно большими;
- сами устройства существуют вне конструкции конкретной ЭВМ. Для того, чтобы подчеркнуть, в чем состоит отличие между двумя способами хранения информации - оперативной и долговременной (или внешней) памятью, приведет чисто бытовую аналогию.

В компьютере данные сохраняются только при обеспечении его непрерывного питания от сети. При падении напряжения или случай-ном\преднамеренном выключении информация теряется. Человек, не надеющийся на свою память, делает те или иные пометки в записной книжке. В противном случае восстановить забытое будет нелегко. Аналогичный процесс реализован в компьютере: по окончании сеанса работы (или несколько раз в процессе работы) содержимое оперативной памяти записывается на диск (это своеобразная компьютерная «записная книжка»). В результате этой операции для данных не опасно внезапное выключение из сети - информация записана на диск. Чтобы вспомнить все, над чем ПК работал ранее, он считывает информацию с диска в оперативную память так же точно, как человек прочтет запись в своей записной книжке.

Мы намеренно подробно не останавливается на всех разновидностях устройств ЭВМ. Это продиктовано тем, что динамика развития компьютерной техники настолько высока, что появление новых образцов компьютерной техники и моральное устаревание уже имеющихся не позволяют нам обращать внимание на конкретную их разновидность. Конечно, в своем исследовании мы указываем многие устройства, поскольку они являются объектами, например, следственного осмотра и полностью абстрагироваться от конкретных их разновидностей мы не может. Однако надо иметь в виду многообразие электронных приборов составляющих в своей совокупности компьютер (в его бытовом понимании). Их даже полное перечисление будет полным лишь на сегодняшний день и уже «завтра» этот список может значительно возрасти.

Компьютерная информация является разновидностью информации вообще, ее видовым понятием. Поэтому все признаки, характерные для понятия информации, присущи в равной степени и понятию компьютерной информации. В

тоже время компьютерная информация имеет существенные специфические особенности, которые позволяют выделить ее в самостоятельное понятие.

Таким образом, исходя их сказанного нам представляется возможным определить компьютерную информацию применительно к процессу доказывания как ***фактические данные, обработанные компьютером и полученные на его выходе в форме, доступной восприятию ЭВМ либо человека или передающиеся по телекоммуникационным каналам, на основе которых в определенном законом порядке устанавливаются обстоятельства, имеющие значение для правильного разрешения дела.***

Применительно к средствам вычислительной техники источниками компьютерной информации могут служить: машинная распечатка, накопители на магнитных, оптических и иных носителях, информация, содержащаяся в оперативной памяти ЭВМ, информация, содержащаяся в постоянном запоминающем устройстве.

Мы разделили источники компьютерной информации по физической природе ее хранения и предоставления пользователю.

Машинная распечатка представляет собой выполненный на традиционном материальном носителе (бумаге, пленке и т.д.) с помощью некоторых устройств вывода ЭВМ (принтера, плоттера, другого печатающего устройства) документ, созданный посредством программных средств ЭВМ. В данном случае для восприятия содержания информации следователем обычно не требуется преобразующих ее устройств.

Для хранения данных в ЭВМ используют различного рода накопители. Их общая память, как правило, в сотни раз превышает размер оперативной памяти. По способу записи и чтения информации дисковые накопители можно подразделить на магнитные, оптические и магнитооптические. Дисковые накопители обычно делят на следующие группы: накопители на гибких дисках; накопители на жестких дисках; накопители на флоптических дисках; накопители на сменных жестких дисках; накопители, используемые эффект Бернулли; накопители на магнитооптических дисках; накопители на оптических компакт-дисках (CD-ROM); накопители на оптических дисках типа WORM (Write Only, Read Many - однократная запись, многократное чтение).

Самыми распространенными накопителями на магнитных носителях в настоящее время являются магнитные диски. По своей природе они являются материальными носителями компьютерной информации и различаются лишь принципами ее записи и считывания. Различают гибкие (floppy) и жесткие (hard) накопители на магнитных дисках (или просто диски), магнитные ленты. Информация непосредственно записывается на магнитный диск (принцип записи и чтения подобен записи и воспроизведению речи или музыки на бытовом магнитофоне).

За последние несколько лет в качестве альтернативы несъемным накопителям на жестких магнитных дисках появились накопители со сменным носителем. Понятие «накопители со сменным носителем» объединяет самые различные изделия от оптических накопителей и дисковых кассет до съемных НЖМД, которые можно извлечь из компьютера и «захватить с собой». Эти устройства сильно разнятся друг от друга по технологии, конструкции, цене, емкости памяти и области предполагаемого применения.

2. Направления преступной деятельности в информационной сфере и их классификация.

Развитие рынка компьютеров и программного обеспечения, повышение профессиональной подготовки пользователей, увеличение потребностей организаций в совершенствовании технологий обработки данных значительно расширило круг применения ЭВМ, которые все чаще организуются в локальные сети, подключаются к сетям широкого доступа.

Все активнее внедряется автоматизированная обработка бухгалтерской и иной производственной документации, «безбумажные» технологии. Информация, содержащаяся в компьютере, зачастую на бумаге вообще не хранится. Компьютер стал практически обязательным элементом рабочего стола не только руководителей, но и рядовых сотрудников.

Процесс компьютеризации оказывает влияние на состояние, и структуры управления, производства, правового регулирования. С их помощью решаются задачи организации производства, заключаются сделки, осуществляется переписка между удаленными пользователями и т.д. Компьютеры уже помогли автоматизировать многие стороны человеческой деятельности. Даже физическую защиту все чаще поручают не охранникам, а интегрированным компьютерным системам, что позволяет одновременно отслеживать перемещение сотрудников и по физическому пространству предприятия и по информационному пространству.

Знакомясь с развитием электронно-вычислительных систем на примерах наиболее развитых стран – «пользователей» компьютеров видно, что явление это объективное, обусловленное коренными изменениями в составе факторов экономического роста.

Круг исследуемых нами вопросов охватывает помимо компьютерных преступлений также и преступления, совершаемые с использованием вычислительной техники, которые законодатель не выделяет в отдельную уголовно-правовую категорию. Рассматривая данное множество преступных деяний (обычно традиционных преступлений, при совершении которых использование вычислительной техники может служить как квалифицирующим признаком, так и орудием совершения преступления) мы полагаем с криминалистической точки зрения правомерным включение в этот перечень способов совершения традиционных преступлений с использованием средств ЭВТ. Более того, на настоящем этапе следственная практика нуждается в криминалистических рекомендациях по собиранию и исследованию «компьютерных следов» при раскрытии и расследовании общеуголовных преступлений. Во-первых, потому, что данный массив уголовных дел по таким преступлениям во много раз превосходит только появляющиеся случаи расследования компьютерных преступлений.

Во-вторых, интеллектуальный уровень и материальный достаток преступников достаточно велик. Новые информационные технологии дали толчок не только в плане прогресса общества, но и стимулировали возникновение и развитие неизвестных ранее негативных процессов.

Особенностью современной криминогенной ситуации является интенсивное перерастание количественных характеристик преступности в негативные качественные. Набирают силу опасные процессы сращивания организованной преступности с так называемой респектабельной («беловоротничковой»), к которой

нами относятся экономическая и компьютерная преступность; лидеров преступных групп и сообществ с коррумпированными должностными лицами. Идет активный процесс размывания граней между различными видами преступлений. Например, преступники, организованные в группы и сообщества, начинают применять методы, традиционно используемые в своей преступной деятельности преступниками экономической сферы, нередко используя при этом средства компьютерной техники, связи и телекоммуникаций, входя в сговор с должностными лицами. Данный процесс приводит к тому, что многие преступные сообщества начинают переориентировать свою преступную деятельность с получения и использования незаконных средств, добытых противоправными действиями (например, вымогательством), на совершение противоправных манипуляций с законными средствами в корыстных целях. Иными словами, переходят от оборота преступных средств к более выгодному преступному обороту законных средств. Международный опыт свидетельствует, что современная преступность проникает в область законного предпринимательства, подрывая репутацию тех, кто так или иначе соприкасается с ней, и коррумпирует должностных лиц, услуги которых ей необходимы для отмывания незаконных доходов. На уровне ООН констатировано, что возможности преступности манипулировать значительным капиталом, проникать в область законного предпринимательства и разорять своих конкурентов с помощью контроля над ценами и курсом валют представляет серьезную угрозу самому существованию любого общества. Например, огромные незаконные средства, проникающие в экономику страны, денежную систему, банковское дело путем манипулирования валютой с целью «отмывания» денег или для получения незаконных доходов, неизбежно приводят к нарушению естественного действия рыночных сил, оказывают пагубное влияние на обменные курсы валют и банковские системы одновременно во многих странах.

Криминальные структуры активно используют для достижения своих преступных целей новейшие достижения науки и техники. В одном ряду здесь стоит использование безбумажных технологий, модернизация технологии документооборота. Таким образом следы преступной деятельности все чаще оставляются на нетрадиционных носителях, к которым в первую очередь относятся машинные носители информации. Изучение практики расследования уголовных дел показывает, что доказательственная информация, «найденная в компьютере», может иметь значение по совершенно различным составам. Сейчас мы акцентируем внимание на том, что при современном развитии вычислительной техники и информационных технологий «компьютерные следы» преступной деятельности имеют широкое распространение. Это должно учитываться следователями и оперативными работниками в их деятельности по собиранию доказательств наряду с поиском уже ставшими традиционными следами (например, относительно недавно разработанные методики использования микрочастиц в доказывании в настоящее время не представляют особых проблем для признания данных следов вещественными доказательствами по уголовным делам).

Изучение специальной литературы показывает, что авторы рассматривают компьютерную информацию, относя данный аспект к проблематике компьютерной преступности. Считаем, что это не вполне оправданно по указанным выше причинам. Современное состояние преступности и практика расследования

заставляют исследователей обратить внимание на поиск, собирание и использование «информационных» следов именно по общеуголовным делам. При этом мы ни сколько не уничижаем исследование феномена компьютерной преступности. Опасность данного вида преступлений для общества значительна и это мы оговорим позднее. Однако данные исследования носят скорее предупреждающий характер, когда как перед практикой остро стоит проблема доказывания иных видов преступлений, количество которых растет лавинообразно.

Выделяются способы использования вычислительной техники для достижения преступной цели:

1. Создание преступником компьютерной базы данных, содержащей информацию о преступлении.

2. Использование ЭВМ и периферийных устройств в качестве полиграфической базы для проектирования и изготовления фальсифицированных (подложных) документов, денежных знаков и т.д.

Распространение компьютерных систем, объединение их в коммуникационные сети усиливает возможности электронного проникновения в них. Диапазон такого рода действий чрезвычайно широк - от тривиального подслушивания до изощренных, требующих отличной математической и технической подготовки действий. С широким распространением персональных компьютеров даже «преступник-дилетант» может проникнуть в большинство компьютерных систем.

В целом система доказательств по делам о компьютерных преступлениях ложится в общую логику доказывания. Основное их отличие в том, что в последнем случае перед следователем изначально стоит задача доказывания факта именно «информационных преступлений», среди которых: установление факта события преступления; определение объекта преступного посягательства; определение предмета преступного посягательства; способ совершения преступления; обстоятельства, способствовавшие совершению преступления и др.

На сегодняшний день в нашей стране не существует статистики, которая бы обобщала накопленный опыт в этом направлении. Поэтому сделанная нами выборка уголовных дел достаточна условна. Мы понимаем, что она не может в полной мере отражать современное состояние практики расследования. Однако проведенный нами анализ позволяет определить тенденции эволюции компьютерной преступности в нашей стране, проверить верность высказанных нами тактических и методических рекомендаций, определить задачи, стоящие перед органами предварительного расследования и судами. Кроме этого, учитывая то, что НТП явление глобального масштаба и коль скоро компьютер является его детищем, то и признаки, выделяющие компьютерные преступления в ряду иных категорий уголовно наказуемых деяний, будут совпадать в различных странах. Поэтому мы считаем уместным в данном разделе обратиться к зарубежному опыту, где к собиранию и использованию компьютерных следов преступления подошли значительно раньше, чем в Республике Казахстан.

Анализ отечественной и зарубежной специальной литературы, изучение уголовных дел, опросы практических работников оперативных служб, следователей и судей позволил нам определить основные проблемы, возникающие при расследовании дел, где в качестве доказательства выступает компьютерная информация: установление самого события преступления и правильная его квалификация; неопределенность следователя при проведении следственных

действий по обнаружению, изъятию, фиксации и исследования компьютерной информации; отсутствие у следователей практики расследования преступлений, совершаемых с использованием компьютерной техники; отсутствие элементарных знаний компьютерной техники и, как следствие этого, психологический барьер, возникающий при расследовании таких дел.

В отечественной и зарубежной литературе достаточно много внимания было уделено классификации способов компьютерных преступлений. Основываясь на результатах собственного исследования, а также на изучении отечественной и зарубежной литературы приведем некоторые способы их совершения. Следует отметить, что равно как развитие вычислительной техники находится на высоком уровне, так и криминализация использования компьютеров соразмерно этому уровню. Поэтому мы не ставили цели собрать воедино все способы совершения таких преступлений из-за постоянного обновления данной выборки.

Как нами отмечалось ранее, компьютерная информация выступает в качестве источника доказательств по: делам о компьютерных преступлениях; делам об иных преступлениях.

Как показывает изучение специальной литературы, исследователи не пришли к однообразному построению классификации компьютерных преступлений. По нашему мнению, эти преступления можно разделить по способам их совершения на несколько следующих групп: методы перехвата; методы несанкционированного доступа; методы манипуляции; комплексные методы.

1. Методы перехвата.

Непосредственный перехват. Вероятно, это старейший из используемых сегодня способов. Все требующееся для этого оборудование нетрудно приобрести в магазинах: микрофон, радиоприемник, кассетный диктофон, модем, принтер. Перехват данных осуществляется либо непосредственно через телефонный канал системы, либо подключением к компьютерным сетям. Вся информация записывается.

Электромагнитный перехват. Не все перехватывающие устройства требуют непосредственного подключения к системе. Так, без прямого контакта можно уловить излучение, производимое центральным процессором, дисплеем, телефоном, принтером, линиями микроволновой связи. С дисплейных терминалов, можно считывать данные при помощи простейших технических средств, доступных каждому. Чтобы выведать банковские секреты или же результаты научных исследований, требуется лишь так называемая дипольная антенна, которая доступна каждому радиолюбителю, а также обычный телевизор.

«Клоп» («жучок»). Установка микрофона в компьютере с целью перехвата разговоров работающего на ЭВМ персонала. Этот простой прием обычно используется как вспомогательный для получения информации о работе компьютерной системы, о персонале, о мерах безопасности и т.д.

«Уборка мусора». Этот способ получения информации состоит в поиске данных, оставленных пользователем после работы с компьютером, и имеет две разновидности - физическую и электронную. В физическом варианте он может сводиться к осмотру содержимого мусорных корзин и сбору оставленных за ненадобностью листингов, ненужной деловой переписки и т.п. Электронный вариант требует исследования данных, оставленных в памяти машины. Здесь используется тот факт, что последние записанные данные не стираются после

завершения работы. Другой пользователь записывает только небольшую часть своей информации, а затем спокойно считывает предыдущие записи, выбирая нужную ему информацию. Таким способом могут быть обнаружены пароли, имена пользователей и т.п.

2. Методы несанкционированного доступа.

«За дураком». Прием «за дураком» часто используется для проникновения в закрытые зоны, как пространственные, так и электронные. Типичный физический вариант состоит в следующем: нужно набрать полные руки всяких предметов, связанных с работой на компьютере, и прохаживаться с деловым видом возле запертой двери, за которой находится терминал. Когда идет законный пользователь остается только пройти в дверь вместе с ним. На этом же принципе основан и электронный вариант. Обычно этот прием проходит, когда компьютерный терминал незаконного пользователя подключается к линии законного пользователя через телефонные каналы, или когда пользователь выходит ненадолго, оставляя терминал в активном режиме.

«За хвост». Этот прием имеет определенное сходство с предыдущим. Здесь незаконный пользователь тоже подключается к линии связи законного пользователя. Но затем он терпеливо дожидается его сигнала, обозначающего конец работы, перехватывает его, а затем осуществляет доступ к системе, когда законный пользователь заканчивает активный режим.

Компьютерный абордаж. Хакеры, набирая на удачу один номер за другим, терпеливо дожидаются, пока на другом конце провода не отзовется чужой компьютер. После этого телефон подключается к приемнику сигналов в собственной ПЭВМ, и связь установлена. Если теперь угадать код (а слова, которые служат паролем часто банальны и обычно берутся из руководства по использованию компьютера), то можно внедриться в чужую компьютерную систему.

Неспешный выбор. В этом случае несанкционированный доступ к файлам законного пользователя осуществляется нахождением слабых мест в защите системы. Однажды обнаружив их, нарушитель может не спеша исследовать содержащуюся в системе информацию, копировать ее, возвращаться к ней много раз.

«Маскарад». «Маскарад» или «самозванство» состоит в том, что некто проникает в компьютерную систему, выдавая себя за законного пользователя. Системы, которые не обладают средствами аутентичной идентификации (например, по физиологическим характеристикам: по отпечаткам пальцев, по рисунку сетчатки глаза, голосу и т.п.), оказываются без защиты против этого приема. Самый простейший путь его осуществления - получить коды и другие идентифицирующие шифры законных пользователей.

Мистификация. Иногда случается, как, например, с ошибочными телефонными звонками, что пользователь с удаленного терминала подключается к чьей-то системе, будучи абсолютно уверенным, что он работает с той системой, с какой и намеревался. Владелец системы, к которой произошло фактическое подключение, формируя правдоподобные отклики, может поддерживать это заблуждение в течение определенного времени, получая одновременно некоторую информацию, в частности коды.

«Аварийный». Прием «аварийный» использует тот факт, что в любом компьютерном центре имеется особая программа, применяемая как системный

инструмент в случае возникновения сбоев или других отклонений в работе ЭВМ. Такая программа – мощный и опасный инструмент в руках злоумышленника.

«Склад без стен». Несанкционированный доступ осуществляется в результате системной поломки. Например, если некоторые файлы пользователя остаются открытыми, он может получить доступ к не принадлежащим ему частям банка данных. Все происходит так, словно клиент банка, войдя в выделенную ему в хранилище комнату, замечает, что у хранилища нет одной стены. В таком случае он может проникнуть в чужие сейфы и похитить все, что в них хранится.

3. Методы манипуляции.

Подмена данных. Изменение или введение новых данных осуществляется, как правило, при вводе или выводе данных с ЭВМ. Это простейший и потому очень часто применяемый способ.

Манипуляция с пультом управления. Манипуляция с пультом управления относится к злоупотреблению механическими элементами управления ЭВМ..

«Троянский конь». Способ состоит в тайном введении в чужую программу таких команд, которые позволяют осуществить новые, не планировавшиеся владельцем программы функции, но одновременно сохранять и прежнюю работоспособность. С помощью «троянского коня» преступники обычно отчисляют на свой счет определенную сумму с каждой операции.

«Салями». Тактика использования «троянского коня», основанная на том, что отчисляемые суммы малы и их потери практически незаметны

«Временная бомба». «Временная бомба», т.е. тайное встраивание в программу набора команд, которые должны сработать (или каждый раз срабатывать) при определенных условиях или по достижении определенного момента времени.

Моделирование. Для компьютерных преступлений становятся все более характерными методы моделирования. Моделируются как те процессы, в которые преступники хотят вмешаться, так и планируемые методы совершения преступления. Тем самым проводится оптимизация способа преступления.

Реверсивная модель. Существо метода заключается в следующем. Создается модель конкретной системы. В нее вводятся реальные исходные данные и учитываются планируемые действия. Затем, исходя из полученных правильных результатов, подбираются правдоподобные желательные результаты. Затем модель прогоняется назад, к исходной точке, и становится ясно, какие манипуляции с входными данными нужно проводить. В принципе, прокручивание модели «вперед-назад» может проходить не один раз, чтобы через несколько итераций добиться желаемого. После этого остается только осуществить задуманное.

4. Примеры комплексных методов.

Как правило, компьютерные преступления совершаются с помощью того или иного сочетания приемов из числа описанных выше. Некоторые из них оказываются вспомогательными, работающими на основной способ, выбранный для конкретной ситуации.

4.1 Подделка кредитных карточек.

4.2 Внесение изменений в программу.

4.3 Хищение денег манипуляцией с компьютером.

4.4 Хищение денег благодаря получению секретных кодов.

4.5 Хищение денег путем компьютерной пересылки.

Следующий круг вопросов, вызывающих особые сложности при расследовании исследуемой категории дел – выдвижение версий о лице, совершившем преступление. В.Б.Вехов, проводя исследованием личности «компьютерного правонарушителя» разделил их на три группы:

1) лица, отличительной особенностью которых является устойчивое сочетание профессионализма в области компьютерной техники и программирования с элементами своеобразного фанатизма и изобретательности. Характерной особенностью преступников этой группы является отсутствие у них четко выраженных противоправных намерений. Практически все действия совершаются ими с целью проявления своих интеллектуальных и профессиональных способностей;

2) компьютерные преступления могут совершаться лицами, страдающими «компьютерными фобиями». При наличии подобных фактов в процессе раскрытия и расследования компьютерного преступления, необходимо обязательное назначение специальной судебно-психиатрической экспертизы лицом, производящим дознание или ведущим расследование по данному уголовному делу на предмет установления вменяемости преступника в момент совершения им преступных деяний. Это, в свою очередь, должно повлиять на квалификацию деяний преступника в случае судебного разбирательства (преступление, совершенное в состоянии аффекта или лицом, страдающим психическим заболеванием и т.д.). Преступления, совершаемые преступниками рассматриваемой группы, в основном связаны с преступными действиями, направленными на физическое уничтожение, либо повреждение средств компьютерной техники без наличия преступного умысла с частичной или полной потерей контроля над своими действиями.

3) профессиональные «компьютерные» преступники с ярко выраженными корыстными целями, так называемые «профи». В отличие от первой переходной группы «любителей» и второй специфической группы «больных», преступники третьей группы характеризуются многократностью совершения компьютерных преступлений с обязательным использованием действий, направленных на их сокрытие, и обладающие в связи с этим устойчивыми преступными навыками. Преступники этой группы обычно являются членами хорошо организованных, мобильных и технически оснащенных высококлассным оборудованием и специальной техникой (нередко оперативно-технического характера) преступных групп и сообществ. Лиц, входящих в их состав, в большинстве своем можно охарактеризовать как высококвалифицированных специалистов, имеющих высшее техническое, юридическое, либо экономическое (финансовое) образование. Именно эта группа преступников и представляет собой основную угрозу для общества, является кадровым ядром компьютерной преступности как в качественном, так и в количественном плане.

По нашему мнению, круг лиц, совершивших компьютерные преступления можно также разделить на 3 группы по степени их допуска к информации:

- первая группа составляется из сотрудников непосредственно работающих в области ЭВМ;

- вторую группу представляют сотрудники-пользователи обрабатываемых данных, которые непосредственно не работают в помещении, где обрабатываются данные, однако вследствие специфики своей деятельности соприкасаются с ЭВМ;

- последнюю большую группу образуют «внешние» сотрудники. К ним относятся все те, кто не входит в число пользователей обрабатываемых данных.

Разделение круга потенциальных преступников на отдельные группы имеет большое значение с точки зрения тактики расследования. Тактические приемы расследования дел, связанных с использованием вычислительной техники не в последнюю очередь также необходимо выбирать с учетом типа преступника. Круг преступников, который занимается главным образом манипуляцией с вычислительными машинами, в первую очередь, составляется из представителей администрации и сотрудников предприятия, занимающегося обработкой данных. Поэтому манипуляции с вычислительными машинами осуществляются так называемыми «своими» людьми, которые работают в учреждении или на предприятии. Существенная опасность, которая заключается в использовании вычислительных машин для обработки данных, возникает в результате постоянного автоматизированного повторения процессов обработки данных. Обработка данных отличается в конце концов тем, что шаги выполнения вычислительной программы повторяются бесчисленное число раз. Постоянство, возникающее в результате этого автоматизма, легко может привести к тому, что преступник также бесчисленное число раз может совершить преступление с минимальным риском.

Для преступности, связанной с использованием вычислительной техники, характерным является то, что действие, направленное на совершение преступления, и преступное действие в противоположность классическим имущественным преступлениям закономерно распадаются. Это неизбежно затрудняет раскрытие преступления. В результате быстро растущего создания сетей ЭВМ потенциал угроз растет также со стороны внешних лиц. Поэтому здесь необходимо исходить из того, что происходит среднее по срокам перемещение в пределах отдельных групп преступников.

В большинстве стран мира наблюдается все возрастающее использование и совершенствование информационных технологий в криминальной деятельности. Это вызывает необходимость постоянного изучения данного криминального проявления, так как развитие компьютерных технологий приводит к использованию этих достижений при совершении компьютерных преступлений. Для правоохранительных органов многих стран данная проблема является новым видом преступности, к борьбе с которой они не всегда оказываются подготовленными. Все большее распространение получают факты совершения международных компьютерных преступлений. Особую озабоченность вызывают компьютерные мошенничества, использование компьютерной техники при «отмывании» преступно нажитых средств, распространение компьютерных вирусов, проникновение хакеров (лиц, осуществляющих несанкционированный доступ в компьютерные сети) в международные информационные системы и кражи информации.

Данная проблема обусловливает необходимость разработки международных процедур по оказанию помощи при расследовании такого рода преступлений и создания в перспективе координирующего органа в рамках Интерпола. Практически во всех выступлениях высказывалась озабоченность правоохранительных органов распространением за рамки одного государства преступлений, связанных с неправомерным использованием компьютеров.

Таким образом, в силу своей сложной организации компьютерная техника и программное обеспечение представляет для лица, производящего расследование, достаточную сложность при ее описании, осмотре, поиске необходимой доказательственной информации. На современном этапе развития нашего государства основные усилия власти направлены на преодоление всеобщего кризиса, поразившего все слои общества. Противодействие же компьютерным злоупотреблениям требует значительных материальных затрат, которые складываются из множества элементов, в том числе из затрат на приобретение дорогостоящих технических средств, обучение сотрудников и т.д. Отсутствие средств, приводящее к невозможности обеспечить сотрудникам соответствующую подготовку, а также к нехватке кадров, зачастую мешает уделить достаточное внимание этому виду преступности. Не для кого не секрет, что следователям не обойтись без досконального знания компьютерных технологий и разнообразных методов, используемых преступниками.

Заключение

В настоящей лекции, посвященной расследованию преступлений в сфере компьютерной информации, раскрытие понятия, состава преступлений в сфере компьютерной информации, рассмотрение отдельных видов компьютерных преступлений и способов защиты компьютерной информации от преступных посягательств позволяет сделать следующие выводы:

1) В настоящее время в нашей стране накоплена богатая научно-теоретическая база, которая свидетельствует о складывающемся устойчивом правовом механизме, нацеленном на защиту компьютерной информации.. Логическим развитием правовой системы, создающей условия безопасности компьютерной информации, стала разработка в УК РК группы статей, предусматривающих основания уголовной ответственности за так называемые компьютерные преступления.

2) Действующее законодательство РК требует дальнейшей доработки. Компьютерная преступность не знает границ, она выходит за пределы действительности Республики Казахстан. Это международное понятие и бороться с ней надо согласованно и сообща. С внедрением в человеческую жизнь новых компьютерных технологий, когда обмен информацией стал быстрым, дешевым и эффективным, преступность в информационной сфере переросла за рамки тех уголовно-правовых норм, направленных для борьбы с ней. Компьютерные преступления условно можно подразделить на две большие категории - преступления, связанные с вмешательством в работу компьютеров, и преступления, использующие компьютеры как необходимые технические средства.

3) Проблемы информационной безопасности постоянно усугубляется процессами незаконного несанкционированного проникновения практически во все сферы деятельности общества технических средств обработки и передачи данных и прежде всего компьютерных вычислительных систем. Не случайно, поэтому защита компьютерной информации становится одной из самых острых проблем в современной информатике. На сегодняшний день

сформулировано четыре базовых принципа информационной безопасности, которая должна обеспечивать:

- целостность данных - защиту от несанкционированных сбоев, ведущих к потере информации, а также неавторизованного, несанкционированного, противоправного создания или уничтожения данных;
- конфиденциальность (законность) информации;
- доступность для всех авторизованных зарегистрированных пользователей;
- защита компьютерной информации от противоправного посягательства (копирование, хищение, распространение, подделка).

Анализ действующего уголовного законодательства в сфере компьютерной информации позволяет говорить о необходимости решения нескольких правовых проблем, которые могут быть рассмотрены в качестве составных частей правового механизма защиты компьютерной информации:

1. Установление контроля над несанкционируемым, противоправным доступом к компьютерным информационным данным системы.
2. Ответственность за выполнение технологических операций, связанных с противоправной деятельностью в отношении компьютерной информации.

Среди наиболее эффективным мер, направленных на предупреждение преступлений в сфере компьютерной информации предлагаем выделить технические, организационные и правовые.

К техническим мерам следует отнести защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев, установку оборудования обнаружения и тушения пожара, оборудования обнаружения воды, принятие конструкционных мер защиты от хищений, саботажа, диверсий, взрывов, установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое.

К организационным мерам относится охрана вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра после выхода его из строя, организацию обслуживания вычислительного центра посторонней организацией или лицами, незаинтересованными в сокрытии фактов нарушения работы центра, универсальность средств защиты от всех пользователей (включая высшее руководство), возложение ответственности на лиц, которые должны обеспечить безопасность центра, выбор места расположения центра и т.п.

К правовым мерам следует отнести разработку правовых норм, устанавливающих уголовную ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства. К правовым мерам относятся также вопросы государственного контроля за

разработчиками компьютерных программ и принятие международных договоров об их ограничениях, если они влияют или могут повлиять на военные, экономические и социальные аспекты стран и др.

РЕЦЕНЗИЯ

на лекцию, подготовленную доцентом кафедры досудебного расследования Кемпировой Ж.С. по теме: «Общая характеристика досудебного расследования в сфере компьютерной информации и высоких технологий»

Представленная на рецензирование лекция, подготовленная Кемпировой Ж.С. соответствует требованиям, установленным для написания такого вида работ. Данная работа посвящена актуальной и практически востребованной проблеме – возникающих в ходе досудебного расследования по уголовным делам в сфере компьютерной информации и высоких технологий.

В данной лекции рассмотрены вопросы понятия и значения преступлений в сфере высоких информационных технологий, а также основные направления преступной деятельности в информационной сфере, предложена их классификация. Представленные вопросы освещены на достаточном теоретическом уровне, использованы различные монографические исследования по рассматриваемой теме, а также нормативные источники.

В данной работе на основе изучения правоприменительной практики и литературы, рассмотрены актуальные на сегодняшний день теоретические и прикладные аспекты тактики и технологии собирания и использования информации при расследовании преступлений, в сфере компьютерной информации и высоких технологий. Кроме того, высказаны соображения и предложения по их разрешению в соответствующем законодательстве РК и

при правоприменительной работе сотрудников правоохранительных органов. Изучая эти проблемы и познания закономерностей этой деятельности, автор определенно выразил и дополнительно сформулировал ряд научных и практических выводов и рекомендаций по повышению эффективности правоотношений в целом и в частности по разрешению проблемных ситуаций по теме исследования.

Проводя изучение и анализ рассматриваемой темы, автор, в достаточной степени проявляет свое умение и приобретенные научно-исследовательские навыки, дает обобщение и выдвигает обоснованные выводы, оперируя материалами научных трудов, а также положениями нормативно-правовых актов. Учитывая изложенное, считаю, что лекция выполнена на достаточно хорошем теоретическом уровне и будет иметь примирительное значение в ходе практической деятельности.

МВД РЕСПУБЛИКИ КАЗАХСТАН
КАРАГАНДИНСКАЯ АКАДЕМИЯ МВД РК
им. БАРИМБЕКА БЕЙСЕНОВА
ЮРИДИЧЕСКИЙ ИНСТИТУТ

КАФЕДРА ДОСУДЕБНОГО РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ

ЛЕКЦИЯ

Тема №2 Деятельность следователя по проверке законности и обоснованности повода к началу досудебного расследования в сфере компьютерной информации и высоких технологий

Лекцию подготовил:
доцент кафедры досудебного расследования преступлений Карагандинской академии МВД РК им. Б. Бейсенова
майор полиции Кемпирова Ж.С.

Лекция обсуждена и одобрена на заседании кафедры досудебного расследования преступлений «___» _____ 2018 года Протокол №___.

Караганда – 2018 г.

Тема: Деятельность следователя по проверке законности и обоснованности повода к началу досудебного расследования в сфере компьютерной информации и высоких технологий

Вид занятия: Лекция Время - 1 час.

План лекции:

Введение

1. Следственные ситуации первоначального этапа расследования преступлений в сфере высоких информационных технологий в сфере компьютерной информации и высоких технологий.

2. Поводы к началу досудебного расследования в сфере компьютерной информации и высоких технологий.

Заключение

Цели занятия**:**

Методическая - подготовка и чтение лекции, выбор средств, обеспечивающих наглядное и полное усвоение дидактического содержания лекции.

Дидактическая - доведение до курсантов определенного комплекса учебной информации, определенного блока знаний на уровне и в объеме, предусмотренном программой и тематическим планом по вопросам организации и проведения следственных осмотров. Доведение материала с использованием методических и технических средств обучения, которые обеспечивают его усвоение.

Воспитательная - выработка психологической установки на возможность осознания, усвоения воспринимаемых научных знаний и понимания значения их реализации через соответствующие практические умения в будущей деятельности при проведении досудебного расследования.

Литература:

1. Аверьянова Т.В. Задачи компьютерно-технической экспертизы // Информатизация правоохранительных систем: Тезисы докладов междун. конф. В 2-х ч. М., 1998. 4.2.

2. Батурин Ю.М., Жодзишский А.М. Компьютерные правонарушения: криминализация, квалификация, раскрытие // Сов. государство и право, 1990. № 12. С.86-94.

3. Гортинский А.В., Пархоменко А.Н. Некоторые рекомендации по организации и проведению следственных действий при расследовании преступлений, совершенных с использованием печатающих средств персональных компьютеров // Материалы семинара: «Вопросы квалификации и расследования некоторых преступлений в сфере экономики». Саратов, 1998. 15-18 дек. С. 184-187.

4. КЕНЖЕТАЕВ Д.Т., КАЛИЕВ А.К., БАЛТАБАЕВ Т.Н. ПРИМЕРНЫЕ ОБРАЗЦЫ УГОЛОВНО-ПРОЦЕССУАЛЬНЫХ ДОКУМЕНТОВ ДОСУДЕБНОГО РАССЛЕДОВАНИЯ, КАРАГАНДА, 2014.

5. КРЫЛОВ В.В. ИНФОРМАЦИЯ КАК ЭЛЕМЕНТ КРИМИНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ // ВЕСТНИК МОСК. УН-ТА. СЕР. 11. ПРАВО. - М., 1998. - № 4. - С. 50-64.

6. РОССИНСКАЯ Е.Р ПРЕДМЕТ И ПРАКТИЧЕСКИЕ ПРИЛОЖЕНИЯ КОМПЬЮТЕРНО-ТЕХНИЧЕСКОЙ ЭКСПЕРТИЗЫ //ИНФОРМАТИЗАЦИЯ ПРАВООХРАНИТЕЛЬНЫХ СИСТЕМ: ТЕЗИСЫ ДОКЛАДОВ МЕЖДУНАР.КОНФ. В 2-Х Ч. М., 1998. Ч. 2.

7. Скоромников К.С. Расследование преступлений в сфере компьютерной информации // Руководство для следователей / Под ред. Н.А.Селиванова, В.А. Снеткова. М., 1997.

8. Толеубекова Б.Х. Компьютерная преступность: вчера, сегодня, завтра. Караганда, 1995.

9. ТЯЖИНА А.О., НОГАЙБАЕВА А.С. НОВЕЛЛЫ ДОСУДЕБНОГО РАССЛЕДОВАНИЯ ПО УПК РЕСПУБЛИКИ КАЗАХСТАН. УЧЕБНО-ПРАКТИЧЕСКОЕ ПОСОБИЕ (КРАТКИЙ АНАЛИЗ В СХЕМАХ). КАРАГАНДА, 2015.

10. ТЯЖИНА А.О., НОГАЙБАЕВА А.С., БЕЙСЕНБАЕВ А.Ж. ДОСУДЕБНОЕ ПРОИЗВОДСТВО ПО УГОЛОВНЫМ ДЕЛАМ: ОБРАЗЦЫ ПРОЦЕССУАЛЬНЫХ ДОКУМЕНТОВ, КАРАГАНДА, 2014.

11. Шурухнов Н.Г. Тактика следственного осмотра и освидетельствования Криминалистика: Курс лекций. М.: Эксмо. 2006.

Нормативные акты:

1. **Конституция Республики Казахстан** *(принята на республиканском референдуме 30 августа 1995 года), (с* изменениями и дополнениями *по состоянию на 10.03.2017 г.).*

2. Уголовно-процессуальный кодекс Республики Казахстан № 231-V-ЗРК *(с* изменениями и дополнениями *по состоянию на 09.01.2018 г.)*

3. Уголовный кодекс Республики Казахстан № 226-V-ЗРК *(с* изменениями и дополнениями *по состоянию на 09.01.2018 г.)*

4. Приказ Генерального Прокурора Республики Казахстан «Об утверждении правил приема и регистрации заявлений и сообщений об уголовных правонарушениях, а также ведения Единого реестра досудебных расследований» №89 от 19.09.2014г. с изм. и доп. от 10.08.2015 г. №99, 23.09.2016 №148.

5. Приказ Генерального прокурора Республики Казахстан от 22 сентября 2014 года №91 «Об утверждении Правил применения научно-технических средств фиксации хода и результатов следственных действий».

6. **Закон Республики Казахстан от 11.01.2007 N 217-III «Об информатизации».**

Введение

За последние годы многие государства в качестве приоритетной задачи выделили разработку и реализацию концепций и программ по переходу к информационному обществу. Вопросам использования достижений науки и техники в области информации уделял и продолжает уделять внимание и Президент РК Н. А. Назарбаев, неоднократно отмечая, что одним из условий успешного развития государства является процесс глобализации и научно-технического прогресса, особенно в развитии новых информационных и телекоммуникационных технологий.

Казахстан на сегодняшний день вступает на очередной этап научно технической революции – становление информационного общества, основными чертами которого являются ускорение темпов развития техники, автоматизация обработки информации, создание новых интеллектуальных технологий, превращение информации в важнейший глобальный ресурс человечества. Перечисленные факторы ведут к кардинальному, многоуровневому изменению культурной, политической, правовой жизни, социальной среды.

Вместе с тем, интеграция информационных технологий имеет место и в преступной среде, подрывая информационную безопасность государства. Информатизация современного общества привела к формированию новых видов преступлений с использованием устройств, в основе которых лежат высокоточные технологии их изготовления и функционирования, иными словами, это преступления, в которых используются высокие информационные технологии. Все вышесказанное и обусловило выбор темы дипломной работы и ее актуальность.

В данной лекции рассмотрены вопросы следственные ситуации первоначального этапа расследования преступлений в сфере высоких информационных технологий в сфере компьютерной информации и высоких технологий, а также поводы к началу досудебного расследования в сфере компьютерной информации и высоких технологий, а также приведен список использованных источников.

1. Следственные ситуации первоначального этапа расследования преступлений в сфере высоких информационных технологий в сфере компьютерной информации и высоких технологий.

Одна из особенностей преступлений в сфере высоких информационных технологий, как нами уже было отмечено, заключается в том, что они чрезвычайно латентны (около 90 %). Это связано с тем, что после совершения компьютерного преступления потерпевший обычно не выказывает особой заинтересованности в поимке преступника, а сам преступник, будучи пойман, всячески рекламирует свою деятельность (но это проявляется не во всех случаях). Возможные причины подобного поведения – жертва компьютерного преступления, как правило, совершенно убеждена, что затраты на его раскрытие (включая потери, понесенные в результате утраты, например, банком своей репутации) существенно превосходят уже причиненный ущерб, а сам преступник в результате огласки приобретает широкую известность в деловых и криминальных кругах.

Между тем раскрывать преступления, совершаемые в сфере высоких информационных технологий, сложно, т. к. нередко преступники прибегают к различным уловкам, маскируют свои преступные деяния многочисленными объективными и субъективными причинами, которые действительно могут иметь место. К ним, как правило, относятся:

-естественные: стихийные бедствия, природные явления (пожары, землетрясения, наводнения, ураганы, смерчи, тайфуны, циклоны и т. п.); самопроизвольное разрушение элементов, составляющих СВТ;

-обусловленные неумышленной деятельностью человека вследствие непреодолимых факторов.

Это ошибки в следующих случаях: при создании (изготовлении) СВТ (недочеты проектирования, в т. ч. системы защиты, кодирования информации, в изготовлении элементов СВТ); в процессе работы (эксплуатации) СВТ (неадекватность концепции обеспечения безопасности

СВТ; недочеты управления системой защиты, ошибки персонала, сбои и отказы оборудования и программного обеспечения, ошибки при производстве пусконаладочных и ремонтных работ).

Как уже установлено, что определение основных направлений расследования и особенности тактики отдельных следственных действий зависят от характера исходных данных. В связи с этим в юридической литературе неоднократно предпринимались попытки систематизации исходных данных, в результате чего появилось понятие исходной следственной ситуации.

Под исходной следственной ситуацией понимается объективно сложившаяся в первый период расследования его информационная среда, обстановка проведения и другие условия расследования, от которых зависит тактика и последовательность проведения первоначальных следственных действий, оперативно-розыскных и организационных мероприятий. По делам рассматриваемой категории можно выделить следующие исходные следственные ситуации:

1.Информация о причинах возникновения общественно опасных деяний, способе их совершения и личности правонарушителя отсутствует.

2.Имеются сведения о причинах возникновения преступления, способе его совершения, но нет сведений о личности преступника.

3.Известны причины возникновения преступления, способы его совершения и сокрытия, личность преступника и другие обстоятельства.

В первых двух следственных ситуациях обычно планируются и осуществляются следующие первоначальные следственные действия, оперативно розыскные и организационные мероприятия:

-допрос заявителя или лиц, на которых указано в исходной информации как на возможных свидетелей;

-решение вопроса о возможности задержания преступника с поличным и о необходимых в связи с этим мероприятиях;

-вызов необходимых специалистов для участия в осмотре места происшествия;

-осмотр места происшествия;

- проведение оперативно-розыскных мероприятий в целях установления причин совершения преступления, выявления лиц, виновных в его совершении, обнаружения следов и других вещественных доказательств;

-выемка и последующий осмотр средств электронно – вычислительной техники, предметов, материалов и документов (в т.ч. находящихся в электронной форме на машинных носителях информации), характеризующих производственную операцию, в ходе которой по имеющимся данным совершены преступные действия;

-допросы свидетелей (очевидцев);

-допросы подозреваемых (свидетелей), ответственных за данный уча сток работы, конкретную производственную операцию и защиту конфиденциальной информации;

-обыски на рабочих местах и по месту проживания подозреваемых;

-назначение программно-технической, радиотехнической, технической, бухгалтерской и иных экспертиз;

-дальнейшие действия, которые планируются с учетом дополнительной информации.

Для третьей следственной ситуации может быть предложена следующая программа расследования и действий следователя на первоначальном этапе:

- изучение поступивших материалов с позиций их полноты, соблюдения норм уголовно-процессуального законодательства и порядка передачи в органы следствия. При необходимости принятие мер к получению недостающей информации;

-возбуждение уголовного дела;

-вызов необходимых специалистов для участия в осмотре места происшествия;

-осмотр места происшествия;

-личные обыски задержанных, их рабочих мест и места проживания;

-допрос подозреваемых;

-выемка и осмотр вещественных и письменных доказательств;

-изъятие и осмотр подлинных документов, удостоверяющих личность задержанных, а также документов, характеризующих те производственные операции, в процессе которых допущены нарушения и преступные действия (в т. ч. и тех документов, которые находятся в электронной форме на машинных носителях информации);

-допрос лиц, названных в документах, переданных в следственные органы, как допустивших нарушения, ответственных за работу (де нежные средства, материальные ценности, услуги и т. п.) по фактам установленных нарушений;

-истребование, а при необходимости производство выемки нормативных актов и документов, характеризующих порядок и организацию работы в данном подразделении (в т. ч. с конфиденциальной информацией, бланками строгой отчетности, использование СВТ ит. п.);

-допрос свидетелей, причастных к соответствующим производственным операциям или подозреваемых в связях с лицами, совершившими преступные действия;

-анализ полученной информации и решение вопроса о необходимости назначения экспертиз, проведения ревизии или проверки, в т. ч. повторной (по каким позициям, за какой период и с участием каких специалистов).

При выполнении вышеуказанных программ следует учитывать особенности методики расследования конкретного вида преступления, о совершении которого выдвинуты версии. Учитывая конкретные обстоятельства, следователем могут быть выдвинуты и проверены следующие общие версии:

1.Преступление совершено сотрудником данного учреждения либо лицом, имеющим свободный доступ к компьютерной технике.

2.Преступление совершено сторонним лицом, входящим в круг родственников, друзей, знакомых сотрудников учреждений.

3.Преступление совершено группой лиц по предварительному сговору или организованной группой с участием сотрудника данного учреждения либо лица, имеющего свободный доступ к компьютерной технике и в совершенстве владеющего навыками работы с ней.

4.Преступление совершено лицом или группой лиц, не связанных с деятельностью учреждения и не представляющих ценность компьютерной информации.

5.Преступление действительно имело место при тех обстоятельствах, которые вытекают из первичных материалов.

6.Ложное заявление о преступлении.

Приведенный перечень следственных версий является общим, и в зависимости от конкретной ситуации может быть расширен. При этом типичными частными версиями являются версии:

-о личности преступника (преступников);

-о способах совершения преступления;

-об обстоятельствах, при которых было совершено преступление;

-о размерах ущерба, причиненного преступлением.

Так, рассматривая главу 7 УК РК, можно отметить, что данная норма фактически предусматривает ответственность за совершение трех составов преступлений: неправомерный доступ к охраняемой законом компьютерной информации; создание, использование и распространение вредоносных программ для ПК; нарушение правил эксплуатации ПК, системы ПК или их сети. Рассмотрим особенности расследования данных преступлений более подробно.

Данную необходимость обуславливает дефицит криминалистических рекомендаций по методике и тактике расследования указанных составов преступлений, в связи с чем, представляется обоснованным предложить методические рекомендации и схемы расследования указанных преступлений, которые будет выглядеть следующим образом.

1. Первоначальный этап расследования неправомерного доступа к охраняемой законом компьютерной информации.

Признаками совершения указанного состава могут являться:

-появление в компьютере фальшивых или искаженных данных;

-не обновление в течение длительного времени в автоматизированной информационной системе кодов, паролей и других защитных средств;

-частые сбои в процессе работы компьютеров;

-участившиеся жалобы клиентов компьютерной системы или сети;

-осуществление сверхурочных работ без видимых на то причин;

-немотивированные отказы некоторых сотрудников, обслуживающих компьютерные системы или сети, от отпусков;

-неожиданное приобретение сотрудником домашнего дорогостоящего компьютера;

-чистые дискеты либо диски, принесенные на работу сотрудниками компьютерной системы под сомнительными предлогами;

-участившиеся случаи перезаписи отдельных данных без серьезных на то причин;

-чрезмерный интерес отдельных сотрудников к содержанию чужих распечаток (листингов), выходящих из принтеров.

При наличии указанных признаков либо иного сигнала о совершенном преступлении следует установить:

1.Факт неправомерного доступа к компьютерной информации.

2.Место несанкционированного проникновения в компьютерную систему или сеть.

3.Время несанкционированного доступа.

4.Надежность средств защиты компьютерной информации.

5.Способ совершения несанкционированного доступа.

6. Круг лиц, совершивших неправомерный доступ

7. Виновность и мотивы лиц, совершивших неправомерный доступ к компьютерной информации.

8.Наличие последствий преступления.

9.Наличие обстоятельств, способствовавших преступлению.

Факт неправомерного доступа к информации в компьютерной систем или сети обычно первыми обнаруживают сами же пользователи информационной системы. Однако они не всегда своевременно сообщают об этом правоохранительным органам. Особенно это относится к руководителям кредитно-финансовых и банковских учреждений, которые не желают вызывать у клиентов сомнения в надежности своих учреждений. Они также опасаются, что по этому факту начнется проведение проверок, ревизий и экспертиз, могущих раскрыть их финансовые и иные служебные тайны вскрыть другие серьезные недостатки.

Факт несанкционированного доступа в сети Интернет вскрывается уже после того, как фирма-провайдер присылает счет о предоставленных услугах на сумму, явно превышающую допустимые пределы работы зарегистрированного пользователя. Кроме того, время работы также не соответствует действительности. В результате этого официально зарегистрированный пользователь отказывается платить за услуги, которыми не пользовался, а фирма-провайдер соответственно несет убытки. Возможны и другие варианты развития событий. Например, в случае если официально зарегистрированный пользователь превышает данные ему полномочия и вносит изменения в страницы, принадлежащие другим пользователям.

Установить факт неправомерного доступа к компьютерной информации можно и в процессе проведения проверочных мероприятий в в ходе проведения ревизий, судебных экспертиз, иных следственных действий по уголовным делам, находящимся в производстве следователей, а также при проведении оперативно-розыскных мероприятий.

Установление места несанкционированного доступа в компьютерную систему или сеть может вызывать определенные трудности, поскольку по

делам данной категории может быть несколько мест совершения одного преступления.

Чаще обнаруживается место неправомерного доступа к компьютерной информации по преступлениям, связанным с хищением денежных средств. На всех этих местах должны были остаться следы одного преступления. Однако на первоначальном этапе расследования установить физический адрес ввода фальшивых документов так и не удалось. По мнению специалистов в той ситуации такой ввод мог быть осуществлен с любого рабочего места, имеющего телекоммуникационную связь с компьютерами. Тем более что эксплуатируемый программный комплекс фактически был открыт для несанкционированного ввода, обновления (корректировки, изменения) и обработки любой информации. Поэтому при обнаружении неправомерного доступа к информации в компьютерной системе или сети следует выявить все места, где расположены компьютеры, имеющие единую телекоммуникационную связь.

Проще обстоит дело, когда совершен несанкционированный доступ к отдельному изолированному компьютеру, находящемуся в одном помещении. Однако и в этом случае необходимо учитывать, что компьютер может находиться в одном помещении, а информация на машинных носителях – в другом. Следовательно, надо выявить и это место.

Труднее устанавливать место непосредственного использования технических средств, для несанкционированного доступа (особенно мобильных), не входящих в данную компьютерную систему или сеть. В данном случае следует установить и место хранения информации на машинных носителях либо в виде распечаток, добытых в результате неправомерного доступа к компьютерной системе или сети.

Установление времени несанкционированного доступа. Любой современный компьютер имеет встроенный таймер, отражающий информацию о дне недели, дате, часе и минуте в реальном времени. Естественно, что его точность определяется правильностью первоначальной установки времени, выбором правильного часового пояса, а также переходом на летнее или зимнее время. Время последней модификации файла отражается в его атрибутах и достаточно просто может быть выяснено с помощью программ общесистемного назначения.

Кроме того, при входе в систему или сеть время работы на компьютере любого пользователя автоматически фиксируется в специальных системных файлах. Исходя из этого, точное время доступа можно установить путем следственного осмотра работающего компьютера либо распечаток ил дискет. Время неправомерного доступа к компьютерной информации можно также установить путем допроса свидетелей из числа сотрудников данной компьютерной системы, выясняя у них, в какое время каждый из них работал на компьютере, если оно не было зафиксировано автоматически.

Установление способа совершения несанкционированного доступа Конкретный способ несанкционированного доступа к компьютерной информации можно установить в процессе допроса свидетелей из числа лиц

обслуживающих эту систему, или ее разработчиков, а также путем производства судебно-технологической экспертизы.

Для установления способа и отдельных обстоятельств механизма неправомерного доступа к компьютерной информации может быть проведен следственный эксперимент с целью проверки возможности преодоления средств защиты компьютерной системы одним из вероятных способов.

При установлении надежности средств защиты компьютерной информации необходимо, прежде всего, установить, предусмотрены ли вообще в данной компьютерной системе меры защиты от несанкционированного доступа к определенным файлам. Это можно выяснить при допросе разработчиков и пользователей, а также при изучении проектной документации и соответствующих инструкций по эксплуатации данной системы. В них должны содержаться специальные разделы, относящиеся к мерам защиты информации, с подробным описанием порядка допуска пользователей к определенным категориям данных (т. е. разграничением их полномочий), организации за доступом контроля, конкретных методов защиты информации (аппаратных, программных, криптографических, организационных и пр.).

Законодательством предусмотрены обязательная сертификация средств защиты систем обработки и хранения информации с ограниченным доступом, обязательное лицензирование всех видов деятельности в области проектирования и производства таких средств. Разработчики, как правило, гарантируют надежность своих средств, при условии соблюдения установленных требований. Поэтому в процессе расследования требуется установить: во-первых, имеется ли лицензия на производство средств защиты информации от несанкционированного доступа, используемых в данной компьютерной системе; во-вторых, соответствуют ли их параметры выданному сертификату. Для проверки такого соответствия назначается судебно технологическая экспертиза.

При исследовании объекта, где совершено преступление, необходимо выяснить;

- технические и конструктивные особенности помещений, связанные с установкой и эксплуатацией вычислительной техники (специальное оборудование полов, потолков и окон, каналы кабельных и вентиляционных шахт, установка и фактическое состояние устройств кондиционирования воздуха, система электропитания и иные особенности);
- особенности установки средств комплекса вычислительной техники (сосредоточены в одном месте или расположены в различных помещениях);
- способы связи компьютеров между собой посредством локально вычислительной сети, устройств телекоммуникации и состояние линий связи;
- структуру, конфигурацию сети ПК и внешних информационных связей;
- режим работы.

Установление лиц, совершивших неправомерный доступ к компьютерной информации. Опрос респондентов из числа лиц, обладающих специальными знаниями в сфере высоких технологий, показывает, что чем хитрее и сложнее в техническом плане способ такого проникновения, тем легче «вычислить» преступника, поскольку круг специалистов, обладающих такими способностями, сужается.

Причастность конкретного лица к несанкционированному доступу к компьютерной информации помимо свидетельских показаний может быть установлена также и по материально-фиксированным отображениям, обнаруженным при производстве следственного осмотра компьютера и его компонентов. Это могут быть следы пальцев рук, оставленные на их поверхности, отдельные записи на внешней упаковке дискет, дисков, где обычно остаются заметки о характере записанной на них информации, а порой и о том, кому принадлежат эти носители информации; следы обуви и другие материальные следы. Для их исследования назначаются традиционные криминалистические экспертизы, дактилоскопические, почерковедческие, трассологические, а также техническое исследование документов.

Чтобы выявить лиц, обязанных обеспечивать соблюдение режима доступа к компьютерной системе или сети, необходимо, прежде всего, ознакомиться с имеющимися инструкциями, устанавливающими полномочия Должностных лиц, ответственных за защиту информации, после чего следует их допросить. При допросе лиц, обслуживающих компьютерную систему, можно установить: кто запускал нештатную программу, было ли это зафиксировано каким-либо способом? Следует также выяснить, кто увлекался программированием (возможно, кто-то учится или учился на компьютерных курсах).

При наличии достаточных оснований у лиц, подозреваемых в неправомерном доступе к компьютерной информации, производится обыск, в процессе которого могут быть обнаружены компьютерная техника, различные записи, дискеты, содержащие сведения, могущие иметь отношение к расследуемому событию, например коды, пароли, идентификационные номера пользователей конкретной компьютерной системы, а также данные о ее пользователях.

Установление виновности и мотивов лиц, совершивших неправомерный доступ к компьютерной информации можно только по совокупности результатов всех процессуальных действий. Решающими из них являются допросы свидетелей, подозреваемых, потерпевших, заключения судебных экспертиз, результаты обыска.

При установлении последствий неправомерного доступа к компьютерным системам или сетям необходимо, прежде всего, выявить - в чем выражены вредные последствия такого доступа (хищение денежных средств или материальных ценностей, завладение компьютерными программами, информацией путем изъятия ее машинных носителей либо копирования, а также незаконное изменение, уничтожение, блокирование

или вывод из строя компьютерного оборудования, введение в компьютерную систему заведомо ложной информации или компьютерного вируса и пр.). Хищение денежных средств, в банковских электронных системах зачастую обнаруживаются самими работниками банков или в результате проведения оперативно розыскных мероприятий. Конкретная сумма хищения устанавливается судебно-бухгалтерской экспертизой.

При выявлении обстоятельств, способствовавших неправомерному доступу к компьютерной информации, формируется целостное представление о данных обстоятельствах. С этой целью изучаются документы, относящиеся к защите информации, и заключение технологической экспертизы. Если по факту неправомерного доступа проводилось внутреннее (служебное) расследование, то его выводы также могут оказаться полезны при выявлении причин и условий его совершения.

2. Первоначальный этап расследования создания, использования распространения вредоносных программ для ПК.

Признаков совершения данных преступлений нет. Как правило, обнаружить можно лишь их результаты – сбои в процессе работы компьютерной системы или сети, жалобы клиентов и т. п.

При расследовании создания вредоносных программ для ПК подлежат установлению следующие обстоятельства:

-факт создания вредоносной программы для ПК;

-способ создания вредоносной программы;

-факт использования и распространения вирусной программы;

-предназначение вредоносной программы и механизм действия;

-место, время создания, используемое для этого программное обеспечение и компьютерная техника;

-круг лиц, виновных в создании, использовании и распространении вирусных программ для ПК;

-цель и мотив создания программы;

-осведомленность лица, использовавшего программу, о ее вредоносных свойствах, наличие или отсутствие умысла на использование и распространение данной программы;

-характер и размер вреда, причиненного данным преступлением;

-наличие обстоятельств, способствовавших совершению расследуемого преступления.

Вредоносная программа, как правило, обнаруживается в момент, когда уже явно проявляются последствия ее применения. Вместе с тем она может быть обнаружена и на машинных носителях информации, в частности, путем изучения информации обложки компакт-диска. Кроме того, выявляется она также в процессе антивирусной проверки, производимой пользователем компьютерной системы перед началом работы на компьютере, особенно часто практикуемой при использовании чужих машинных носителей или получении электронной почты.

Наибольшую сложность для расследования представляет совершение преступления в условиях неочевидности. Здесь основными направлениями расследования должны быть:

- пресечение противоправной деятельности;

- выяснение механизма преступления и уточнение отдельных его обстоятельств;

- установление лица, распространяющего вредоносную программу;

- получение сведений о личности потерпевших;

- установление суммы материального ущерба;

-сбор доказательств о причастности установленного лица к каждым выявленным эпизодам преступной деятельности;

-выяснение причин и условий, способствовавших совершению преступления;

- получение характеризующего личность подозреваемого материала.

Наиболее распространенными условиями, способствовавшими совершению данного преступления, являются: использование не сертифицированного программного обеспечения; использование нелегальных копий программ для ПК; отсутствие резервных копий программ и системных файлов; отсутствие учета и контроля за доступом к компьютерным системам- использование компьютеров не по назначению (для компьютерных игр обучения посторонних, написания программ лицами, в обязанности которых это не входит); нерегулярное проведение антивирусной проверки компьютерной системы и машинных носителей, и др.

3. Первоначальный этап расследования нарушения правил эксплуатации ПК, системы ПК или их сети.

При расследовании нарушения правил эксплуатации ПК, системы ПК или их сети подлежат установлению следующие обстоятельства:

1) факт преступного нарушения правил эксплуатации ПК, системы ПК или их сети;

2) место и время совершения преступления;

3) характер информации, являющейся предметом посягательства;

4) способ и механизм нарушения правил эксплуатации ПК, системы ПК или их сети;

5) характер и размер ущерба, причиненного преступлением;

6) виновность лица;

7) обстоятельства, способствовавшие совершению преступления.

В расследовании данной категории преступлений одной из главных проблем становится установление самого факта нарушения правил эксплуатации ПК. Здесь необходимо, прежде всего, установить факт существования конкретных правил эксплуатации ПК на данном объекте, к которым может относиться: техническая документация на приобретаемые компьютеры; конкретные принимаемые в определенном учреждении или организации, оформленные нормативно и подлежащие доведению до сведения соответствующих работников правила внутреннего распорядка;

требования по сертификации компьютерных сетей и оборудования; должностные инструкции конкретных сотрудников; правила пользования компьютерными сетями.

Факт нарушения правил эксплуатации ПК обычно становится известным в первую очередь непосредственным владельцам и пользователями компьютерной системы или сети после обнаружения ими отсутствия необходимой информации или существенного изменения ее, когда это уже отрицательно отразилось на основной деятельности предприятия, организации учреждения.

Для установления конкретного правила эксплуатации ПК, нарушение привело к вредным последствиям, следователю целесообразно допросить всех лиц, работавших на ПК или обслуживающих компьютерное оборудование в тот период, когда это произошло (с участием специалиста). При допросе необходимо выяснить: функциональные обязанности конкретного сотрудника при работе с ПК (либо оборудованием к ней), какими правилами они установлены, имеет ли данное лицо доступ к ПК, их системе или сети; какую конкретно работу на ПК и в каком порядке данный сотрудник выполнял; когда произошел факт уничтожения, блокирования, модификации компьютерной информации или наступили иные вредные последствия; какие неполадки в компьютерной системе были обнаружены при работе на ПК, не было ли при этом каких-то сбоев, которые могли бы причинить существенный вред компьютерной информации; какой установленный порядок при работе с компьютером мог быть нарушен в данной ситуации либо они явились следствием непредвиденных обстоятельств, если да, то с какими конкретно.

Факт нарушения правил эксплуатации ПК может быть установлен по материалам служебного расследования. Поступившие следователю материалы подлежат тщательному и всестороннему изучению. Следователь должен усмотреть в них наличие достаточных данных, указывающих на признаки преступления.

Конкретное место нарушения правил эксплуатации ПК устанавливается при осмотре рабочих мест пользователей ПК, компьютерной системы или сети. Осмотру подлежат все компьютеры, подключенные к сети ПК. Цель - установить местонахождение компьютера, эксплуатация которого привела к вредным последствиям в результате преступного нарушения определенных правил его использования.

Необходимо различать место нарушения и место наступления вредоносных последствий. Они не всегда совпадают, особенно если идет речь о нарушении правил эксплуатации компьютерных сетей, которые, как известно, представляют собой объединение отдельных персональных компьютеров, расположенных на расстоянии друг от друга, и предназначены для использования информации и обращении к периферийному оборудованию (принтерам, прокси-серверам и пр.). Осмотру подлежат: рабочие станции локальных вычислительных сетей, в качестве которых применяются персональные компьютеры, объединенные внутри здания

пределах небольшой территории; файловый сервер, обслуживающий рабочие станции и осуществляющий совместное использование файл размещаемых на его дисках; принтеры, которые тоже могут находиться далеко от того места, где расположена рабочая станция.

Таким образом, основная задача осмотров рабочих мест – установить, где расположена рабочая станция, эксплуатация которой осуществлялась грубым нарушением правил информационной безопасности. В первую очередь необходимо обратить внимание на рабочие станции, имеющие собственные дисководы. У них значительно больше возможностей для преступных нарушений. Они, к примеру, имеют возможность копировать данные с файлового сервера на свою дискету или использовать дискеты с различными программами, в т. ч. с компьютерными вирусами, и подвергать опасности целостность информации, содержащейся в центральных файловых серверах, чего не имеют бездисковые рабочие станции. Таков один из важных признаков, по которому можно установить место совершения преступления.

2. Поводы к началу досудебного расследования в сфере компьютерной информации и высоких технологий.

Собирание значимой информации в вычислительной сети имеет свои особенности. В первую очередь необходимо установить общее количество компьютеров и их распределение по другим помещениям, а также количество и тип используемых серверов и рабочих мест. Далее важно выяснить тип используемой сетевой операционной системы и состав прикладного программного обеспечения, используемого в вычислительной сети. Следует также установить факт наличия резервных копий данных и места их хранения. Особое внимание должно уделяться выявлению выхода в другие, в том числе и глобальные, сети; установлению возможностей использования коммуникационных средств для связи с удаленными пользователями, другими организациями (фирмами), частными лицами.

В это же время определяются принятые в организации мероприятия по защите информации и наличие выхода в Интернет. В случае использования телефонной линии для связи с другими сетями обеспечить отключение телефона; по возможности удалить из помещения все взрывчатые, едкие и легковоспламеняющиеся материалы.

Для обеспечения сохранности информации необходимо: предотвратить отключение энергоснабжения организации, обеспечив охрану распределительного щита;

- запретить работникам организации и прочим лицам производить какие-либо манипуляции с компьютерными средствами;
- предупредить всех участников следственного действия о недопустимости самостоятельных манипуляций с компьютерными средствами;

▪ точно установить местоположение серверов; определить местоположение компьютеров, подключенных к вычислительной сети (иногда помогает электропроводка: достаточно проследить трассы кабелей или специальных коробов для защиты кабелей).

Следственная группа должна иметь физическую возможность одновременно занять все помещения, в которых находятся компьютеры, входящие в сеть. Наличие средств удаленного доступа позволяет оперативно манипулировать информацией в сети любым компьютером, входящим в нее.
Завершающим этапом осмотра, обыска или выемки по делам, сопряженным с использованием компьютерных технологий, являются фиксация и изъятие компьютерных средств. От того, как произведены изъятие, транспортировка и хранение этих объектов, часто зависит их доказательственное значение. Все изъятые системные блоки и другие устройства должны быть упакованы и опечатаны таким образом, чтобы исключить возможность их повреждения, включения в сеть и разборки. В протоколе должны быть точно отражены место, время и внешний вид изымаемых предметов и документов. При изъятии компьютеров и носителей данных их следует упаковывать и опечатывать.

Одним из следствий массовой компьютеризации в Казахстане явились преступления в сфере компьютерной информации. Интеграция современных информационных технологий практически во все области человеческой деятельности привела к тому, что с помощью компьютерных средств и систем совершаются «традиционные» преступления (например, присвоение, кража, мошенничество, фальшивомонетничество, лжепредпринимательство и др.). Компьютерные технологии используются с целью: фальсификации платежных документов; хищения наличных и безналичных денежных средств путем перечисления на фиктивные счета; отмывания денег; вторичного получения уже произведенных выплат; совершения покупок с использованием фальсифицированных или похищенных электронных платежных средств; продажи секретной информации и проч.

Преступления, сопряженные с использованием компьютерных технологий, представляют серьезную угрозу для любой располагающей компьютерной техникой организации. При этом наряду с высокой степенью риска ей наносится и значительный материальный ущерб: вывод из строя электронно-вычислительной системы в результате возникновения нештатной технической ситуации или преступления может привести даже самый крупный банк к полному разорению за четверо суток, а более мелкое учреждение – за сутки.

Преступления, совершаемые с использованием компьютерных средств и систем, принято называть компьютерными преступлениями. Эта дефиниция должна употребляться не в уголовно-правовом аспекте, где это только затрудняет квалификацию деяния, а в криминалистическом, поскольку связана не с квалификацией, а именно со способом совершения и сокрытия преступления и, соответственно, с методикой его раскрытия и расследования.

Компьютерная информация применительно к процессу доказывания может быть определена как фактические данные, обработанные компьютерной системой и (или) передающиеся по телекоммуникационным каналам, а также доступные для восприятия, на основе которых в определенном законом порядке устанавливаются обстоятельства, имеющие значение для правильного разрешения уголовного или гражданского дела. Источниками компьютерной информации служат:

- машинная распечатка;
- накопители на магнитных, оптических и иных носителях;
- база данных (фонд) оперативной памяти ЭВМ или постоянного запоминающего устройства.

Для совершения компьютерных преступлений злоумышленники используют:

- подбор паролей, ключей и другой идентификационной или аутентификационной информации;
- подмену IP-адресов пакетов, передаваемых по Интернету или другой глобальной сети, так, что они выглядят поступившими изнутри сети, где каждый узел доверяет адресной информации другого;
- инициирование отказа в обслуживании – воздействие на сеть или отдельные ее части с целью нарушения порядка штатного функционирования;
- прослушивание и расшифровку трафика с целыо сбора передаваемых паролей, ключей и другой идентификационной или аутентификационной информации;
- сканирование с использованием программ, последовательно перебирающих возможные точки входа в систему (например, номера TCP-портов или телефонные номера) с целью установления путей и возможностей проникновения;
- подмену, навязывание, уничтожение, переупорядочивание или изменение содержимого данных (сообщений), передаваемых по сети, и др.

Известны следующие способы совершения компьютерных преступлений:

а) методы перехвата: подключение к компьютерным сетям; поиск данных, оставленных пользователем после работы с компьютером (физический поиск – осмотр содержимого мусорных корзин и сбор оставленных за ненадобностью распечаток, деловой переписки и т. п.; электронный поиск – последние из сохраненных данных обычно не стираются после завершения работы), для обнаружения паролей, имен пользователей и проч.;

б) методы несанкционированного доступа: подключение к линии законного пользователя через Интернет, через слабые места в защите системы, при системной поломке либо под видом законного пользователя (физический вариант – пользователь выходит ненадолго, оставляя терминал в активном режиме). Системы, не обладающие средствами аутентичной идентификации (по отпечаткам пальцев, голосу и т. п.), оказываются без

защиты против этого приема. Простейший путь – получение идентифицирующих шифров законных пользователей либо использование особой программы, применяемой в компьютерных центрах при сбоях в работе ЭВМ;

в) методы манипуляции:

- подмена данных – изменение или введение новых данных осуществляется, как правило, при вводе или выводе информации с ЭВМ;
- манипуляции с пультом управления компьютера – механическое воздействие на технические средства машины, что создает возможность манипулирования данными;
- «троянский конь» – тайный ввод в чужую программу команд, позволяющих, не изменяя работоспособность программы, осуществить определенные функции. Этим способом преступники обычно отчисляют на свой счет определенную сумму с каждой операции. Вариантом является «салями», когда отчисляемые суммы малы и их потери практически незаметны (например, по 10 центов с операции), а накопление осуществляется за счет большого количества операций;
- «бомба» – тайное встраивание в программу набора команд, которые должны сработать (или срабатывать каждый раз) при определенных условиях либо в определенные моменты времени (например, вирус «Чернобыль», который активизируется 26 апреля – в день аварии на Чернобыльской АЭС);
- моделирование процессов, в которые преступники хотят вмешаться, и планируемые методы совершения и сокрытия посягательства для оптимизации способа преступления. Одним из вариантов является реверсивная модель, когда создается модель конкретной системы, в которую вводятся реальные исходные данные и учитываются планируемые действия. Из полученных правильных результатов подбираются правдоподобные желательные. Затем путем прогона модели назад, к началу, выясняют результаты и устанавливают, какие манипуляции с исходными данными нужно проводить. Таких операций может быть несколько. После этого остается только осуществить задуманное.

Как правило, компьютерные преступления совершаются с помощью того или иного сочетания приемов.

Личность преступника отличается целым рядом особенностей:

- четко формулирует любую профессиональную задачу, но часто характеризуется хаотическим поведением в быту;
- обладает развитым формально-логическим мышлением, которое зачастую подводит в реальной жизни;
- стремится к точности, четкости и однозначности в языке, постоянно задает уточняющие вопросы и переспрашивает, что вызывает раздражение собеседника;
- постоянно использует компьютерный жаргон, малопонятный непосвященным.

Отечественные правонарушители в сфере компьютерной информации могут быть разделены на две возрастные группы: первая – 14-20 лет, вторая – с 21 года и старше.

Представители первой возрастной группы – это старшие школьники или студенты младших курсов высших или средних специальных учебных заведений, которые активно ищут пути самовыражения и находят их, погружаясь в виртуальный мир компьютерных сетей. При этом чаще всего ими движет скорее любопытство и желание проверить свои силы, нежели корыстные мотивы. К числу особенностей, указывающих на совершение компьютерного преступления лицами рассматриваемой категории, можно отнести: отсутствие целеустремленной, продуманной подготовки к преступлению; оригинальность способа; непринятие мер к сокрытию преступления; факты немотивированного озорства.

Компьютерные преступники, входящие во вторую возрастную группу, – это уже вполне сформировавшиеся личности, обладающие высокими профессиональными и устойчивыми преступными навыками, а также определенным жизненным опытом. Совершаемые ими деяния носят осознанный корыстный характер, при этом, как правило, предпринимаются меры по противодействию раскрытию преступления. Преступления, которые носят серийный, многоэпизодный характер, обязательно сопровождаются действиями по сокрытию. Это обычно высококвалифицированные специалисты с высшим математическим, инженерно-техническим или экономическим образованием, входящие в организованные преступные группы и сообщества, прекрасно оснащенные технически (нередко специальной оперативной техникой). Особую опасность с точки зрения совершения преступлений в сфере компьютерной информации представляют профессионалы в области новых информационных технологий. На долю этой группы приходится большинство особо опасных должностных преступлений, совершаемых с использованием средств компьютерной техники, присвоений денежных средств в особо крупных размерах, мошенничества и проч.

Среди мотивов и целей совершения посягательств можно выделить:

- корыстные (присвоение денежных средств и имущества);
- политические (шпионаж, деяния, направленные на подрыв финансовой и денежно-кредитной политики, валютной системы страны);
- исследовательский интерес;
- хулиганские побуждения и озорство;
- месть и иные побуждения.

Сведения о потерпевшей стороне. Потерпевших можно подразделить на три основные группы: собственники компьютерной системы; клиенты, пользующиеся их услугами; иные лица.

Потерпевший, особенно относящийся к первой группе, часто неохотно сообщает (или вовсе не сообщает) правоохранительным органам о преступных фактах в сфере движения компьютерной информации по следующим причинам:

- из-за некомпетентности сотрудников правоохранительных органов в данном вопросе;
- боязни, что убытки от расследования превысят размер причиненного ущерба и к тому же будет подорван авторитет фирмы;
- боязни раскрытия в ходе судебного разбирательства системы безопасности организации;
- боязни выявления собственных незаконных действий; боязни должностных лиц, что одним из итогов расследования станут выводы об их профессиональной непригодности (некомпетентности);
- из-за правовой неграмотности;
- из-за непонимания истинной ценности имеющейся информации.

В компьютере информация может находиться непосредственно в оперативном запоминающем устройстве (ОЗУ) при выполнении программы, в ОЗУ периферийных устройств и на внешних запоминающих устройствах (ВЗУ).

Наиболее эффективным и простым способом фиксации данных из ОЗУ является распечатка на бумагу информации, появляющейся на дисплее.

Если компьютер не работает, информация может находиться в ВЗУ и других компьютерах информационной системы или в «почтовых ящиках» электронной почты или сети ЭВМ.

Необходимо произвести детальный осмотр файлов и структур их расположения; лучше это осуществить с участием специалиста в лабораторных условиях или на рабочем месте следователя.

Следует обращать внимание на поиск так называемых «скрытых» файлов и архивов, где может храниться важная информация.

Периферийные устройства ввода-вывода могут также некоторое время сохранять фрагменты программного обеспечения и информации, однако для вывода этой информации необходимы глубокие специальные познания.

Осмотр компьютеров и изъятие информации производится в присутствии понятых, которые расписываются на распечатках информации, изготовленных в ходе осмотра.

ПОИСК И ИЗЪЯТИЕ ИНФОРМАЦИИ И СЛЕДОВ ВОЗДЕЙСТВИЯ НА НЕЕ ВНЕ ЭВМ

В ходе осмотров по делам данной категории могут быть обнаружены и изъяты следующие виды важных документов, которые могут стать вещественными доказательствами по делу:

а) документы, носящие следы совершенного преступления, - телефонные счета, пароли и коды доступа, дневники связи и пр.;

б) документы со следами действия аппаратуры. Всегда следует искать в устройствах вывода (например, в принтерах) бумажные носители информации, которые могли остаться внутри их в результате сбоя в работе устройства;

в) документы, описывающие аппаратуру и программное обеспечение;

г) документы, устанавливающие правила работы с ЭВМ, нормативные акты, регламентирующие правила работы с данной ЭВМ, системой, сетью, доказывающие, что преступник их знал и умышленно нарушал;

д) личные документы подозреваемого или обвиняемого.

ИСПОЛЬЗОВАНИЕ СПЕЦИАЛЬНЫХ ПОЗНАНИЙ И НАЗНАЧЕНИЕ ЭКСПЕРТИЗ

Лицо, осуществляющее досудебное расследование не в состоянии отслеживать все технологические изменения в данной области. Поэтому специалисты крайне необходимы для участия в обысках, осмотрах, выемках.

Поиск таких специалистов следует проводить на предприятиях и в учреждениях, осуществляющих обслуживание и эксплуатацию компьютерной и коммуникационной техники, в учебных и научно-исследовательских организациях.

Специалисты, привлекаемые в качестве экспертов, могут оказать действенную помощь при решении следующих вопросов (примерный список):

1. Какова конфигурация и состав компьютерных средств и можно ли с помощью этих средств осуществить действия, инкриминируемые обвиняемому?

2. Какие информационные ресурсы находятся в данной ЭВМ?

3. Не являются ли обнаруженные файлы копиями информации, находившейся на конкретной ЭВМ?

4. Не являются ли представленные файлы с программами, зараженными вирусом, и если да, то каким именно?

5. Не являются ли представленные тексты на бумажном носителе записями исходного кода программы, и каково назначение этой программы?

6. Подвергалась ли данная компьютерная информация уничтожению, копированию, модификации?

7. Какие правила эксплуатации ЭВМ существуют в данной информационной системе, и были ли нарушены эти правила?

8. Находится ли нарушение правил эксплуатации в причинной связи с уничтожением, копированием, модификацией?

Большую помощь в расследовании могут оказать специалисты зональных информационно-вычислительных центров региональных УВД МВД России. Следует иметь в виду, что в системе МВД начато производство так называемых программно-технических экспертиз.

Программно-технической экспертизой (ПТЭ) решаются следующие задачи:

1) распечатка всей или части информации, содержащейся на жестких дисках компьютеров и на внешних магнитных носителях, в том числе из нетекстовых документов;

2) распечатка информации по определенным темам;

3) восстановление стертых файлов и стертых записей в базах данных, уточнение времени стирания и внесения изменений;

4) установление времени ввода в компьютер определенных файлов, записей в базы данных;

5) расшифровка закодированных файлов и другой информации, преодоление рубежей защиты, подбор паролей;

6) выяснение каналов утечки информации из ЛВС, глобальных сетей и распределенных баз данных;

7) установление авторства, места подготовки и способа изготовления некоторых документов;

8) выяснение технического состояния и исправности СКТ.

Наряду с этими основными задачами при проведении ПТЭ могут быть решены и некоторые вспомогательные задачи:

1) оценка стоимости компьютерной техники, периферийных устройств, магнитных носителей, программных продуктов, а также проверка контрактов на их поставку;

2) установление уровня профессиональной подготовки отдельных лиц в области программирования и работы с СКТ;

3) перевод документов технического содержания.

В связи с тем, что при осмотре ЭВМ и носителей информации производится изъятие различных документов, в ходе расследования возникает необходимость в назначении криминалистической экспертизы для исследования документов.

Дактилоскопическая экспертиза позволит выявить на документах, частях ЭВМ и машинных носителях следы пальцев рук причастных к делу лиц.

Заключение

Развитие информационных технологий и аппаратно-программных комплексов преобразования информации привело к появлению беспрецедентных по масштабам и глобальных по географии проявлений угроз безопасности информации. Утеря либо нежелательное распространение информации, составляющей государственную, коммерческую или личную тайну – одна из основных сегодняшних угроз. Избежать этой угрозы можно путем разработки и последовательной реализации целенаправленной политики в этой сфере, причем эффективной и действенной эта политика будет только в том случае, если она будет опираться на взвешенную и обоснованную методологическую базу.

Раскрытие и расследование преступлений в сфере компьютерной информации, а также таких «традиционных» преступлений, как: присвоение, мошенничество, фальшивомонетничество, лжепредпринимательство и др., когда компьютерные средства используются для совершения и сокрытия преступлений невозможно без привлечения специальных познаний в области современных информационных технологий.

В целом система доказательств по делам о компьютерных преступлениях подчиняется общей логике доказывания в пределах действующего уголовно-процессуального законодательства. Однако специфика самой электронно-вычислительной техники налагает определенные особенности на деятельность по собиранию доказательств при расследовании названных деяний.

Компьютерная информация является разновидностью информации вообще, ее видовым понятием. Поэтому все признаки, характерные для понятия информации, присущи в равной степени и понятию компьютерной информации. В тоже время компьютерная информация имеет существенные специфические особенности, которые позволяют выделить ее в самостоятельное понятие.

Использование компьютерной техники в преступных целях может осуществляться в следующих формах:

- использование программных продуктов в качестве объекта преступления (незаконное копирование, причинение ущерба применением разрушающих программ - вирусов);

- использование программных продуктов в качестве инструмента совершения преступления (несанкционированное проникновение в компьютерную систему, искажения и подлоги информации);

- объектом совершения преступления являются технические средства ЭВМ (кража компьютерной информации, незаконное использование машинного времени);

- использование технических средств ЭВМ как средства совершения преступления (внесение изменений в информационную базу, изготовление с помощью печатной базы ЭВМ фальшивых документов).

Исходя их сказанного нам представляется возможным определить компьютерную информацию применительно к процессу доказывания как фактические данные, обработанные компьютером и полученные на его выходе в форме, доступной восприятию ЭВМ либо человека или передающиеся по телекоммуникационным каналам, на основе которых в определенном законом порядке орган дознания, лицо, осуществляющее досудебное расследование и суд устанавливают наличие или отсутствие общественно опасного деяния, виновность лица, совершившего это деяние, и иные обстоятельства, имеющие значение для правильного разрешения дела.

Применительно к средствам вычислительной техники источниками компьютерной информации могут служить: машинная распечатка; накопители на магнитных, оптических и иных носителях; информация, содержащаяся в оперативной памяти ЭВМ; информация, содержащаяся в постоянном запоминающем устройстве.

Анализ отечественной и зарубежной специальной литературы, изучение уголовных дел, опросы практических работников оперативных служб, лиц, осуществляющих досудебное расследование и судей позволил нам определить основные проблемы, возникающие при расследовании дел, где в качестве доказательства выступает компьютерная информация:

1) установление самого события преступления и правильная его квалификация;

2) неопределенность лица, осуществляющего досудебное расследование при проведении следственных действий по обнаружению, изъятию, фиксации и исследования компьютерной информации вследствие недостаточной нормативной базы и отсутствия методических разработок;

3) отсутствие у лиц, осуществляющих досудебное расследование практики расследования преступлений, совершаемых с использованием компьютерной техники;

4) отсутствие элементарных знаний компьютерной техники и, как следствие этого, психологический барьер, возникающий при расследовании таких дел.

РЕЦЕНЗИЯ

на лекцию, подготовленную доцентом кафедры досудебного расследования Кемпировой Ж.С. по теме: «Деятельность следователя по проверке законности и обоснованности повода к началу досудебного расследования в сфере компьютерной информации и высоких технологий»

Представленная на рецензирование лекция, подготовленная Кемпировой Ж.С. соответствует требованиям, установленным для написания такого вида работ. Данная работа посвящена актуальной и практически востребованной проблеме – возникающих в ходе досудебного расследования по уголовным делам в сфере компьютерной информации и высоких технологий.

В данной лекции рассмотрены следственные ситуации первоначального этапа расследования преступлений в сфере высоких информационных технологий в сфере компьютерной информации и высоких технологий, а также поводы к началу досудебного расследования по делам данной категории. Представленные вопросы освещены на достаточном теоретическом уровне, использованы различные монографические исследования по рассматриваемой теме, а также нормативные источники.

В данной работе на основе изучения правоприменительной практики и литературы, рассмотрены актуальные на сегодняшний день теоретические и прикладные аспекты тактики и технологии собирания и использования информации при расследовании преступлений, в сфере компьютерной информации и высоких технологий. Кроме того, высказаны соображения и предложения по их разрешению в соответствующем законодательстве РК и при правоприменительной работе сотрудников правоохранительных органов. Изучая эти проблемы и познания закономерностей этой деятельности, автор определенно выразил и дополнительно сформулировал ряд научных и практических выводов и рекомендаций по повышению эффективности правоотношений в целом и в частности по разрешению проблемных ситуаций по теме исследования.

Проводя изучение и анализ рассматриваемой темы, автор, в достаточной степени проявляет свое умение и приобретенные научно-исследовательские навыки, дает обобщение и выдвигает обоснованные выводы, оперируя материалами научных трудов, а также положениями нормативно-правовых актов. Учитывая изложенное, считаю, что лекция выполнена на достаточно хорошем теоретическом уровне и будет иметь примирительное значение в ходе практической деятельности.

МВД РЕСПУБЛИКИ КАЗАХСТАН
КАРАГАНДИНСКАЯ АКАДЕМИЯ МВД РК
им. БАРИМБЕКА БЕЙСЕНОВА
ЮРИДИЧЕСКИЙ ИНСТИТУТ

КАФЕДРА ДОСУДЕБНОГО РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ

ЛЕКЦИЯ

Тема №2 Деятельность следователя по проверке законности и обоснованности повода к началу досудебного расследования в сфере компьютерной информации и высоких технологий

Лекцию подготовил:
доцент кафедры досудебного расследования преступлений Карагандинской академии МВД РК им. Б. Бейсенова
майор полиции Кемпирова Ж.С.

Лекция обсуждена и одобрена на заседании кафедры досудебного расследования преступлений «___» _____ 2018 года Протокол №___.

Караганда – 2018 г.

Тема: Деятельность следователя по проверке законности и обоснованности повода к началу досудебного расследования в сфере компьютерной информации и высоких технологий

Вид занятия: Лекция Время - 1 час.

План лекции:

Введение

1. Особенности проведения отдельных следственных действий на первоначальном этапе расследования преступлений в сфере высоких информационных технологий

Заключение

Цели занятия**:**

Методическая - подготовка и чтение лекции, выбор средств, обеспечивающих наглядное и полное усвоение дидактического содержания лекции.

Дидактическая - доведение до курсантов определенного комплекса учебной информации, определенного блока знаний на уровне и в объеме, предусмотренном программой и тематическим планом по вопросам организации и проведения следственных осмотров. Доведение материала с использованием методических и технических средств обучения, которые обеспечивают его усвоение.

Воспитательная - выработка психологической установки на возможность осознания, усвоения воспринимаемых научных знаний и понимания значения их реализации через соответствующие практические умения в будущей деятельности при проведении досудебного расследования.

Литература:

1. Аверьянова Т.В. Задачи компьютерно-технической экспертизы // Информатизация правоохранительных систем: Тезисы докладов междун. конф. В 2-х ч. М., 1998. 4.2.

2. Батурин Ю.М., Жодзишский А.М. Компьютерные правонарушения: криминализация, квалификация, раскрытие // Сов. государство и право, 1990. № 12. С.86-94.

3. Гортинский А.В., Пархоменко А.Н. Некоторые рекомендации по организации и проведению следственных действий при расследовании преступлений, совершенных с использованием печатающих средств персональных компьютеров // Материалы семинара: «Вопросы квалификации и расследования некоторых преступлений в сфере экономики». Саратов, 1998. 15-18 дек. С. 184-187.

4. КЕНЖЕТАЕВ Д.Т., КАЛИЕВ А.К., БАЛТАБАЕВ Т.Н. ПРИМЕРНЫЕ ОБРАЗЦЫ УГОЛОВНО-ПРОЦЕССУАЛЬНЫХ ДОКУМЕНТОВ ДОСУДЕБНОГО РАССЛЕДОВАНИЯ, КАРАГАНДА, 2014.

5. КРЫЛОВ В.В. ИНФОРМАЦИЯ КАК ЭЛЕМЕНТ КРИМИНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ // ВЕСТНИК МОСК. УН-ТА. СЕР. 11. ПРАВО. - М., 1998. - № 4. - С. 50-64.

6. РОССИНСКАЯ Е.Р ПРЕДМЕТ И ПРАКТИЧЕСКИЕ ПРИЛОЖЕНИЯ КОМПЬЮТЕРНО-ТЕХНИЧЕСКОЙ ЭКСПЕРТИЗЫ //ИНФОРМАТИЗАЦИЯ ПРАВООХРАНИТЕЛЬНЫХ СИСТЕМ: ТЕЗИСЫ ДОКЛАДОВ МЕЖДУНАР.КОНФ. В 2-Х Ч. М., 1998. Ч. 2.

7. Скоромников К.С. Расследование преступлений в сфере компьютерной информации // Руководство для следователей / Под ред. Н.А.Селиванова, В.А. Снеткова. М., 1997.

8. Толеубекова Б.Х. Компьютерная преступность: вчера, сегодня, завтра. Караганда, 1995.

9. ТЯЖИНА А.О., НОГАЙБАЕВА А.С. НОВЕЛЛЫ ДОСУДЕБНОГО РАССЛЕДОВАНИЯ ПО УПК РЕСПУБЛИКИ КАЗАХСТАН. УЧЕБНО-ПРАКТИЧЕСКОЕ ПОСОБИЕ (КРАТКИЙ АНАЛИЗ В СХЕМАХ). КАРАГАНДА, 2015.

10. ТЯЖИНА А.О., НОГАЙБАЕВА А.С., БЕЙСЕНБАЕВ А.Ж. ДОСУДЕБНОЕ ПРОИЗВОДСТВО ПО УГОЛОВНЫМ ДЕЛАМ: ОБРАЗЦЫ ПРОЦЕССУАЛЬНЫХ ДОКУМЕНТОВ, КАРАГАНДА, 2014.

11. Шурухнов Н.Г. Тактика следственного осмотра и освидетельствования Криминалистика: Курс лекций. М.: Эксмо. 2006.

Нормативные акты:

1. **Конституция Республики Казахстан** *(принята на республиканском референдуме 30 августа 1995 года), (с* изменениями и дополнениями *по состоянию на 10.03.2017 г.).*

2. Уголовно-процессуальный кодекс Республики Казахстан № 231-V-ЗРК *(с* изменениями и дополнениями *по состоянию на 09.01.2018 г.)*

3. Уголовный кодекс Республики Казахстан № 226-V-ЗРК *(с* изменениями и дополнениями *по состоянию на 09.01.2018 г.)*

4. Приказ Генерального Прокурора Республики Казахстан «Об утверждении правил приема и регистрации заявлений и сообщений об уголовных правонарушениях, а также ведения Единого реестра досудебных расследований» №89 от 19.09.2014г. с изм. и доп. от 10.08.2015 г. №99, 23.09.2016 №148.

5. Приказ Генерального прокурора Республики Казахстан от 22 сентября 2014 года №91 «Об утверждении Правил применения научно-технических средств фиксации хода и результатов следственных действий».

6. Закон Республики Казахстан от 11.01.2007 N 217-III «Об информатизации».

Введение

Информационная эра привела к драматическим изменениям в способе выполнения своих обязанностей для большого числа профессий. Теперь нетехнический специалист среднего уровня может выполнять работу, которую раньше делал высококвалифицированный программист. Служащий имеет в своем распоряжении столько точной и оперативной информации, сколько никогда не имел.

Но использование компьютеров и автоматизированных технологий приводит к появлению ряда проблем для руководства организацией. Компьютеры, часто объединенные в сети, могут предоставлять доступ к колоссальному количеству самых разнообразных данных. Поэтому люди беспокоятся о безопасности информации и наличии рисков, связанных с автоматизацией и предоставлением гораздо большего доступа к конфиденциальным, персональным или другим критическим данным. Все увеличивается число компьютерных преступлений, что может привести в конечном счете к подрыву экономики. И поэтому должно быть ясно, что информация - это ресурс, который надо защищать. Ответственность за

защиту информации лежит на низшем звене руководства. Но также кто-то должен осуществлять общее руководство этой деятельностью, поэтому в организации должно иметься лицо в верхнем звене руководства, отвечающее за поддержание работоспособности информационных систем.

И так как автоматизация привела к тому, что теперь операции с вычислительной техникой выполняются простыми служащими организации, а не специально подготовленным техническим персоналом, нужно, чтобы конечные пользователи знали о своей ответственности за защиту информации.

Еще совсем недавно все, что связано с ЭВМ (компьютерами), было непривычным для широких слоев населения Казахстана. Одной из причин возникновения компьютерной преступности явилось информационно-технологическое перевооружение предприятий, учреждений и организаций, насыщение их компьютерной техникой, программным обеспечением, базами данных. Другая причина - реальная возможность получения значительной экономической выгоды за противоправные деяния с использованием ЭВМ. Появилась заманчивая возможность как бы обменивать продукт своего неправомерного труда на иные материальные ценности. Страны, уже прошедшие период компьютерного переоснащения, накопили свой криминальный опыт. Например, бухгалтер одной из зарубежных пароходных компаний вычислил, что незначительное искажение отчетности не будет замечено ревизионной службой. Организовав 17 подставных фирм, он похитил значительные суммы без каких-либо видимых нарушений финансовой деятельности компании. Другой пример: преступник открывает не менее двух счетов в банках, перечисляя денежные суммы с процентами со счета на счет, в конечном итоге он исчезает с похищенной суммой. Заполучил своих компьютерных взломщиков и Казахстан. Не исключено, что в РК компьютерная преступность имеет высокую степень латентности в связи с общей криминогенной обстановкой и отсутствием до недавнего времени соответствующих норм уголовного законодательства, а также специфичностью самой компьютерной сферы, требующей специальных познаний.

Ситуация, сложившаяся в обществе, потребовала принятия законодательных норм, которые предусматривали бы ответственность за совершение преступлений в сфере компьютерной информации.

В настоящее время перед правоохранительными органами при расследовании компьютерных преступлений возникают проблемы, характеризующие одновременно и специфику этого процесса, а именно:

1) сложность в установлении факта совершения компьютерного преступления и решении вопроса о начале досудебного расследования;

2) сложность в подготовке и проведении отдельных следственных действий;

3) особенности выбора и назначения необходимых судебных экспертиз;

4) целесообразность использования средств компьютерной техники в расследовании преступлений данной категории;

5) отсутствие методики расследования компьютерных преступлений.

Таким образом, по оценкам отечественных и зарубежных исследователей, решение проблем раскрытия и расследования преступлений данного вида представляет собой задачу на несколько порядков более сложную, чем задачи, сопряженные с их предупреждением.

1. Особенности проведения отдельных следственных действий на первоначальном этапе расследования преступлений в сфере высоких информационных технологий

Общее изучение сущности рассматриваемого вопроса предполагает анализ следующих следственных действий, чье проведение характерно для первоначального этапа расследования по делам о преступлениях, совершенных в сфере высоких информационных технологий:

По мнению Э. Мелик, целями следственных действий при расследовании данного вида преступлений могут являться:

- осмотр и изъятие компьютерной техники;
- поиск и изъятие информации и следов воздействия на нее непосредственно на носителях информации ПК и ее устройствах;
- поиск и изъятие информации и следов воздействия на нее вне ПК.

Полагаем, что указанные цели усекают перечень следственных действий, производство которых возможно при расследовании преступлений в сфере высоких информационных технологий, проводимых с целью установления обстоятельств, имеющих значение для дела. На этот счет думается, что необходимо расширить перечень указанных целей и дополнить их, где: целями следственных действий, проводимых при расследовании и раскрытии преступлений в сфере высоких информационных технологий, являются:

-установление и уточнение обстоятельств, происшедшего события (способ, место, время, личность совершившего преступное посягательство и пр.);

-выявление, фиксация, изъятие и оценка следов преступления (как традиционных криминалистических, так и нетрадиционных - информационных следов преступлений в сфере высоких технологий), различных вещественных доказательств;

-получение информации, необходимой для построения и проверки следственных версий и осуществления розыскной работы по делу;

-поиск и изъятие информации и следов воздействия на нее непосредственно на носителях информации ПК и ее устройствах;

-поиск и изъятие информации и следов воздействия на нес вне ПК;

-обнаружение предметов и объектов преступлений;

-осмотр и изъятие компьютерной техники;

-установление лиц, способствующих совершению преступления;

-определение принадлежности компьютерной информации;

-проверка и оценка следственных версий;

-установление причин и условий, способствовавших совершению преступления;

-получение новых доказательств.

Таким образом, приступая к непосредственному исследованию особенностей проведения отдельных следственных действий при расследовании преступлении в сфере высоких информационных технологий (исходя из указанных целей), мы выделяем следующие виды следственных действий, чье рассмотрение будет осуществлено далее: осмотр (включая несколько его разновидностей), обыск и выемка, допрос, следственный эксперимент, предъявление для опознания, назначение экспертиз.

По своей сути, все перечисленные действия могут быть проведены как на первоначальном этапе расследования преступлений в сфере высоких информационных технологий, так и на последующем. Данный факт определяется конкретными условиями расследования преступления. Вместе с тем, исследование сущности установления события преступления и лица его совершившего свидетельствует о том, что успешность проведения перечисленных действий и определяет достижение задач, направленных на быстрое и полное раскрытие преступления, изобличение и привлечение к уголовной ответственности лиц, его совершивших.

Рассматривая следственные действия, производство которых осуществляется при расследовании преступлений указанной категории, еще раз отметим, что проводятся они в строгом соответствии с правилами, регламентированными действующим уголовно-процессуальным законодательством, но с учетом некоторых особенностей.

Осмотр. Следственный осмотр – это следственное действие, состоящее в непосредственном восприятии, анализе и фиксации следователем или лицом, проводящим дознание, различных материальных предметов и отдельных их элементов в целях обнаружения следов преступления и других вещественных доказательств, выяснения обстановки происшествия, а также иных обстоятельств, имеющих значение для дела. Цель осмотра места происшествия по делам указанной категории – установление конкретного СВТ, выступающего в качестве предмета и (или) орудия совершения преступления и имеющего следы преступной деятельности. При производстве следственного действия целесообразно использовать тактический прием «от центра – к периферии», где «центром» (отправной точкой осмотра места происшествия) являются СВТ, находящиеся на месте осмотра. Исследование специфики следственного осмотра производится, исходя из этапов его производства: подготовительного, рабочего, заключительного.

1. Подготовительный этап.

В процессе подготовки к проведению этого следственного действия, еще до выезда на место происшествия необходимо решить ряд

организационных вопросов, которые в последующем обеспечат качество проведения осмотра места происшествия.

Рассматриваемое следственное действие должно быть заблаговременно подготовлено и детально спланировано, необходимо предварительно провести следующую работу:

-с учетом сложившейся следственной ситуации, наметить круг лиц, участвующих в осмотре;

-определить последовательность действия лиц при осмотре места происшествия;

-пригласить соответствующих квалифицированных специалистов;

-подготовить соответствующую компьютерную технику и программное обеспечение, которые будут использоваться для считывания и хранения изъятой информации, при обнаружении изменений в компьютерной информации, исследовании полученной информации, обнаружении информационных следов преступления;

-перед началом осмотра разъяснить цели проведения следственного действия и задачи, стоящие перед специалистами, а также их права и обязанности;

-провести подбор и инструктаж понятых, в качестве которых целесообразнее привлекать лиц, обладающих минимально необходимыми знаниями в области СВТ и компьютерных технологий, разъяснить их права и обязанности.

При осмотре места происшествия в состав следственно-оперативной группы (СОГ) в зависимости от конкретной следственной ситуации должны входить следующие лица:

-следователь, специализирующийся на расследовании уголовных дел рассматриваемой категории — руководитель СОГ;

-специалист-криминалист, знающий особенности работы со следами преступлений данной категории;

-сотрудник оперативно-технического подразделения правоохранительного органа;

-специалист по сетевым технологиям СВТ (в случае наличия на месте происшествия периферийного оборудования удаленного доступа или локальной компьютерной сети);

-специалист по системам связи (при использовании для дистанционной передачи данных каналов электросвязи);

-оперативные сотрудники;

-участковый инспектор, обслуживающий данную территорию;

-инспектор отдела вневедомственной охраны (в случае, когда место происшествия или СВТ, находящееся на нем, являются охраняемыми объектами).

При необходимости для участия в осмотре места происшествия могут быть приглашены и другие незаинтересованные в деле специалисты, знающие специфику работы осматриваемого объекта (инженеры-электрики,

бухгалтеры со знанием СВТ, специалисты спутниковых систем связи, операторы компьютерных систем и сетей – сотовых, Интернет и др., и т. д.).

Особенности выбора специалиста. Характерной чертой преступлений в сфере высоких информационных технологий является то, что при проведении большинства следственных действий необходимо участие специалиста. Как справедливо отмечают Е. Р. Российская и А. И. Усов, при расследовании преступлений, сопряженных с использованием компьютерных средств, участие специалиста необходимо, поскольку даже малейшие неквалифицированные действия с компьютерной системой зачастую заканчиваются безвозвратной утратой ценной розыскной и доказательственной информации.

При расследовании преступлений в сфере высоких информационных технологий основными задачами специалистов в области компьютерной техники являются: выполнение всех манипуляций с компьютерной техникой (включение-выключение, разборка-сборка и пр.); оказание помощи следователю в описании компьютерной техники и периферийного оборудования в протоколах следственных действий; проведение экспресс анализа компьютерной информации; обнаружение информационных следов преступления; предотвращение уничтожения или повреждения компьютерной информации; изъятие компьютерной информации и др.

Следует отметить, что информационные технологии достаточно разнообразны и выбор специалиста для решения конкретных задач расследования может быть весьма сложен. При решении в ходе следственных действий задач, связанных с изъятием технических средств, может быть полезен специалист, знающий элементы и устройства вычислительной техники и систем управления, знакомый с вопросами функционирования автоматизированных систем управления. Для установления фактов проникновения извне в информационные системы специалист должен обладать познаниями в области программного обеспечения вычислительных систем и организации вычислительных процессов, а также обязан знать основы методов защиты информации и информационной безопасности. При исследовании систем ПК и их сетей специалист должен иметь специализацию в области математического и программного обеспечения вычислительных комплексов, систем и сетей, ему также необходимы познания в области компьютерных сетей, узлов связи и средств коммуникаций, организации и распределения информационных потоков.

Поиск таких специалистов следует проводить заблаговременно на предприятиях, в учреждениях, фирмах и компаниях, осуществляющих обслуживание и эксплуатацию компьютерной и коммуникационной техники, разработку программного обеспечения, средств защиты компьютерной информации. Необходимые специалисты могут быть приглашены из учебных заведений и научно-исследовательских организаций, а также из органов внутренних дел. Поскольку отдельные виды судебно-технологических экспертиз проводятся в экспертных подразделениях ОВД на региональном уровне, то производящие их лица также - могут быть приглашены в качестве

специалистов. В исключительных случаях, могут быть приглашены в качестве специалистов сотрудники организации, компьютеры которой подверглись вторжению.

Понятые. В качестве понятых рекомендуется приглашать людей, сведущих в компьютерной технике. Непонимание смысла происходящего для человека, приглашенного в качестве понятого, а позднее допрошенного в суде, может не убедить суд в признании тех или иных обстоятельств доказательствами. Понятых в отдельных случаях можно приглашать из числа служащих того предприятия, организации, учреждения, фирмы, компании, в которой проводится осмотр места происшествия, при условии, что они не заинтересованы в исходе дела. В любом случае, поскольку объектом осмотра выступает дорогостоящее оборудование, осмотр места происшествия целесообразно производить в присутствии руководства предприятия, организации, учреждения, фирмы, компании.

Подготовка соответствующей компьютерной техники и программного обеспечения. Это может быть персональный компьютер, исполненный в переносном варианте «Notebook». Кроме компьютера, необходим кабель, а также специальное программное обеспечение, позволяющее осуществлять копирование и экспресс-анализ информации на месте. Следует иметь в виду, что для полного и качественного копирования информации необходимо соответствие не марок компьютеров, а объемов используемых жестких дисков (у переносного компьютера этот объем должен быть не меньше, а в идеальном случае равен объему диска осматриваемого компьютера). Помимо переносного компьютера типа «Notebook», при производстве осмотра могут быть использованы иные носители информации, обладающие большой емкостью: лазерные и DVD диски, ZlP-накопители и др.

При инструктаже членов следственно-оперативной группы особое внимание необходимо уделить их поведению во время осмотра: внимательно следить за поведением всех лиц, которые могут находиться в помещении, где производится осмотр; проявлять особую осторожность при обращении с компьютерной техникой, создавая условия для работы с ней специалисту. Следует помнить, что компьютерная техника - это дорогостоящее оборудование, которое требует осторожности при обращении с ней, в том числе и при ее изъятии. К тому же она может хранить значительное количество информации, являющейся собственностью, как отдельного лица, так и фирмы. Единственная ошибка может привести к миллионным убыткам. В ходе инструктажа участников следственно-оперативной группы следователь указывает основные задачи предстоящего следственного действия, особенности его производства по рассматриваемому виду преступлений, указывает на характер действий каждого лица. Представляется обоснованным такой инструктаж проводить следователю в паре со специалистом. При этом необходим категорический запрет кому бы то ни было из лиц, работающих на объекте осмотра или находящихся на нем по иным причинам, соприкасаться с ПК, выключать без специального указания со стороны следователя энергоснабжение объекта, самостоятельно

производить какие-либо манипуляции со средствами компьютерной техники, если результат этих манипуляций заранее не известен.

При разрешении возникших конфликтов следователя с персоналом дополнительно к вышеизложенным правилам желательно руководствоваться следующими рекомендациями:

1) недопустимо производить изъятие в несколько приемов, даже если следователь не располагает необходимым транспортом. В этом случае нужно сделать несколько рейсов с объекта до места хранения изъятых материалов;

2) изъятые материалы не могут быть оставлены на ответственное хранение на самом объекте или в другом месте, где к ним могут иметь доступ посторонние лица;

3) недопустимо оставление на объекте части средств компьютерной техники по мотивам ее «абсолютной необходимости» для деятельности данной фирмы (организации). Желание персонала сохранить от изъятия определенные СКТ – обычно указывает на наличие на них важной для следствия информации;

4) следует изымать все СКТ, находящиеся в помещении объекта, независимо от их юридической принадлежности;

5) если персонал настаивает на отражении в протоколе следственного действия конкретных качеств изымаемых СКТ (марка, быстродействие, марка процессора, объем памяти и т. д.), то эти сведения могут быть записаны лишь как отдельные заявления.

2. Рабочий этап.

Прежде чем приступить к осмотру, следователь и участники следственно-оперативной группы должны знать и соблюдать общие правила обращения с вычислительной техникой и носителями информации. Несоблюдение этих правил может привести к потере важной для расследования информации и нанесению материального ущерба, вызванного этими действиями.

Общими правилами обращения с вычислительной техникой и носителями информации являются:

- все включения (выключения) компьютеров и других технических средств производятся только специалистом или под его руководством;

- применение средств криминалистической техники – магнитных искателей, ультрафиолетового осветителя, инфракрасного преобразователя, во избежание разрушения носителей информации и микросхем памяти ПК, должно быть согласовано со специалистом;

- необходимо исключить попадания мелких частиц и порошков на рабочие части компьютеров (разъемы, дисковод, вентилятор и др.);

- при работе с магнитными носителями информации запрещается прикасаться руками к рабочей поверхности дисков, подвергать их электромагнитному воздействию, сгибать диски, хранить без специальных конвертов (пакетов, коробок);

- диапазон допустимых температур при хранении и транспортировке

должен варьироваться в температурных пределах от 0 до + 50 граду сов Цельсия;

- со всеми непонятными вопросами, затрагивающими терминологию, устройство и функционирование вычислительной техники необходимо обращаться только к специалисту.

По прибытию на место происшествия следователь должен:

1)удалить с места происшествия всех посторонних лиц и организовать его охрану, если этого не было сделано. Обязательной охране подлежат: территория места происшествия; все СВТ, находящиеся на территории (в помещении); пункты отключения электропитания СВТ, находящиеся в здании (учреждении, организации, на территории);

2)зафиксировать обстановку, сложившуюся на момент осмотра места происшествия, произвести ориентирующую и обзорную фото-, видеосъемку;

3)исключить возможность посторонним лицам (да и участникам следственно-оперативной группы) соприкасаться с оборудованием. Желательно лишить их возможности пользоваться телефоном, а при острой необходимости делать это только с разрешения следователя. «Не допускайте, чтобы кто-либо производил любые действия с компьютером. Риск, связанный с непосредственным вмешательством в систему, значительно больше, чем малый шанс дистанционного влияния на систему с другого устройства». Необходимо организовать охрану каждого компьютера (терминала), для чего возможно привлечение дополнительных сил (подразделений ОВД и пр.);

4) допросить потерпевшего, материально ответственное лицо и очевидцев (операторов СВТ) об изменениях, внесенных в обстановку, о категории обрабатываемой информации (общедоступная или конфиденциальная), а также о действиях потерпевшего до прибытия СОГ. Вопросы необходимо конкретизировать по мере детального осмотра места происшествия, поиска следов и других вещественных доказательств;

5) определить, соединены ли находящиеся в помещении компьютеры в локальную вычислительную сеть. На это могут указать коаксиальные кабели, идущие от компьютера к компьютеру, или просто телефонные провода. При наличии локальной компьютерной сети наибольший интерес представляет центральный компьютер, так называемый сервер, на котором хранится большая часть информации и к которому имеют доступ все ПК. Этот компьютер необходимо обследовать более тщательно и осторожно;

6) установить – имеются ли соединения компьютера с оборудованием или вычислительной техникой вне осматриваемого помещения. На это могут указывать кабели и провода, идущие от компьютера в другие помещения или здания. Если есть соединения, то существует реальная возможность непосредственного обмена информацией, независимо от желания специалиста, ее изменения или уничтожения с удаленных рабочих мест, находящихся за несколько метров или даже километров от обыскиваемого помещения. Для предотвращения этого на время съема информации вычислительную сеть необходимо

отключить от «внешнего мира» программно или физическим отключением кабелей. Эту работу квалифицировано может выполнить только специалист в области вычислительной техники;

7) выяснить – подключен ли компьютер к телефонной линии. В случае подключения на него могут поступать вызовы с дальнейшими приемами или передачами информации. Следует иметь в виду, что установить запрограммирован ли компьютер на передачу может только специалист. Если информация, поступающая на компьютер – по электронной почте, факсимильной или телетайпной связи может иметь интерес, то отключать телефонную или телетайпную линии нет смысла, но необходимо воздерживаться от телефонных разговоров по данной линии;

8) определить – запушены ли программы на ПК и какие именно. Для этого необходимо изучить изображение на экране и, по возможности, детально описать его в протоколе. Если специалисту удастся определить, что на компьютере работает программа уничтожения информации или ее зашифровки, то такие программы сюит приостановить и обследование начать именно с этого компьютера. Важно отметить, что следователю в любом случае не следует самому производить какие-либо манипуляции с вычислительной техникой. Их должен осуществлять специалист.

На рабочей (исследовательской) стадии осмотра места происшествия каждый объект подлежит тщательному обследованию. В этот период времени важно установить – не содержится ли на компьютере информация, которая может способствовать более плодотворному и целенаправленному осмотру (различные планы помещений, участков местности, пароли, коды доступа, шифры и т. п.). Для этого специалистом проводится экспресс-анализ компьютерной информации путем просмотра содержимого дисков. Интерес могут представлять файлы с текстовой или графической информацией. Следует обращать внимание не только на наличие (отсутствие) физических повреждений компьютерной техники, магнитных носителей и т. п., но и на состояние окон, дверей и запорных устройств на них.

В этот период осмотра фиксируется текущее состояние компьютерной информации, делается вывод о произошедшем событии и его последствиях: уничтожение, блокирование, модификация, копирование информации, нарушение работы ПК, их системы или сети; устанавливается способ совершения преступления. Для этого с помощью специалиста наблюдается» действие программ, содержимое текстовых файлов и баз данных. При этом особое внимание следует уделить изучению имеющихся в большинстве компьютерных систем файлов регистрации. Какое бы событие не произошло в системе, информация о нем (в том числе, кто инициировал его, когда и в какое время оно произошло, какие при этом были затронуты файлы) регистрируется в этих файлах. В частности, в файлах регистрации может получить отражение информация о паролях пользователей, их именах, идентификационных номерах. В последствии данная информация может

быть использована для установления компьютера, с которого произошел неправомерный доступ к компьютерной информации.

В протоколе осмотра следует отразить следующие фактические данные:

- наименование и назначение объекта, где совершено преступление;

- территориальное расположение объекта осмотра (на улице, в помещении, в банке, в магазине, на автостоянке, бензоколонке, станции метро, в ресторане, гостинице, помещении кассы, на складе, вокзале, контроль но-пропускном пункте и т. д.) и его ориентация относительно сторон света;

- ближайшее окружение объекта и подступы к нему – здания, технические сооружения, площади, зоны, участки (производственные, административные, жилые) и расстояние до них; наличие дорог, подъездных путей (в т. ч. и водного транспорта), парковок и автостоянок; наличие линий и пунктов (колодцев, концентраторов т. д.) инженерно-технических коммуникаций (электросвязи, электропередачи, тепло-, водо- и газоснабжения, вентиляции и т. д.);

- технические и конструктивные особенности местности, связанные с установкой и эксплуатацией СВТ (этажность, материал стен и других строительных конструкций, форма строения, наличие дверей, окон, ограждений, фальшполов и подвесных потолков, наличие и состояние электрооборудования и др.);

- наличие, внешнее состояние и расположение охраны объекта, специальных защитных и сигнальных устройств от несанкционированного съема и утечки информации – постов охраны, (охранно-пожарной сигнализации, контрольно-пропускных пунктов доступа лиц на данную территорию (неавтоматический, полуавтоматический или автоматический), освещения, металлических решеток, штор, жалюзи, рольставен, замков и запорных механизмов, экранов, заземлений, специальных стекол и пленок, генераторов шума, фильтров и т. д.; расположение СВТ относительно вентиляционных и иных отверстий в строительных конструкциях, дверных и оконных проемов, технических средств видео наблюдения, а также других рабочих мест (если таковых несколько в одном помещении);

- расположение в одном помещении вместе с СВТ других электрических устройств и приборов – телефонных и иных аппаратов электросвязи, систем электро-часофикации, оргтехники (ксероксов, аудио-, видеомагнитофонов, автоответчиков, электрических пишущих машинок и т. п.), приборов электроосвещения (настольных, напольных, настенных, потолочных, подвесных и т. д.), абонентских громкоговорителей, телевизоров и мониторов, радиоприемников и магнитол, электроплиток, печей, чайников, кондиционеров и т. д.; наличие в одном помещении с СВТ линий, пунктов, разъемов промежуточных и оконечных устройств систем инженерно-технических коммуникаций (электросвязи, электропередачи, антенны-провода, водо- и газоснабжения);

- наличие или отсутствие технических средств сопряжения СВТ с каналами электросвязи и между собой (на это могут указывать кабели и провода, которыми СВТ соединены между собой, а также с аппаратами или линией электросвязи);

- наличие или отсутствие соединений СВТ с оборудованием или вычислительной техникой, находящейся вне территории (помещения) осмотра; на это могут указывать кабели и провода, идущие от осматриваемого СВТ за границу места осмотра (в другие помещения или здания) либо к аппаратам внутренней связи (в этом случае граница осмотра места происшествия значительно расширяется); наличие на объекте, путях подхода и отхода следов преступления и преступника, специфическими среди которых являются: следы орудий взлома, повреждения, уничтожения и(или) модификации охранных и сигнальных устройств; показания регистрирующей (электронный журнал) или специальной мониторинговой (тестовой) аппаратуры; следы пальцев рук на СВТ, охранных и сигнальных устройствах, на их клавиатуре, соединительных и электра питающих проводах и разъемах, на розетках и штепсельных вилках, тумблерах, кнопках и рубильниках, включающих СВТ и электрооборудование; остатки соединительных проводов и изоляционных материалов, капли припоя, канифоли; следы проплавления, прокола, надреза изоляции проводов СВТ, наличие участков механического сдавливания и приклеивания сторонних предметов;

- наличие или отсутствие учетно-справочной документации к СВТ технического паспорта и подобного ему документа; журнала оператора или протокола автоматической фиксации расчетно-кассовых и иных операций; журнала учета машинных носителей информации (МНИ), машинных документов, заказов (заданий или запросов); журнала (карточки) учета выдачи МНИ и документов; журнала (карточки) учета массивов (участков, зон), программ, записанных на МНИ; журнала учета уничтожения брака бумажных МНИ и машинных документов; актов на стирание конфиденциальной информации, уничтожение машинных носителей с конфиденциальной информацией, конфиденциальных машинных документов.

Непосредственно в ходе осмотра компьютерной техники следует принимать во внимание следующие неблагоприятные факторы:

- возможные попытки со стороны персонала повредить ПК с целью уничтожения информации и ценных данных;

- возможное наличие на компьютере специальных средств защиты от несанкционированного доступа, которые, не получив в установленное время специальный код, автоматически уничтожат всю информацию;

- возможное наличие на ПК иных средств защиты от несанкционированного доступа;

- постоянное совершенствование компьютерной техники, следствием чего может быть наличие на объекте программно-технических средств не знакомых следователю и специалисту.

В связи с чем необходимо предвидеть «меры безопасности», предпринимаемые преступниками с целью уничтожения вещественных доказательств. Ими может, например, использоваться специальное оборудование, в критических случаях создающее сильное магнитное поле, стирающее магнитные записи. Известна легенда о хакере, который создал магнитное поле в дверном проеме такой силы, что оно уничтожало магнитные носители информации при выносе их из его комнаты. Преступник имеет возможность включить в состав программного обеспечения своей машины программу, которая заставит компьютер требовать пароль периодически и, если несколько секунд правильный пароль не введен, данные в компьютере автоматически уничтожатся. Изобретательные владельцы компьютеров устанавливают иногда скрытые команды, удаляющие или архивирующие с паролями важные данные, если некоторые процедуры запуска машины не сопровождаются специальными действиями, известными только им.

В целях, недопущения вредных последствий перечисленных факторов следователь должен придерживаться следующих рекомендаций:

- перед выключением питания по возможности корректно закрыть все используемые программы, а в сомнительных случаях просто отключить компьютер (в некоторых случаях некорректное отключение компьютера путем перезагрузки или выключения питания без предварительного выхода из программы и записи информации на постоянный носитель приводит к потере информации в оперативной памяти и даже к частичному стиранию информационных ресурсов на данном компьютере);

- принять меры к установлению пароля доступа в защищенных программах;

- при необходимости консультаций у персонала предприятия получать их у разных сотрудников данного отдела путем опроса порознь. Такой метод позволит получить максимально правдивую информацию и избежать преднамеренного вредительства;

- при нахождении ПК в локальной вычислительной сети необходимо иметь бригаду специалистов для быстрого реагирования на движение информации по сети;

- наряду с осмотром компьютера, обеспечить осмотр документов о пользовании им, в' которых следует обратить особое внимание на рабочие записи операторов ПК, так как часто именно в этих записях неопытных пользователей можно обнаружить коды, пароли и другую очень ценную для следствия информацию. При осмотре должен присутствовать кто-либо из сотрудников предприятия, способный дать пояснения по установленному на ПК программному обеспечению. Если на начальной стадии осмотра не удалось установить пароли и коды используемых программ, то компьютер подлежит опечатыванию и выемке, с тем чтобы в последующем в стационарных условиях прокуратуры или лаборатории с привлечением специалистов-программистов выявить существующие пароли и коды доступа, осуществить надлежащий осмотр

компьютера и содержащихся на нем файлов. В таких случаях достаточно изъять только системный блок, в который входят процессор и накопители на магнитных дисках. Остальную часть компьютера (монитор, клавиатуру, принтер) следует опечатать. Кроме того, необходимо соблюдение также следующих рекомендаций:

- недопустимо производить изъятие в несколько приемов. В том случае, если следователь не располагает необходимым транспортом, следует сделать несколько рейсов от объекта до места хранения изъятых материалов с выставлением охраны на объекте изъятия (охране подлежат не изъятые СВТ и помещение, в котором они находятся);

- изъятые предметы и материалы не могут быть оставлены на ответственное хранение на самом объекте или в другом месте, где к ним мо гут иметь доступ посторонние лица;

- недопустимо оставлять на объекте части СВТ по причине их «абсолютной необходимости» в деятельности данного пользователя: как правило, желание сохранить от изъятия определенные СВТ указывает на наличие в них важной для следствия информации;

- следует изымать все СВТ, находящиеся в помещении объекта и не сущие следы преступной деятельности;

- в протоколе следственного действия должны обязательно фиксироваться конкретные признаки изымаемых СВТ (марка, быстродействие, марка процессора, объем памяти и т. д.).

3. Заключительный этап.

Изъятие средств компьютерной техники производится только в выключенном состоянии. При этом должны быть выполнены и отражены в протоколе следующие действия;

- установлено включенное состояние оборудования и зафиксирован порядок его отключения;

- описано точное местонахождение изымаемых предметов и их расположение относительно друг друга и окружающих предметов (с приложением необходимых схем и планов);

- описан порядок соединения между собой всех устройств с указанием особенностей соединения (цвет, количество, размеры, характерные индивидуальные признаки соединительных проводов, кабелей, шлейфов, разъемов, штекеров и их спецификация); - определено отсутствие либо наличие компьютерной сети, используемый канал (каналы) связи и телекоммуникаций. В последнем случае установлен тип связи, используемая аппаратура, абонентский номер, позывной либо рабочая частота;

- произведено разъединение (с соблюдением всех необходимых мер предосторожности) аппаратных частей (устройств) с одновременным опломбированием их технических входов и выходов;

- определен вид упаковки и транспортировки изъятых предметов.

Транспортировка и хранение компьютерной техники и информации должны осуществляться в условиях, исключающих ее повреждение, в том числе в результате воздействия метало детекторов, используемых для

проверки багажа в аэропортах. Хранят компьютеры и их комплектующие в сухом, отапливаемом помещении. Следует удостовериться, что в нем нет грызунов, которые часто являются причиной неисправности аппаратуры. Учитывая нестандартность обстановки, в которой может производиться осмотр места происшествия, вопрос о возможности изъятия компьютерной техники и информации, способе упаковки, транспортировки и хранении изъятых объектов решается следователем в каждом конкретно случае совместно со специалистом. Процессуальный порядок изъятия объектов определяется общими требованиями Уголовно-процессуального кодекса.

Осмотр средств вычислительной техники (СВТ), участвовавших в преступлении, производят для достижения следующих целей:

- обнаружения следов, образовавшихся в результате происшествия или совершения преступления, и других вещественных доказательств для установления, кем, с какой целью и при каких обстоятельствах было совершено преступление;

- выяснения обстановки происшествия для восстановления механизма совершения преступления;

- установления технического состояния СВТ.

При реализации первой цели требуется участие специалиста-криминалиста и специалиста в области СВТ и информационных технологий. В решении двух других непосредственное участие специалиста-криминалиста не требуется.

Осмотр машинного носителя информации (МНИ) может быть произведен в ходе осмотра места происшествия или как самостоятельное следственное действие.

Осмотр МНИ производится с участием специалиста и начинается с определения типа, вида, назначения, технических параметров и ознакомления с его содержанием. К машинным носителям информации, как правило, относятся магнитные диски (гибкие – дискеты, жесткие – «винчестеры», «банки» и «Zip»); пластиковые карты (карточки); интегральные микросхемы (ИМС), в т. ч. находящиеся в различных СВТ – в виде оперативной памяти (ОЗУ) и(или) постоянного запоминающего устройства (ПЗУ) – персональных компьютерах, сотовых и иных аппаратах электросвязи, электронных записных книжках, электронных переносных справочниках и переводчиках, контрольно-кассовых аппаратах, банкоматах, контрольно-пропускных устройствах, смарт-картах и т. д.).

В протоколе осмотра должны быть зафиксированы следующие фактические данные:

1.Тип, вид, марка, назначение, цвет и заводской номер (или учетный номер носителя).

2. Наличие индивидуальных признаков и техническое состояние футляра (коробки, упаковки, специального технического устройства) – тип, размеры, цвет, материал, физические повреждения, наклейки, принцип функционирования, емкость и т. д.

3. Техническое состояние – размеры носителя, внешний вид, материал каркаса носителя, его целостность и индивидуальные признаки, материал основного информационно-несущего слоя и его целостность (механические повреждения – царапины, деформации, нарушения несущего слоя и т. д.), наличие и положение (сохранность) приспособлений от несанкционированного уничтожения (перезаписи) информации (ключей, пломб, заглушек, маркеров), наличие и техническое состояние механизмов защиты информационно-несущего материала (отверстий окон для считывания и записи информации).

4.Наличие, размеры, цвет, марка и техническое состояние разъемов для подключения к специальному считывающему устройству.

5.Присутствие внешней спецификации, ее цвет и размеры (заводские или пользовательские наклейки с текстом или специальными пометками).

6.Наличие индивидуальных признаков защиты носителя от несанкционированного использования (тип – голография, штрих-код, флюоресцирование, перфорация, ламинирование, вплавление личной подписи пользователя и т. д.; размеры, цвет, вид).

7.Признаки материальной подделки МНИ и их защиты – подчистки, подтирки, травления, термическое воздействие, переклеивание (склеивание, наклеивание, заклеивание), дописки, замены, перепайки и т. д.

8.Работоспособность и внутренняя спецификация – серийный номер и(или) метка тома, либо код; размер разметки (для дисков – по объему записи информации, для лент - по продолжительности записи); размер области носителя, свободной от записи и занятой под информацию; количество и номера сбойных зон, секторов, участков, кластеров, цилиндров; количество записанных программ, файлов, каталогов (подкаталогов), данных, их структура, название (имя и расширение), размер и объем, который занимают их названия, дата и время создания (или последнего изменения), а также специальная метка или флаг (системный, архивный, скрытый, только для чтения или записи и т. д.); наличие скрытых или ранее стертых файлов (программ) и их реквизиты (название, размер, дата и время создания или уничтожения).

9.Результат осмотра содержимого файлов (программ, компьютерной информации), записанных на МНИ или находящихся в оперативной памяти СВТ и имеющих значение для дела.

10.Все манипуляции (нажатия на клавиши и т. д.) со средствами вычислительной техники, совершенные в процессе осмотра.

11.Индивидуальные признаки СВТ, используемые в процессе осмотра, – тип, вид, марка, название, заводской или регистрационный номер и т. п.

12. Ссылка на то, что используемые в процессе осмотра СВТ перед началом следственного действия были тестированы специалистом на предмет отсутствия в них вредоносных программных и аппаратных средств.

Обыск, выемка.

Обыск – следственное действие, в процессе которого производится поиск и принудительное изъятие объектов, имеющих значение для

правильного решения задач уголовного судопроизводства. Выемка – следственное действие, в процессе которого производится изъятие объектов, имеющих значение для правильного решения задач уголовного судопроизводства, в тех случаях, когда их местонахождение точно известно следователю.

Задачами обыска при расследовании преступлений в сфере высоких информационных технологий являются отыскание и изъятие:

1) орудий, используемых для совершения преступления в сфере компьютерной информации, в том числе носителей информации, примененных для копирования похищенной информации или содержащие программы «взлома» защиты компьютера, вредоносные программы, иные программы и файлы данных (например, библиотеки паролей и имен), использованные при совершении преступления;

2) компьютерной информации;

3) специальной литературы, посвященной вопросам компьютерной безопасности, эксплуатации ПК, создания вредоносных программ, неправомерного доступа к компьютерной информации, принципов и алгоритмов организации компьютерных сетей, программного обеспечения и пр.;

4) иных вещественных доказательств и документов, имеющих значение для дела;

5) разыскиваемого лица.

Поскольку одним из основных процессуальных способов изъятия вещественных доказательств является обыск, целесообразно уделить особое внимание не только самому факту его проведения, но и процессу подготовки к нему (разумеется, в случаях, когда такая возможность имеется). Как показывает практика, среду, в которой проводится обыск, можно разделить на два вида – «агрессивная», когда рассчитывать на содействие сотрудников или владельцев не приходится, и «позитивная» – когда собственник заинтересован в установлении истины.

В первом случае подготовка к обыску должна базироваться в основном на материалах оперативных разработок. Сам факт возможного проведения обыска должен оставаться непредсказуемым для подозреваемого до последнего момента, для исключения возможности уничтожения следов.

Во втором случае подготовка может быть более проработана. Необходимо получить схему проводки локальной вычислительной сети с по кабинетной расстановкой компьютеров. По информации файлового сервера в режиме реального времени установить, кто и с какой задачей работает в настоящий момент, после этого проводить обыск на рабочем месте. Если имеется возможность, целесообразно заблаговременно установить специальную технику. Это позволит задержать преступника с поличным.

На подготовительной стадии следователь должен решить ряд вопросов организационного характера. Необходимо получить максимум информации об условиях и обстановке места, где предстоит произвести обыск. Для получения указанных данных может быть использована как

доказательственная, так и не процессуальная информация. В процессе планирования обыска следователь собирает необходимую информацию и решает конкретные задачи:

1.Сбор сведений об искомых объектах. Подробно выясняются вид и содержание информации, которая предположительно могла попасть к обыскиваемому преступным путем; характер вредоносных программ, вирусов; программные средства, которые в состоянии определить их наличие, и пр. Выясняется, на каком типе носителей машинной информации могут содержаться искомые данные. Необходимо также изучить личность владельца компьютера, его профессиональные навыки по владению компьютерной техникой. Если это программист со стажем, то для изъятия и анализа компьютерной информации может понадобиться специальное программное обеспечение для ее поиска, просмотра, распаковки, расшифровки или иного исследования.

2.Ознакомление с местом предстоящего обыска. Необходимо выяснить сведения о помещении (служебное или жилище). Устанавливается точный адрес, расположение и планировка, пути подхода, наличие службы охраны. Выясняется количество и тип компьютерной техники, наличие локальной сети и ее устройство, количество компьютеров, объединенных в сеть, возможность выхода в Интернет, удаленного доступа, средств защиты информации от несанкционированного доступа (программных и технических), наименование операционной системы. Указанные данные можно получить из документации по строению у провайдера путем оперативно-розыскных мероприятий.

3.Определение времени проведения обыска. Время выбирается с учетом
особенностей каждой конкретной ситуации. Поспешность или медлительность могут оказать негативное влияние на процесс расследования (наиболее удачными являются утренние часы – с 6.00 до 8.00). При решении этого вопроса необходимо попытаться обеспечить, прежде всего, внезапность проведения обыска. Внезапность проникновения на место обеспечивается общими тактическими приемами обыска: транспорт оставляется вне возможного поля зрения лиц, находящихся в обыскиваемом помещении; организуется наблюдение за окнами и входом в помещение; подход к дому осуществляется, как правило, несколькими группами, чтобы не вызвать подозрений. Для проникновения в квартиру используют помощь работников коммунальной службы, соседей.

4.Подготовка материально-технического обеспечения. Готовится переносной компьютер, при помощи которого можно будет осмотреть исследуемую информацию, носители машинной информации. Решается вопрос с транспортом и материалами для транспортировки при изъятии оборудования и машинных носителей.

5.Обеспечение необходимых участников обыска. Подбирается соответствующий специалист. В зависимости от обстановки возможно участие двух и более специалистов. По возможности подбираются понятые,

обладающие некоторыми познаниями в области компьютерной техники. В случае, когда возможно воспрепятствование проходу следственно-оперативной группе к месту обыска, необходимо решить вопрос о привлечении дополнительных сил и средств.

6.Получение санкции на производство обыска.

По прибытии к месту проведения обыска необходимо вести себя следующим образом:

- быстро и внезапно войти в обыскиваемый объект (или одновременно в несколько помещений);

- при оказании сопротивления со стороны лиц, находящихся на объекте обыска, – обыскиваемого, его родственников, охранников (сторожей), сотрудников организации и т. п. – принять срочные меры по нейтрализации противодействия и скорейшему проникновению в обыскиваемое помещение;

-организовать охрану места обыска и наблюдение за ним; охране под лежат периметр обыскиваемых площадей, СВТ, хранилища МНИ, все пункты (пульты) связи, охраны и электропитания, находящиеся на объекте обыска (в здании, помещении, на производственной площади), специальные средства защиты от несанкционированного доступа, хранилища ключей аварийного и регламентного доступа к СВТ, помещениям и другим объектам (пульты, пункты, стенды, сейфы и т. п.).

Детальный этап обыска является очень трудоемким и требует высокой квалификации как специалиста в области СВТ, так и всей следственно-оперативной группы.

Необходимо четко организовать поисковые мероприятия, направленные на поиск тайников, в которых могут находиться предметы, устройства и документы. Ими может служить и само СВТ – аппаратные и программные оболочки модулей. его составляющих. Например, внутри корпуса резервируется место для расширения и наращивания возможностей компьютера путем установки дополнительных плат. Это и приводит к большому объему дополнительного места внутри корпуса системного блока компьютера.

Поскольку наиболее распространенным носителем компьютерной информации являются магнитные дискеты, а они имеют сравнительно малые размеры – до 150 мм в диаметре и 2 мм в толщину, поиск их значительно затруднен. Если нет возможности, чтобы специалист просмотрел дискеты на месте, они должны быть изъяты для дальнейшего исследования (с соблюдением всех процессуальных правил).

Наряду с дискетами для хранения информации могут использоваться лазерные диски, т. к. они внешне не отличаются от аудио- и видеодисков, это делает возможным их хранение среди музыкальной или видео коллекции.

В связи с тем, что быстро проанализировать огромное количество информации на компьютере не всегда возможно, ее необходимо изъять для дальнейшего исследования. Устройства, на которых произведено копирование, должны быть соответствующим образом упакованы и

опечатаны. При этом следует иметь в виду, что нецелесообразно изымать все компьютерное оборудование, находящееся в месте обыска. В криминалистической литературе справедливо отмечается, что кроме технических сложностей подобного изъятия существуют и экономические: «в случае выхода из строя ПК банк, как правило, может "продержаться" не более двух дней, оптовая фирма – 3-5, компания обрабатывающей промышленности – 4-8, страховая компания – 5-6 дней. В связи с этим, радикальное изъятие компьютерной техники грозит последующими претензиями пострадавших организации».

Следователю стоит придерживаться следующих рекомендаций:

- при невозможности вскрытия корпуса СВТ (если это может привести к утрате информации, физическому повреждению ее носителя либо приведению к неисправному состоянию) необходимо изъять СВТ целиком для лабораторного исследования;

- все обнаруженные машинные носители информации (дискеты, пластиковые карточки, в т. ч. аудио-, видеокассеты и оптические компакт-диски) следует изъять для последующего анализа содержащихся на них данных на аттестованном исследовательском оборудовании, при отсутствии которого осмотр информации недопустим;

- нельзя использовать специальную поисковую и досмотровую технику, один из элементов которой – источник электромагнитных или магнитных излучений (метало детекторы, магниты, электронные стетоскопы, рентгеновские установки и т. п.), поскольку их применение может привести к стиранию информации на носителях;

- при необходимости изъятия жесткого диска персонального компьютера целесообразно изъять весь процессорный (системный) блок;

- в случае изъятия печатающего устройства (принтера) необходимо помнить, что в настоящее время возможна идентификация печатной продукции, изготовленной лишь на матричном (игольчатом) принтере. Для лазерного (электрографического) и струйного типов принтеров данный анализ практически невозможен.

На заключительном этапе составляются протокол следственного действия и описи к нему; вычерчиваются планы обыскиваемых помещений, схемы расположения СВТ относительно друг друга, строительных проемов, инженерно-технических коммуникаций, оконечных устройств электро несущей арматуры, а также принципиальная схема соединения СВТ между собой и с другими техническими устройствами; проводятся дополнительная фотосъемка и видеозапись.

При производстве выемки следует придерживаться рассмотренных нами рекомендаций по осмотру, обыску с учетом процессуальной процедуры производства данного следственного действия.

Допрос.

Допрос подозреваемого. При допросе лица в качестве подозреваемого в каждом конкретном случае, как минимум, необходимо получить ответы на следующие вопросы: «Где и кем (в какой должности) работал

подозреваемый; к какой компьютерной информации имеет доступ; какие операции с информацией он имеет право проводить; какова его категория доступа к информации; умеет ли работать подозреваемый на компьютере, владеет ли он определенным программным обеспечением, каков уровень его квалификации; кто научил его работать с конкретным программным обеспечением; какие идентификационные коды и пароли закреплены за ним (в том числе при работе в компьютерной сети); к каким видам программного обеспечения имеет доступ подозреваемый; каков источник его происхождения; обнаруживались ли программы, источник происхождения которых неизвестен; какие виды операций с компьютерной информацией данное лицо выполняло в исследуемое время; из какого источника или от кого конкретно подозреваемый узнал о содержании информации, к которой произвел неправомерный доступ; какой способ использовал подозреваемый для совершения неправомерного доступа к компьютерной информации; как подозреваемому удалось проникнуть в компьютерную систему (сеть); откуда подозреваемый мог узнать пароль (код) доступа к информации».

При установлении факта сбоев в работе средств компьютерной техники и устройств защиты информации в период работы данного лица в определенное время возможна постановка следующих вопросов: «Обнаруживал ли он сбои в работе программ, компьютерные вирусы и другие нарушения в нормальном функционировании программного обеспечения; обнаруживал ли подозреваемый случаи незаконного проникновения в свой компьютер, незаконного подключения к компьютерной сети; имеет ли он ограничения на допуск в помещения, где установлена компьютерная техника и какие именно; ознакомлен ли он с порядком работы с информацией, инструкциями о порядке проведения работ; не было ли случаев нарушения подозреваемым распорядка дня, порядка проведения работ, порядка доступа к компьютерной информации; не поступало ли к подозреваемому от других лиц предложений о передаче какой-либо компьютерной информации, программного обеспечения; неизвестны ли ему лица, проявлявшие интерес к получению идентификационных кодов и паролей».

Следует иметь в виду, что на первом допросе подозреваемый может попытаться объяснить факт неправомерного доступа к компьютерной информации некриминальными причинами (случайностью, стечением определенных обстоятельств, посторонним воздействием и т. п.). Может рассказывать о неправомерном доступе к компьютерной информации, как о факте, который совершился при отсутствии преступного умысла.

Для изобличения таких лиц хорошие результаты дает правильная реализация информации о преступной деятельности этого лица, полученной при проведении оперативно-розыскных мероприятий, а так же предъявление предметов и документов, принадлежащих подозреваемому и использовавшихся для неправомерного доступа к компьютерной информации. Умелое использование указанных сведений оказывает

определенное воздействие на допрашиваемого и позволяет получить правдивые показания на первом допросе.

Для успешного проведения допроса подозреваемого необходимо тщательно изучить все материалы дела, особенности личности подозреваемого, способы совершения преступления, доказательства, указывающие на виновность конкретного лица, и т. п. Ко времени привлечения лица в качестве подозреваемого следствие должно располагать двумя категориями доказательств. В первой из них предусматривается доказывание обстоятельств, свидетельствующих о том, что расследуемое событие (деяние) имело место, во второй – что это деяние совершено привлекаемым к уголовной ответственности лицом, и оно соответствует составу преступления, предусмотренного соответствующей статьей УК.

Как отмечает ряд авторов, допрос подозреваемого является одним из-важнейших, наиболее сложных и зачастую конфликтных следственных действий. Не преследуя цели рассмотрения тактики допроса подозреваемого в целом, отметим, что обвиняемые дают правдивые показания в тех случаях, когда убедятся, что расследованием установлен круг фактических данных. Поэтому обычно наиболее результативны приемы представления допрашиваемым собранных по делу доказательств и подробного изложения обстоятельств преступления без ссылки на источники.

Круг вопросов, подлежащих выяснению у подозреваемого, определяется конкретной следственной ситуацией, сложившейся по уголовному делу:

- при допросе подозреваемого в совершении создания вредоносных программ для ПК требуется установить уровень его профессиональной подготовленности как программиста, опыт работы по созданию программ конкретного класса на данном языке программирования, знание алгоритмов работы программ, подвергшихся воздействию;

- при расследовании преступлений, связанных с распространением вредоносных программ, особенно компьютерных вирусов, требуется выяснить: соблюдались ли требования противовирусной защиты, каков уровень владения соответствующими программами, каким образом был нарушен режим использования программных средств.

Кроме этого, необходимо установить конкретные факты несоблюдения режима доступа на объект, доступа к средствам вычислительной техники и программным средствам, способы преодоления программных и аппаратных средств защиты информации и другие обстоятельства, способные облегчить совершение преступления.

При допросе подозреваемого требуется выяснить все обстоятельства подготовки и совершения преступления, алгоритм функционирования вредоносной программы, а также на какую информацию и как она воздействует, характер наступающих последствий, связанных с нарушением работы ПК, их системы или сети и несанкционированным уничтожением,

блокированием, модификацией или копированием информации и какие действия по их преодолению могут быть наиболее эффективны.

В ходе допросов свидетелей выясняются следующие обстоятельства:

- на какой рабочей станции могли быть нарушены правила эксплуатации компьютерной сети и где она расположена;

- могли ли быть нарушены правила эксплуатации данной локальной сети на рабочей станции, расположенной в определенном месте (если нарушение правил произошло непосредственно на файловом сервере, то место нарушения этих правил может совпадать с местом наступления вредных последствий).

Время нарушения правил можно установить путем допроса свидетелей из числа лиц, участвующих в эксплуатации ПК. При этом могут быть заданы такие вопросы: «Каким образом в данной компьютерной системе фиксируются факты и время отклонения от установленных правил (порядка) эксплуатации ПК?». «Когда могло быть нарушено определенное правило эксплуатации ПК, после которого наступили известные вредные последствия?».

Следственный эксперимент.

На последующем этапе расследования преступлений в сфере высоких информационных технологий в целях проверки и иллюстрации собранных по делу доказательств, проверки и оценки следственных версий, установления причин и условий, способствовавших совершению преступления, получения новых доказательств возникает необходимость проведения следственного эксперимента. Как и другие следственные действия, проводящиеся при расследовании преступлений данной категории, следственный эксперимент имеет ряд специфических особенностей, определяющих его виды и специфику тактики.

Виды следственного эксперимента, проводимого при расследовании неправомерного доступа к компьютерной информации, варьируются и зависят, прежде всего, от способов совершения преступления (непосредственный или опосредованный доступ). В практике при расследовании анализируемого преступления проводятся эксперименты по:

- проверке возможности проникновения в помещение (через двери, окно, с отключением и без отключения сигнализации);

- проверке возможности подключения компьютерной техники и совершения непосредственного доступа к компьютерной информации;

- проверке возможности проникновения в закрытые зоны (путем подбора паролей, идентификационных кодов и установлению периода времени для данного подбора);

- проверке возможности подключения к компьютерной сети;

- проверке возможности электромагнитного перехвата;

- установлению периода времени, необходимого на подключение к компьютерной сети;

- установлению периода времени, необходимого на отключение технических средств защиты информации;

- установлению промежутка времени, необходимого для модификации, копирования компьютерной информации;

- проверке возможности совершения определенных операций к компьютерной информации в одиночку;

- проверке возможности совершения определенных операций с помощью конкретной компьютерной техники за определенный промежуток времени и др.

При проведении следственного эксперимента должны соблюдаться обще тактические положения:

- оптимальное ограничение количества участников следственного эксперимента;

- максимальное сходство условий проведения следственного эксперимента с условиями, в которых происходило совершение преступления;

- многократность проведения однородных опытов;

- проведение опытных действий в изменяющихся по степени сложности условиях;

- соответствие профессиональных навыков лица, осуществляющего опыты, профессиональным навыкам непосредственного участника исследуемого события;

- обеспечение безопасности участников следственного действия.

Заключение

В заключении хотелось бы напомнить, что процесс расследования рассматриваемого вида преступлений обусловлен установлением основных обстоятельств, подлежащих доказыванию, которые на различных этапах расследования уточняются и детализируются. Установление ряда вспомогательных обстоятельств только способствуют раскрытию основных обстоятельств, подлежащих доказыванию. Поэтому успех расследования преступления заключается в том, насколько правильно дознаватель или следователь определили основные обстоятельства, подлежащие доказыванию, в зависимости от сложившейся следственной ситуации на каждом этапе расследования.

По делам рассматриваемой категории в работе выделены типичные исходные следственные ситуации, по которым определены программы проведения первоначальных следственных действий, оперативно-розыскных и организационных мероприятий.

Следственные действия - часть сложного и многообразного комплекса процессуальных действий и решений, реализуемых в рамках досудебного производства. Следственные действия используются в доказывании как наиболее эффективный с точки зрения процессуальной техники механизм отыскания и закрепления сведений, имеющих значение для расследуемого уголовного дела. Ни одно уголовное дело не обходится без их производства. Именно путем своевременного, обоснованного и полного проведения

следственных действий обеспечиваются раскрытие преступления, установление и привлечение к уголовной ответственности виновного лица.

В связи с этим представлены разработанные методические рекомендации и схемы расследования первоначального этапа расследования отдельных видов преступлений в сфере высоких информационных технологий: при расследовании неправомерного доступа к охраняемой законом компьютерной информации; при расследовании создания, использования и распространения вредоносных программ для ПК; при расследовании преступления, совершенного в условиях неочевидности; при расследовании нарушения правил эксплуатации ПК, системы ПК или их сети. А также исследованы тактические особенности проведения отдельных следственных действии при расследовании данных видов преступлений: осмотр места происшествия, средств вычислительной техники, машинного носителя информации, машинного документа; обыск, выемка, допрос подозреваемого, подозреваемого, свидетелей; следственный эксперимент; предъявление для опознания; назначение экспертиз.

МВД РЕСПУБЛИКИ КАЗАХСТАН
КАРАГАНДИНСКАЯ АКАДЕМИЯ МВД РК
им. БАРИМБЕКА БЕЙСЕНОВА
ЮРИДИЧЕСКИЙ ИНСТИТУТ

КАФЕДРА ДОСУДЕБНОГО РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ

ЛЕКЦИЯ

Тема №3 Процессуальный порядок определения статуса подозреваемого, организация и проведение допроса подозреваемого

Лекцию подготовил:
доцент кафедры досудебного расследования преступлений Карагандинской академии МВД РК им. Б. Бейсенова
майор полиции Кемпирова Ж.С.

Лекция обсуждена и одобрена на заседании кафедры досудебного расследования преступлений «___» _____ 2018 года Протокол №___.

Караганда – 2018 г.

Тема: Процессуальный порядок определения статуса подозреваемого, организация и проведение допроса подозреваемого

Вид занятия: Лекция Время - 1 час.

План лекции:

Введение

1. Особенности проведения допроса подозреваемого на первоначальном этапе расследования преступлений в сфере высоких информационных технологий

Заключение

Цели занятия:

Методическая - подготовка и чтение лекции, выбор средств, обеспечивающих наглядное и полное усвоение дидактического содержания лекции.

Дидактическая - доведение до курсантов определенного комплекса учебной информации, определенного блока знаний на уровне и в объеме, предусмотренном программой и тематическим планом по вопросам организации и проведения следственных осмотров. Доведение материала с использованием методических и технических средств обучения, которые обеспечивают его усвоение.

Воспитательная - выработка психологической установки на возможность осознания, усвоения воспринимаемых научных знаний и понимания значения их реализации через соответствующие практические умения в будущей деятельности при проведении досудебного расследования.

Литература:

1. Аверьянова Т.В. Задачи компьютерно-технической экспертизы // Информатизация правоохранительных систем: Тезисы докладов междун. конф. В 2-х ч. М., 1998. 4.2.

2. Батурин Ю.М., Жодзишский А.М. Компьютерные правонарушения: криминализация, квалификация, раскрытие // Сов. государство и право, 1990. № 12. С.86-94.

3. Гортинский А.В., Пархоменко А.Н. Некоторые рекомендации по организации и проведению следственных действий при расследовании преступлений, совершенных с использованием печатающих средств персональных компьютеров // Материалы семинара: «Вопросы квалификации и расследования некоторых преступлений в сфере экономики». Саратов, 1998. 15-18 дек. С. 184-187.

4. КЕНЖЕТАЕВ Д.Т., КАЛИЕВ А.К., БАЛТАБАЕВ Т.Н. ПРИМЕРНЫЕ ОБРАЗЦЫ УГОЛОВНО-ПРОЦЕССУАЛЬНЫХ ДОКУМЕНТОВ ДОСУДЕБНОГО РАССЛЕДОВАНИЯ, КАРАГАНДА, 2014.

5. КРЫЛОВ В.В. ИНФОРМАЦИЯ КАК ЭЛЕМЕНТ КРИМИНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ // ВЕСТНИК МОСК. УН-ТА. СЕР. 11. ПРАВО. - М., 1998. - № 4. - С. 50-64.

6. РОССИНСКАЯ Е.Р ПРЕДМЕТ И ПРАКТИЧЕСКИЕ ПРИЛОЖЕНИЯ КОМПЬЮТЕРНО-ТЕХНИЧЕСКОЙ ЭКСПЕРТИЗЫ //ИНФОРМАТИЗАЦИЯ ПРАВООХРАНИТЕЛЬНЫХ СИСТЕМ: ТЕЗИСЫ ДОКЛАДОВ МЕЖДУНАР.КОНФ. В 2-Х Ч. М., 1998. Ч. 2.

7. Скоромников К.С. Расследование преступлений в сфере компьютерной информации // Руководство для следователей / Под ред. Н.А.Селиванова, В.А. Снеткова. М., 1997.

8. Толеубекова Б.Х. Компьютерная преступность: вчера, сегодня, завтра. Караганда, 1995.

9. ТЯЖИНА А.О., НОГАЙБАЕВА А.С. НОВЕЛЛЫ ДОСУДЕБНОГО РАССЛЕДОВАНИЯ ПО УПК РЕСПУБЛИКИ КАЗАХСТАН. УЧЕБНО-ПРАКТИЧЕСКОЕ ПОСОБИЕ (КРАТКИЙ АНАЛИЗ В СХЕМАХ). КАРАГАНДА, 2015.

10. ТЯЖИНА А.О., НОГАЙБАЕВА А.С., БЕЙСЕНБАЕВ А.Ж. ДОСУДЕБНОЕ ПРОИЗВОДСТВО ПО УГОЛОВНЫМ ДЕЛАМ: ОБРАЗЦЫ ПРОЦЕССУАЛЬНЫХ ДОКУМЕНТОВ, КАРАГАНДА, 2014.

11. Шурухнов Н.Г. Тактика следственного осмотра и освидетельствования Криминалистика: Курс лекций. М.: Эксмо. 2006.

Нормативные акты:

1. **Конституция Республики Казахстан** *(принята на республиканском референдуме 30 августа 1995 года), (с* изменениями и дополнениями *по состоянию на 10.03.2017 г.).*

2. Уголовно-процессуальный кодекс Республики Казахстан № 231-V-ЗРК *(с* изменениями и дополнениями *по состоянию на 09.01.2018 г.)*

3. Уголовный кодекс Республики Казахстан № 226-V-ЗРК *(с* изменениями и дополнениями *по состоянию на 09.01.2018 г.)*

4. Приказ Генерального Прокурора Республики Казахстан «Об утверждении правил приема и регистрации заявлений и сообщений об уголовных правонарушениях, а также ведения Единого реестра досудебных расследований» №89 от 19.09.2014г. с изм. и доп. от 10.08.2015 г. №99, 23.09.2016 №148.

5. Приказ Генерального прокурора Республики Казахстан от 22 сентября 2014 года №91 «Об утверждении Правил применения научно-технических средств фиксации хода и результатов следственных действий».

6. Закон Республики Казахстан от 11.01.2007 N 217-III «Об информатизации».

Введение

Одним из следствий массовой компьютеризации в Республике Казахстан явились преступления в сфере компьютерной информации. Интеграция современных информационных технологий практически во все области человеческой деятельности привела к тому, что с помощью компьютерных средств и систем совершаются «традиционные» преступления (например, присвоение, кража, мошенничество, фальшивомонетничество, лжепредпринимательство и др.). Компьютерные технологии используются с целью: фальсификации платежных документов; хищения наличных и безналичных денежных средств путем перечисления на фиктивные счета; отмывания денег; вторичного получения уже произведенных выплат; совершения покупок с использованием фальсифицированных или похищенных электронных платежных средств; продажи секретной информации и проч.

Преступления, сопряженные с использованием компьютерных технологий, представляют серьезную угрозу для любой располагающей компьютерной техникой организации. При этом наряду с высокой степенью

риска ей наносится и значительный материальный ущерб: вывод из строя электронно-вычислительной системы в результате возникновения нештатной технической ситуации или преступления может привести даже самый крупный банк к полному разорению за четверо суток, а более мелкое учреждение – за сутки.

Преступления, совершаемые с использованием компьютерных средств и систем, принято называть **компьютерными преступлениями.** Эта дефиниция со способом совершения и сокрытия преступления и, соответственно, с методикой его раскрытия и расследования.

Общественная опасность противоправных действий в области электронной техники и информационных технологий выражается в том, что они могут повлечь за собой нарушение деятельности автоматизированных систем управления и контроля различных (включая и жизнеобеспечивающие) объектов, серьезное нарушение работы ЭВМ и их систем.

Несанкционированные действия по уничтожению, модификации, искажению, копированию информации и информационных ресурсов, иные формы незаконного вмешательства в информационные системы способны вызвать тяжкие и необратимые последствия, связанные не только с имущественным ущербом, но и с физическим вредом людям. Опасность компьютерных преступлений многократно возрастает, когда они совершаются в отношении функционирования объектов жизнеобеспечения, транспортных и оборонных систем, атомной энергетики.

Вышеприведенные факты убедительно свидетельствуют о действительной остроте проблемы с преступлениями в сфере компьютерной информации. Преступления данной категории причиняют как серьезный экономический ущерб, так и непосредственную угрозу даже существованию человечества.

1. Особенности проведения допроса подозреваемого на первоначальном этапе расследования преступлений в сфере высоких информационных технологий

При расследовании компьютерных преступлений можно выделить три типичные следственные ситуации:

1. Собственник информационной системы собственными силами выявил нарушение целостности/конфиденциальности информации в системе, обнаружил виновное лицо и заявил об этом в правоохранительные органы.

2. Собственник информационной системы собственными силами выявил нарушение целостности/конфиденциальности информации в системе, не смог обнаружить виновное лицо и заявил об этом в правоохранительные органы.

3. Данные о нарушении целостности/конфиденциальности информации в информационной системе и виновном лице стали общеизвестными или

непосредственно обнаружены органом дознания (например, в ходе проведения оперативно-розыскных мероприятий по другому делу).

При наличии заподозренного виновного лица первоначальная задача следствия заключается в сборе с помощью собственника информационной системы и процессуальной фиксации доказательств:

а) нарушения целостности/конфиденциальности информации в системе;

б) размера ущерба, причиненного нарушением целостности/конфиденциальности информации;

в) причинной связи между действиями, образующими способ нарушения, и наступившими последствиями путем детализации способа нарушения целостности/конфиденциальности информации в системе и характера совершенных виновным действий;

г) отношения виновного лица к совершенным действиям и наступившим последствиям.

Т.к. подозреваемые задержаны сразу же после совершения преступления, для данной ситуации характерны следующие первоначальные следственные действия:

а) личный обыск задержанных;

б) допрос задержанных;

в) обыск по месту жительства задержанных.

Осмотр и обыск (выемка) по делам данной категории являются важнейшими инструментами установления обстоятельств расследуемого события.

Известно, что главными процессуальными способами изъятия вещественных доказательств являются осмотр, обыск и выемка.

Следует напомнить, что осмотр – это непосредственное обнаружение, восприятие и исследование следователем материальных объектов, имеющих отношение к исследуемому событию. Обыск – следственное действие, в процессе которого производится поиск и принудительное изъятие объектов, имеющих значение для правильного решения задач уголовного судопроизводства. Выемка – следственное действие, в процессе которого производится изъятие объектов, имеющих значение для правильного решения задач уголовного судопроизводства, в тех случаях, когда их местонахождение точно известно следователю и изъятие прямо или косвенно не нарушает прав личности.

Носители информации, имеющей отношение к расследуемому событию, могут быть с соблюдением установленного УПК РК порядка изъяты и приобщены к уголовному делу в качестве вещественного доказательства.

Для участия в обыске и выемке целесообразно приглашать специалиста в области компьютерной техники.

При осмотрах, обысках, выемках, сопряженных с изъятием ЭВМ, машинных носителей и информации возникает ряд общих проблем, связанных со спецификой изымаемых технических средств.

Так, необходимо предвидеть меры безопасности, предпринимаемые преступниками с целью уничтожения вещественных доказательств.

Например, они могут использовать специальное оборудование, в критических случаях создающее сильное магнитное поле, стирающее магнитные записи. Известна легенда о хакере, который создал в дверном проеме магнитное поле такой силы, что оно уничтожало магнитные носители информации при выносе их из его комнаты.

Преступник имеет возможность включить в состав программного обеспечения своей машины программу, которая заставит компьютер периодически требовать пароль, и, если несколько секунд правильный пароль не введен, данные в компьютере автоматически уничтожаются.

Желательно иметь с собой и использовать при обыске и осмотре устройство для определения и измерения магнитных полей.

Вещественные доказательства в виде ЭВМ, машинных носителей требуют особой аккуратности при транспортировке и хранении. Им противопоказаны резкие броски, удары, повышенные температуры, влажность. Все эти внешние факторы могут повлечь потерю данных, информации и свойств аппаратуры.

Не следует забывать при осмотрах и обысках о возможностях сбора традиционных доказательств (скрытых отпечатков пальцев на клавиатуре, выключателях и др., шифрованных рукописных записей и пр.).

Осмотру подлежат все устройства конкретной ЭВМ.

Фактически оптимальный вариант изъятия ЭВМ и машинных носителей информации – это фиксация их и их конфигурации на месте обнаружения и упаковка таким образом, чтобы аппаратуру можно было бы успешно, правильно и точно так же, как на месте обнаружения, соединить в лабораторных условиях или в месте производства следствия с участием специалистов.

Указанные следственные действия могут производиться с целями:

а) осмотра и изъятия ЭВМ и ее устройств;

б) поиска и изъятия информации и следов воздействия на нее в ЭВМ и ее устройствах;

в) поиска и изъятия информации и следов воздействия на нее вне ЭВМ.

По прибытии на место осмотра или обыска следует принять меры к обеспечению сохранности информации на находящихся здесь компьютерах и магнитных носителях. Для этого необходимо:

1) не разрешать кому бы то ни было из лиц, работающих на объекте обыска, прикасаться к работающим компьютерам, магнитным носителям, включать и выключать компьютеры;

2) самому не производить никаких манипуляций с компьютерной техникой, если результат этих манипуляций заранее не известен;

3) при наличии в помещении, где находятся СКТ и магнитные носители информации, взрывчатых, легковоспламеняющихся, токсичных и едких веществ или материалов как можно скорее удалить эти вещества в другое помещение.

Если компьютер работает, ситуация для следователя, производящего следственное действие без помощи специалиста, существенно осложняется, однако и в этом случае не следует отказываться от оперативного изъятия необходимых данных.

В данной ситуации:

а) определить, какая программа выполняется. Для этого необходимо изучить изображение на экране дисплея и по возможности детально описать его.

После остановки программы и выхода в операционную систему иногда при нажатии функциональной клавиши «F3» можно восстановить наименование вызывавшейся последний раз программы.

Можно осуществить фотографирование или видеозапись изображения;

б) остановить исполнение программы. Остановка осуществляется одновременным нажатием клавиш Ctrl-C, либо Ctrl-Break;

в) зафиксировать (отразить в протоколе) результаты своих действий и реакции компьютера на них;

г) определить наличие у компьютера внешних устройств – накопителей информации на жестких магнитных дисках и виртуального диска;

д) определить наличие у компьютера внешних устройств удаленного доступа к системе и определить их состояние (отразить в протоколе), после чего разъединить сетевые кабели так, чтобы никто не мог изменить или стереть информацию в ходе обыска (например, отключить телефонный шнур из модема);

е) скопировать программы и файлы данных. Копирование осуществляется стандартными средствами ЭВМ или командой DOS COPY;

ж) выключить подачу энергии в компьютер и далее действовать по схеме «компьютер не работает».

Если компьютер не работает, следует:

а) точно отразить в протоколе и на прилагаемой к нему схеме местонахождение ПК и его периферийных устройств;

б) точно описать порядок соединения между собой этих устройств с указанием особенностей (цвет, количество соединительных разъемов, их спецификация) соединительных проводов и кабелей; перед разъединением полезно осуществить видеозапись или фотографирование мест соединения;

в) с соблюдением всех мер предосторожности разъединить устройства компьютера, предварительно обесточив его;

г) упаковать раздельно носители на дискетах и магнитных лентах и поместить их в оболочки, не несущие заряда статического электричества;

д) упаковать каждое устройство и соединительные кабели, провода;

е) защитить дисководы гибких дисков согласно рекомендации изготовителя (вставить новую дискету или часть картона в щель дисковода);

ж) особой осторожности требует транспортировка винчестера.

Поиск и изъятие информации и следов воздействия на нее в ЭВМ и ее устройствах

В компьютере информация может находиться непосредственно в оперативном запоминающем устройстве (ОЗУ) при выполнении программы, в ОЗУ периферийных устройств и на внешних запоминающих устройствах (ВЗУ).

Наиболее эффективным и простым способом фиксации данных из ОЗУ является распечатка на бумагу информации, появляющейся на дисплее.

Если компьютер не работает, информация может находиться в ВЗУ и других компьютерах информационной системы или в «почтовых ящиках» электронной почты или сети ЭВМ.

Необходимо произвести детальный осмотр файлов и структур их расположения; лучше это осуществить с участием специалиста в лабораторных условиях или на рабочем месте следователя.

Следует обращать внимание на поиск так называемых «скрытых» файлов и архивов, где может храниться важная информация.

Периферийные устройства ввода-вывода могут также некоторое время сохранять фрагменты программного обеспечения и информации, однако для вывода этой информации необходимы глубокие специальные познания.

Осмотр компьютеров и изъятие информации производится в присутствии понятых, которые расписываются на распечатках информации, изготовленных в ходе осмотра.

В ходе осмотров по делам данной категории могут быть обнаружены и изъяты следующие виды важных документов, которые могут стать вещественными доказательствами по делу:

а) документы, носящие следы совершенного преступления, – телефонные счета, пароли и коды доступа, дневники связи и пр.;

б) документы со следами действия аппаратуры. Всегда следует искать в устройствах вывода (например, в принтерах) бумажные носители информации, которые могли остаться внутри их в результате сбоя в работе устройства;

в) документы, описывающие аппаратуру и программное обеспечение;

г) документы, устанавливающие правила работы с ЭВМ, нормативные акты, регламентирующие правила работы с данной ЭВМ, системой, сетью, доказывающие, что преступник их знал и умышленно нарушал;

д) личные документы подозреваемого или обвиняемого.

1. Проведение обыска в служебном помещении, на рабочем месте подозреваемого с целью обнаружения и изъятия физических носителей машинной информации и других документов, имеющих или возможно имеющих отношение к несанкционированному отношению программного обеспечения или носящих иные следы подготовки к хищению денежных средств.

2. Исследование:

- журналов сбойных ситуаций, рабочего времени ЭВМ, по передачи смен операторами;

- средств защиты и контроля банковских компьютерных систем, регистрирующих пользователей, моменты включения (активации) системы

либо подключение к ним абонентов с определенным индексом или без такового;

- протоколов вечернего решения, представляющих собой копию действий операторов, отображенную на бумажном носителе в ходе вечерней обработки информации, которая проводится по истечении каждого операционного дня;

- контрольных чисел файлов;

- всего программного обеспечения ЭВМ;

- «прошитых» микросхем постоянно запоминающих устройств, микропроцессоров и их схемного исследования.

3. Истребование и анализ технических указаний по обработке ежедневной бухгалтерской информации с перечнем выходящих форм.

4. Допрос лиц из числа инженеров-программистов, занимавшихся разработкой программного обеспечения и его сопровождением, специалистов отвечающих за защиту информации и специалистов электронщиков, занимающихся эксплуатацией и ремонтов вычислительной техники.

5. Назначение комплексной судебно-бухгалтерской и программно-технической экспертизы с привлечением специалистов правоохранительных органов, специалистов в области средств компьютерной техники, по ведению банковского учета с использованием средств компьютерной техники, документообороту, организации бухучета и отчетности, специалистов по обеспечению безопасности информации в компьютерных системах.

В ходе судебно-бухгалтерской экспертизы должно быть установлено, имеются ли нарушения требований положений о документообороте при отображении первичных документов в регистрах бухгалтерского учета и отчетности зафиксированных на машинном носителе, установлены их причины (с целью совершения преступления, злоупотребления или ошибки), ответственных лиц за эти нарушения.

Результаты программно-технической экспертизы должны быть оформлены как заключение экспертов для того, чтобы они могли играть роль доказательств в процессе суда. В настоящее время с помощью таких экспертиз могут решаться следующие задачи:

1. Воспроизведение и распечатка всей или части информации, содержащейся на физических носителях. В том числе находящихся в нетекстовой форме.

2. Восстановление информации, ранее содержавшейся на физических носителях и в последствии стертой или измененной по различным причинам.

3. Установление времени ввода, изменение, уничтожение либо копирование той или иной информации.

4. Расшифровка закодированной информации, подбор паролей и раскрытие систем защиты.

5. Установление авторства, места, средства, подготовки и способа изготовления документов (файлов, программ).

6. Выяснения возможных каналов утечки информации из компьютерной сети и помещений.

7. Выяснение технического состояния, исправности программно-аппаратных комплексов БИВС, возможности их адаптации под конкретного пользователя.

8. Установления уровня профессиональной подготовки отдельных лиц, проходящих по делу в области программирования и в качестве пользователя.

В соответствии со ст. 210 УПК РК имеются общие правила проведения допросов.

Статья 210. Общие правила производства допроса.

1. Перед допросом лицо, осуществляющее досудебное расследование, должно удостовериться в личности допрашиваемого. Если возникают сомнения, владеет ли допрашиваемый языком, на котором ведется производство по делу, выясняется, на каком языке он желает давать показания. В необходимых случаях он обеспечивается бесплатно переводчиком.

2. Лицу, вызванному на допрос, сообщается, в качестве кого, по какому уголовному делу он будет допрошен, разъясняются права и обязанности, предусмотренные настоящим Кодексом, о чем делается отметка в протоколе.

Лица, вызванные по одному делу, допрашиваются отдельно от других допрашиваемых лиц. Лицо, осуществляющее досудебное расследование, принимает меры к тому, чтобы допрашиваемые, вызванные по одному делу, не могли общаться между собой до начала допроса.

3. Допрос начинается с предложения рассказать об известных допрашиваемому лицу обстоятельствах дела. Если допрашиваемый говорит об обстоятельствах, явно не относящихся к делу, ему должно быть указано на это.

4. По окончании свободного рассказа допрашиваемому могут быть заданы вопросы, направленные на уточнение и дополнение показаний. Задавать наводящие вопросы запрещается.

5. Если показания связаны с цифровыми данными или иными сведениями, которые трудно удержать в памяти, допрашиваемый вправе пользоваться документами и записями, которые по ходатайству или с согласия допрашиваемого лица могут быть приобщены к протоколу.

6. Если в ходе допроса допрашиваемому лицу предъявлялись вещественные доказательства и документы, оглашались протоколы других следственных действий и воспроизводились материалы звуко- и (или) видеозаписи, киносъемки следственных действий, то об этом делается соответствующая запись в протоколе допроса. При этом в протоколе отражаются показания допрашиваемого лица, данные им по предъявленным доказательствам, оглашенным протоколам, воспроизведенным звуко- и (или) видеозаписям, киносъемкам следственных действий.

7. Допрос немого или глухого свидетеля, потерпевшего, подозреваемого, обвиняемого осуществляется с участием лица, владеющего навыками сурдоперевода. Участие этого лица в допросе отражается в протоколе.

8. При наличии у допрашиваемого психического или иного тяжкого заболевания его допрос осуществляется с разрешения врача и в его присутствии.

9. По решению лица, осуществляющего досудебное расследование, а также по просьбе подозреваемого, обвиняемого, свидетеля или потерпевшего при допросе могут быть применены звуко- и видеозаписи. О применении звуко- и видеозаписи допрашиваемый уведомляется до начала допроса.

10. Звуко- и видеозаписи должны отражать весь ход допроса и содержать полностью показания допрашиваемых лиц. Звуко- и видеозаписи части допроса, а также повторение специально для записи показаний, данных в ходе того же допроса, не допускаются.

11. По окончании допроса звуко- и видеозаписи полностью воспроизводятся допрашиваемому. Дополнения к звуко- и видеозаписям показаний, сделанные допрашиваемым, также заносятся на фонограмму и видеограмму. Звуко- и видеозаписи заканчиваются заявлением допрашиваемого, удостоверяющим их правильность.

12. Показания, полученные в ходе допроса с применением звуко- и видеозаписей, заносятся в протокол допроса. Протокол допроса должен также содержать: отметку о применении звуко- и видеозаписи и уведомлении об этом допрашиваемого; сведения о научно-технических средствах, условиях звуко- и видеозаписей и фактах их приостановления, причине и длительности остановки; заявление допрашиваемого по поводу применения звуко- и видеозаписей; отметку о воспроизведении звуко- и видеозаписей допрашиваемому; удостоверение правильности протокола и звуко- и видеозаписей допрашиваемым и лицом, осуществляющим досудебное расследование. Фонограмма и видео грамма хранятся при деле и по окончании досудебного расследования опечатываются.

Планируя преодоление возможного противодействия, необходимо учитывать такие личностные особенности допрашиваемого, как рефлексивность, гибкость или ригидность (застойность) его мышления, а также характерологические качества - агрессивность, конфликтность поведения, устойчивость или неустойчивость к стрессам, к неожиданно возникшим сложным обстоятельствам. Поскольку исходные данные о личности допрашиваемого часто бывают очень скудными, возможно построение нескольких наиболее вероятностных моделей поведения подлежащего допросу лица и вариантов тактики его допроса.

Подготовка допроса завершается составлением его плана. План может быть развернутым или кратким, письменным или зафиксированным только мысленно. Но он должен содержать систему вопросов, обусловленных общими задачами расследования. Отметим вопросы, наиболее существенные в правовом и психологическом отношениях, подлежащие обязательному включению в план допроса:

• обстоятельства, условия совершения деяния, участвовавшие в нем лица, их взаимоотношения и взаимодействие: поведение потерпевшего;

• мотивация и личностная детерминация деяния, условия, способствовавшие его совершению;

• способ совершения деяния, система использованных приемов и операций, индивидуализированных стереотипов поведения - навыков и привычек, орудий и приспособлений; действия, характеризующие устойчивые психические качества личности;

• способ сокрытия преступления, условия, способствовавшие его сокрытию;

• отношение обвиняемого (подозреваемого) к результатам совершенного деяния.

Подготовка к допросу, его планирование - это моделирование предстоящей деятельности, формирование ее ориентировочной основы.

Особенно детальной предварительной проработке подлежат различные аспекты допроса обвиняемого (подозреваемого).

Следователь критически оценивает материалы уголовного дела, выявляет взаимосвязь всех фактов, обстоятельств расследуемого происшествия, определяет место каждого факта в системе событий, классифицирует имеющиеся доказательства на “сильные” и “слабые”.

Предвидя возможность противодействия обвиняемого (подозреваемого), следователь мысленно актуализирует возможную систему приемов правомерного психического воздействия, планирует условия их реализации. Он должен тщательно продумать систему дополнительных, уточняющих, напоминающих и контрольных вопросов относительно всех имеющихся доказательств. Постановка этих вопросов может преследовать следующие цели:

• получение объяснений по имеющимся доказательствам, по доводам, выдвигаемым обвиняемым в свою защиту:

• получение новых сведений о фактах, имеющих значение для расследования;

• устранение противоречий в имеющихся доказательствах;

• проверка правдивости показаний;

• получение и накопление противоречивых ответов для изобличения ложности показаний.

В тех случаях, когда при допросе необходимо присутствие педагога, к его выбору следует подходить очень внимательно. Это должно быть авторитетное для подростка лицо, способствующее установлению коммуникативного контакта, взаимопониманию следователя и несовершеннолетнего.

В процессе подготовки к допросу следователь решает и такую тактически значимую задачу, как время и место его проведения, а также последовательность допроса различных лиц. При этом он должен учитывать психологию отдельных лиц, их позицию в отношении правосудия, групповой статус, динамику групповых отношений, взаимоотношения с другими проходящими по делу лицами.

В ряде случаев из тактических соображений можно срочно вызвать подозреваемого повесткой с нарочным, в других случаях целесообразнее отсроченный вызов, когда лицо, находясь в ситуации ожидания, испытывает нервное напряжение, а иногда предпринимает разоблачающие его действия.

Существенное значение для проведения допроса имеют внешние условия, обстановка общения. Выбор места проведения допроса - один из существенных тактических факторов. Чаще всего допрос проводится в кабинете следователя. Психологически важно, чтобы следователь и допрашиваемое лицо оставались наедине. Присутствие третьих лиц, как правило, сковывает коммуникативную активность.

Допрос подозреваемого. При допросе лица в качестве подозреваемого в каждом конкретном случае, как минимум, необходимо получить ответы на следующие вопросы: «Где и кем (в какой должности) работал подозреваемый; к какой компьютерной информации имеет доступ; какие операции с информацией он имеет право проводить; какова его категория доступа к информации; умеет ли работать подозреваемый на компьютере, владеет ли он определенным программным обеспечением, каков уровень его квалификации; кто научил его работать с конкретным программным обеспечением; какие идентификационные коды и пароли закреплены за ним (в том числе при работе в компьютерной сети); к каким видам программного обеспечения имеет доступ подозреваемый; каков источник его происхождения; обнаруживались ли программы, источник происхождения которых неизвестен; какие виды операций с компьютерной информацией данное лицо выполняло в исследуемое время; из какого источника или от кого конкретно подозреваемый узнал о содержании информации, к которой произвел неправомерный доступ; какой способ использовал подозреваемый для совершения неправомерного доступа к компьютерной информации; как подозреваемому удалось проникнуть в компьютерную систему (сеть); откуда подозреваемый мог узнать пароль (код) доступа к информации».

При установлении факта сбоев в работе средств компьютерной техники и устройств защиты информации в период работы данного лица в определенное время возможна постановка следующих вопросов: «Обнаруживал ли он сбои в работе программ, компьютерные вирусы и другие нарушения в нормальном функционировании программного обеспечения; обнаруживал ли подозреваемый случаи незаконного проникновения в свой компьютер, незаконного подключения к компьютерной сети; имеет ли он ограничения на допуск в помещения, где установлена компьютерная техника и какие именно; ознакомлен ли он с порядком работы с информацией, инструкциями о порядке проведения работ; не было ли случаев нарушения подозреваемым распорядка дня, порядка проведения работ, порядка доступа к компьютерной информации; не поступало ли к подозреваемому от других лиц предложений о передаче какой-либо компьютерной информации, программного обеспечения; неизвестны ли ему лица, проявлявшие интерес к получению идентификационных кодов и паролей».

Следует иметь в виду, что на первом допросе подозреваемый может попытаться объяснить факт неправомерного доступа к компьютерной информации некриминальными причинами (случайностью, стечением определенных обстоятельств, посторонним воздействием и т. п.). Может рассказывать о неправомерном доступе к компьютерной информации, как о факте, который совершился при отсутствии преступного умысла.

Для изобличения таких лиц хорошие результаты дает правильная реализация информации о преступной деятельности этого лица, полученной при проведении оперативно-розыскных мероприятий, а так же предъявление предметов и документов, принадлежащих подозреваемому и использовавшихся для неправомерного доступа к компьютерной информации. Умелое использование указанных сведений оказывает определенное воздействие на допрашиваемого и позволяет получить правдивые показания на первом допросе.

Для успешного проведения допроса подозреваемого необходимо тщательно изучить все материалы дела, особенности личности подозреваемого, способы совершения преступления, доказательства, указывающие на виновность конкретного лица, и т. п. Ко времени привлечения лица в качестве подозреваемого следствие должно располагать двумя категориями доказательств. В первой из них предусматривается доказывание обстоятельств, свидетельствующих о том, что расследуемое событие (деяние) имело место, во второй — что это деяние совершено привлекаемым к уголовной ответственности лицом, и оно соответствует составу преступления, предусмотренного соответствующей статьей УК.

Как отмечает ряд авторов, допрос подозреваемого является одним из-важнейших, наиболее сложных и зачастую конфликтных следственных действий. Не преследуя цели рассмотрения тактики допроса подозреваемого в целом, отметим, что обвиняемые дают правдивые показания в тех случаях, когда убедятся, что расследованием установлен круг фактических данных. Поэтому обычно наиболее результативны приемы представления допрашиваемым собранных по делу доказательств и подробного изложения обстоятельств преступления без ссылки на источники.

Круг вопросов, подлежащих выяснению у подозреваемого, определяется конкретной следственной ситуацией, сложившейся по уголовному делу:

- при допросе подозреваемого в совершении создания вредоносных программ для ПК требуется установить уровень его профессиональной подготовленности как программиста, опыт работы по созданию программ конкретного класса на данном языке программирования, знание алгоритмов работы программ, подвергшихся воздействию;

- при расследовании преступлений, связанных с распространением вредоносных программ, особенно компьютерных вирусов, требуется выяснить: соблюдались ли требования противовирусной защиты, каков

уровень владения соответствующими программами, каким образом был нарушен режим использования программных средств.

Кроме этого, необходимо установить конкретные факты несоблюдения режима доступа на объект, доступа к средствам вычислительной техники и программным средствам, способы преодоления программных и аппаратных средств защиты информации и другие обстоятельства, способные облегчить совершение преступления.

При допросе подозреваемого требуется выяснить все обстоятельства подготовки и совершения преступления, алгоритм функционирования вредоносной программы, а также на какую информацию и как она воздействует, характер наступающих последствий, связанных с нарушением работы ПК, их системы или сети и несанкционированным уничтожением, блокированием, модификацией или копированием информации и какие действия по их преодолению могут быть наиболее эффективны.

В ходе допросов свидетелей выясняются следующие обстоятельства:

- на какой рабочей станции могли быть нарушены правила эксплуатации компьютерной сети и где она расположена;

- могли ли быть нарушены правила эксплуатации данной локальной сети на рабочей станции, расположенной в определенном месте (если нарушение правил произошло непосредственно на файловом сервере, то место нарушения этих правил может совпадать с местом наступления вредных последствий).

Время нарушения правил можно установить путем допроса свидетелей из числа лиц, участвующих в эксплуатации ПК. При этом могут быть заданы такие вопросы: «Каким образом в данной компьютерной системе фиксируются факты и время отклонения от установленных правил (порядка) эксплуатации ПК?». «Когда могло быть нарушено определенное правило эксплуатации ПК, после которого наступили известные вредные последствия?».

Процессуальное закрепление результатов допроса участников. Основным способом процессуального закрепления результатов допроса служит протоколирование, порядок которого определен законом.

На практике бывают случаи, когда недобросовестные допрашиваемые под разными предлогами изменяют свои показания. Для противодействия подобным попыткам разработан ряд приемов:

– детализация показаний при протоколировании с максимально возможным сохранением особенностей речи допрашиваемого;

– предоставление допрашиваемому возможности в конце протокола сделать запись о соответствии текста его показаниям либо собственноручно занести свои показания в протокол;

– фиксирование в протоколе допрошенным каждого его ответа на поставленный вопрос.

Технические средства фиксации – звуко- и видеозапись имеют в сравнении с протоколом преимущества. Главное из них – максимально полное запечатление всей информации, полученной при допросе, ибо

дословно фиксируется все сказанное допрошенным и следователем, интонационные оттенки речи, обстановка допроса. Суд, прокурор, адвокат получают возможность объективно оценить ход и результаты допроса.

Однако технические средства существенно увеличивают время, затрачиваемое на проведение следственного действия. Поэтому их использование целесообразно при допросах лиц, чьи показания имеют особенно важное значение для дела; склонных изменять показания в ходе следствия; возможность вызова которых в суд исключена или сомнительна, а их показания важны для дела; не владеющих или слабо владеющих языком, на котором ведется допрос.

Точность и ясность изложения показаний допрашиваемого, грамматически правильное написание протокола.

Употребление в протоколе допроса слов и выражений, не свойственных допрашиваемому, может привести к тому, что в суде он может отказаться от своих показаний. Неточная и неполная запись показаний допрашиваемого приводит к тому, что при судебном разбирательстве дела может возникнуть противоречие между тем показанием, которое свидетель дает суду, и тем, которое записано следователем, хотя в действительности, если бы следователь записал показание более точно, никакого противоречия не было.

Протокол допроса должен быть написан грамотным, литературным языком, разборчиво и без исправлений. Стилизация показаний допустима лишь в целях исправления неправильно построенных фраз и устранения повторений. Встречающаяся еще на практике небрежная литературная редакция протоколов допроса, несомненно снижает значение этого процессуального документа, затрудняет понимание его, а иногда ведет и к ликвидации его процессуальной значимости.

Итак, простота, ясность, четкость и лаконичность и вместе с тем полнота, обстоятельность, конкретность и стройность изложения хода и результатов допроса — непреложные требования к качеству протокола.

В описательной части протокола очной ставки фиксируются:

1) факт выяснения следователем отношений между допрашиваемыми лицами и его предложение поочередно дать показания по обстоятельствам, относительно которых имеются существенные противоречия;

2) показания участников очной ставки, вопросы следователя каждому из них, а также вопросы ее участников друг другу (в том числе отведенные следователем) и ответы на них в той последовательности, в которой они давались на очной ставке;

3) предъявление доказательств участникам очной ставки;

4) оглашение ранее данных показаний, в том числе зафиксированных посредством звуко- и видеозаписи;

5) вопросы, заданные, с разрешения следователя, допрашиваемым иным участникам очной ставки;

6) ходатайства, заявленные участниками очной ставки.

В качестве средства фиксации аудио- и (или) видеозапись обеспечивают полноту содержания показаний, так как сохраняют всю информацию, поступающую от допрашиваемого; способствуют исключению необоснованных утверждений обвиняемого о том, что допрос был проведен с нарушением закона и протокольная запись не соответствует его показаниям; обязывают следователя вести допрос более целеустремленно; дисциплинируют как следователя, так и допрашиваемого. Прослушивание аудиозаписи и просмотр видеозаписи проведенного допроса способствует овладению мастерством его ведения, исправлению в ходе дальнейшего следствия сделанных в ходе допроса ошибок, более глубокому психологическому анализу данного допроса, более качественной подготовке последующих допросов.

Аудио- и (или) видеозапись позволяют не только проверить фактическую сторону допроса, но и проследить степень убежденности допрашиваемого, т.е. установить не только то, что он говорил, но и как он это говорил. Обеспечивая полноту содержания показаний, аудио- и (или) видеозапись позволяют записать их даже при условиях, когда протоколирование представляется затруднительным (допрос умирающего). Аудио- и (или) видеозапись являются наиболее полным и объективным отражением показаний допрашиваемого, обязывающих записывать показания в первом лице и по возможности дословно. Воспроизведение аудио- или видеозаписи, оказывает на участников процесса большее воздействие, чем ознакомление с протоколом, так как аудио- или видеозапись по сравнению с протокольной обладает большей эмоциональной силой. Обвиняемый, давший правдивые показания, которые записаны на магнитофоне, считает невозможным от них отказаться аналогично тем случаям, когда в деле имеются фотографии, фиксирующие стадии проверки и уточнения показаний на месте или производство следственного эксперимента.

Аудио- и (или) видеозапись запись имеет и тактическое значение — способствует изобличению других лиц. Она позволяет выдержать темп допроса, освобождает следователя от необходимости немедленно делать пометки или отдельные записи. Только аудио- или видеозапись может в полной мере зафиксировать тот переломный момент, когда допрашиваемый прекращает запирательство и суд по записи может установить, насколько добровольно и чистосердечно допрашиваемый давал показания. При применении аудио- или видеозаписи исключаются случаи заявлений в суде, что следователь проявил к допрашиваемому необъективность.

Необходимость применения аудио- или видеозаписи диктуется обстоятельствами дела, значимостью следственного действия, личностью допрашиваемого. В каждом конкретном случае это решает следователь. Однако аудио- или видеозапись может быть применена по просьбе обвиняемого, подозреваемого, свидетеля и потерпевшего.

Анализ следственной практики позволяет сделать вывод, что аудио- или видеозапись в основном применяется для записи показаний на допросе:

а) несовершеннолетних, когда важно проверить не только фактическую сторону показаний, но и тактику допроса, способ установления контакта с несовершеннолетним;

б) лиц, явившихся с повинной;

в) тяжелобольных или раненых, когда процесс протоколирования может отрицательно сказаться на здоровье допрашиваемого;

г) лиц, допрашиваемых при выполнении отдельного поручения.

Аудио- или видеозаписи в этом случае позволяет проверить, насколько уверенно допрашиваемый отвечает на вопросы, в какой последовательности они ставились и правильно ли были сформулированы;

д) лиц, в психической полноценности которых следователь сомневается.

Прослушивание таких записей экспертами-психиатрами будет иметь большое значение при даче ими заключений;

е) лиц, не владеющих языком, на котором ведется следствие (запись позволит проверить, насколько правильно сделан перевод, исключить ссылки обвиняемого на то, что показаний, записанных в переводе, он не давал);

ж) лиц, допрашиваемых на очной ставке;

з) лиц, расследование дела которых ведется группой следователей. Эти записи нужны для прослушивания следователями, которые не могли присутствовать на допросе и которым для последующего ведения следствия необходимо иметь полную и объективную информацию об этом допросе. Запись показаний может быть проведена во всех других случаях, когда в этом возникает необходимость, но нельзя согласиться с требованием применять аудио- или видеозапись при любом допросе. Проведение допроса с применением аудио- или видеозаписи намного сложнее в процессуальном и организационно-техническом отношении. Такой допрос занимает гораздо больше времени. Процессуальными гарантиями применения аудио- или видеозапись, обеспечивающими достоверность записи, являются следующие.

Во-первых, допрашиваемого ставят в известность о записи его показаний и обязаны выяснить заявления допрашиваемого по поводу проведения аудио- и (или)видеозаписи.

Во-вторых, в протоколе допроса отражаются технические условия применения аудио- или видеозаписи (марка магнитофона или видеокамеры, скорость записи, тип пленки), заявление по поводу применения звукозаписи;

отметка о воспроизведении звукозаписи допрашиваемому; удостоверение допрашиваемого о правильности протокола и звукозаписи.

В-третьих, аудио- или видеозапись части допроса, а также повторение специально для записи показаний в ходе того же допроса не допускаются. Но это требование закона не исключает применения аудио- или видеозаписи при дополнительном и повторном допросе, а также при проведении очной ставки.

В-четвертых, аудио- или видеозапись должна отражать время начала и конца допроса, место производства допроса, установочные данные допрашиваемого, фамилию и звание следователя. Обязательно записывается на аудио- или видеозапись разъяснение прав и обязанностей

допрашиваемому и его роспись в протоколе допроса, что они ему понятны. Данные об участии в допросе третьего лица — прокурора, защитника, педагога или переводчика и задаваемые ими вопросы также фиксируются на магнитофонную ленту.

В-пятых, по окончании допроса аудио- или видеозапись полностью воспроизводится допрашиваемому. Дополнения к аудио- или видеозапись также заносятся на фонограмму. Аудио- или видеозапись заканчивается заявлением допрашиваемого, в котором он удостоверяет ее правильность. Недопустимо стирание и вырезание фонограммы с последующей склейкой, монтаж видеозаписи. Склейка возможна лишь по техническим причинам и фиксируется на ленте, о чем указывается и в протоколе допроса. Фонограмма или видеозапись хранится в деле и по окончании предварительного следствия опечатывается. Желательно на кассету или пакет, где хранится пленка, наклеить реестр, в котором отмечаются все случаи воспроизведения записи. Если запись воспроизводилась в процессе допроса другого лица, об этом также делается отметка в реестре.

Заключение

В ходе изучения действующего уголовного законодательства в области регулирования компьютерного права и специфики расследования преступлений в сфере компьютерной информации были сделаны определенные обобщения:

Преступления в области компьютерной информации являются частью информационных преступлений: объединенных единым инструментом обработки информации – компьютером.

Известные на сегодня способы совершения компьютерных преступлений отличаются значительным и постоянно расширяющимся разнообразием. Совершают преступления данной категории чаще всего люди со специальной подготовкой в области автоматизированной обработки информации, причем более половины из их числа в составе преступных групп. Основная опасность исходит от внутренних пользователей – ими совершается более 90% преступлений.

Типичными следственными действиями, применяющимися при расследовании преступлений в сфере компьютерной информации, являются следственный осмотр, допрос (свидетеля, потерпевшего, обвиняемого, подозреваемого), производство судебных информационно-технических экспертиз, обыск и выемка, а также следственный эксперимент.

При расследовании преступлений в сфере компьютерной информации следственные задачи решаются в следующей последовательности:

- Установление факта совершения преступления: времени его совершения: способа и других обстоятельств, знание которых необходимо для успешного проведения расследования;

- установление лица (или лиц), совершившего преступное деяние: виновности и мотивов преступления;

- установление вредных последствий преступления и выявление обстоятельств, способствовавших преступлению.

При производстве следственных осмотра объектов преступления в целях обнаружения следов преступления, выяснения обстановки происшествия и иных значимых для дела обстоятельств целесообразно привлекать к ним технических специалистов с достаточно высокой степенью компетенции. Соответствующие специалисты призываются также для участия при производстве обыска (последующего осмотра изъятого) и следственного эксперимента.

Вышеуказанные участники следственных действий должны оказать помощь следователю при установлении факта совершения преступления, времени его совершения, способа совершения и обстоятельств, способствовавших преступлению.

Существенное значение для проведения допроса имеют внешние условия, обстановка общения. Выбор места проведения допроса - один из существенных тактических факторов. Чаще всего допрос проводится в кабинете следователя. Психологически важно, чтобы следователь и допрашиваемое лицо оставались наедине. Присутствие третьих лиц, как правило, сковывает коммуникативную активность.

Протокол допроса должен быть написан грамотным, литературным языком, разборчиво и без исправлений. Стилизация показаний допустима лишь в целях исправления неправильно построенных фраз и устранения повторений. Встречающаяся еще на практике небрежная литературная редакция протоколов допроса, несомненно снижает значение этого процессуального документа, затрудняет понимание его, а иногда ведет и к ликвидации его процессуальной значимости.

РЕЦЕНЗИЯ

на лекцию, подготовленную доцентом кафедры досудебного расследования Кемпировой Ж.С. по теме: «Процессуальный порядок определения статуса подозреваемого, организация и проведение допроса подозреваемого»

Представленная на рецензирование лекция, подготовленная Кемпировой Ж.С. соответствует требованиям, установленным для написания такого вида работ. Данная работа посвящена актуальной и практически востребованной проблеме – возникающих в ходе досудебного расследования по уголовным делам в сфере компьютерной информации и высоких технологий.

В данной лекции рассмотрены особенности проведения допроса подозреваемого на первоначальном этапе расследования преступлений в сфере высоких информационных технологий. Представленные вопросы освещены на достаточном теоретическом уровне, использованы различные монографические исследования по рассматриваемой теме, а также нормативные источники.

В данной работе на основе изучения правоприменительной практики и литературы, рассмотрены актуальные на сегодняшний день теоретические и прикладные аспекты тактики и технологии собирания и использования информации при расследовании преступлений, в сфере компьютерной информации и высоких технологий. Кроме того, высказаны соображения и предложения по их разрешению в соответствующем законодательстве РК и при правоприменительной работе сотрудников правоохранительных органов. Изучая эти проблемы и познания закономерностей этой деятельности, автор определенно выразил и дополнительно сформулировал ряд научных и практических выводов и рекомендаций по повышению эффективности правоотношений в целом и в частности по разрешению проблемных ситуаций по теме исследования.

Проводя изучение и анализ рассматриваемой темы, автор, в достаточной степени проявляет свое умение и приобретенные научно-исследовательские навыки, дает обобщение и выдвигает обоснованные выводы, оперируя материалами научных трудов, а также положениями нормативно-правовых актов. Учитывая изложенное, считаю, что лекция выполнена на достаточно хорошем теоретическом уровне и будет иметь примирительное значение в ходе практической деятельности.

Иллюстративный и раздаточный материал.

№	Тема занятия	Активные методы обучения Раздаточный материал	Примечание
1	Общая характеристика досудебного расследования в сфере компьютерной информации и высоких технологий	Макеты уголовных дел	
2	Понятие и значение преступления в сфере высоких информационных технологий	Макеты уголовных дел	
3	Следственные ситуации первоначального этапа расследования преступлений в сфере высоких информационных технологий в сфере компьютерной информации и высоких технологий	Макеты уголовных дел	
4	Поводы к началу досудебного расследования в сфере компьютерной информации и высоких технологий	Макеты уголовных дел	
5	Деятельность следователя по проверке законности и обоснованности повода к началу досудебного расследования в сфере компьютерной информации и высоких технологий	Макеты уголовных дел	
6	Процессуальный порядок определения статуса потерпевшего, организация и проведение допроса потерпевшего	Макеты уголовных дел	

Программное и мультимедийное сопровождение учебных занятий

Перечень программного и мультимедийного сопровождения учебных занятий

№	Перечень программного и мультимедийного сопровождения учебных занятий	Год подготовки	Язык обучения	Количество
1.	Тема №1: Общая характеристика досудебного расследования в сфере компьютерной информации и высоких технологий	2018	русский	17
2.	Тема №2: Понятие и значение преступления в сфере высоких информационных технологий	2018	русский	15
3.	Тема №3: Следственные ситуации первоначального этапа расследования преступлений в сфере высоких информационных технологий в сфере компьютерной информации и высоких технологий	2018	русский	10
4.	Тема №4: Поводы к началу досудебного расследования в сфере компьютерной информации и высоких технологий	2018	русский	13
5.	Тема №5: Деятельность следователя по проверке законности и обоснованности повода к началу досудебного расследования в сфере компьютерной информации и высоких технологий	2018	русский	9
6.	Тема №6: Процессуальный порядок определения статуса потерпевшего, организация и проведение допроса потерпевшего	2018	Русский	10

Начальник кафедры досудебного расследования преступлений
полковник полиции **Калиев А.К.**

«____»_____2018 г.

Карта учебно-методической обеспеченности специального курса (КУМОД)
«Расследование уголовных правонарушений, связанных в сфере компьютерной информации и высоких технологий»

/п	Наименование учебно-методических материалов	Авторы	на гос.языке (название и выходные данные)	на рус.языке (название и выходные данные)	Кол-во	
					в библиотеке	на кафедре
1	2	3	4	5	6	7
	Учебно-теоретические издания					
.	Учебное пособие	1.ТяжинаА.О., НогайбаеваА.С., Бейсембаев А.Ж.		Досудебное производство по уголовным делам: образцы процессуальных документов -2014г.	15	5
		2.КенжетаевД.Т., КалиевА.К., Балтабаев Т.Н.		Примерные образцы уголовно-процессуальных документов досудебного расследования -2014г.	100	10
		3.Генеральная Прокуратура РК		Приказ № 89 от 19.09.2014г. «О порядке приема и регистрации заявлений и сообщений о совершенных уголовных правонарушений»	10	1
		4. Сарсенбаев Т.Е. Хан А.Л.		Уголовный процесс. Досудебное производство: учебное пособие- Астана: ИКФ «Фолиант» 2000г.	150	7
		5. Сарсенбаев Т.Е. Смирнов С.В. Хан А.Л.		Расследование уголовного дела: кража чужого имущества: учебно-практическое пособие.- Астана: Акрам групп, 2006г.	50	1
		6. Авторский коллектив под ред. А.Н.Ахпанова	Бөтеннің мүлкін ұрлауға қатысты қылмыстық істі тергеу:оқу тәжірибелік құрал.- Қарағанды: 2010ж.	Примерные образцы уголовно-процессуальных актов досудебного производства: учебно-практическое пособие.- Алматы: Жеті жарғы, 2006г.	20	1
		7. Авторский коллектив под ред. Т.Е.Сарсенбаева	Қылмыстық іс жүргізу актілерінің үлгілері (сотқа дейінгі саты) : Тәжірибелік	Комментарий к	50	1
		8. Тяжина А.О.,			50	1

		Ногайбаева А.С.	оқу құралы.-Қарағанды: Болашақ Баспа: 2010ж.	изменениям и дополнениям в Уголовно-процессуальный кодекс Республики Казахстан	40	1
		9. Бейсенбаев А.Ж., Кондратьев И.В.		Новеллы досудебного расследования по УПК Республики Казахстан учебно-практическое пособие (краткий анализ в схемах). Караганда 2015.	10	1
		10. Тяжина А.О., Ногайбаева А.С.		Дознание по присвоению или растрате вверенного чужого имушествы образцы процессуальных документов. Учебно-практическое пособие. Караганда 2015.	30	1
		11. Калиев А.К., Кондратьев И.В., Хасенов Е.А.			20	1
		12. Калиев А.К., Шакжанов А.Т., Ақшолақов Р.Б.		Досудебное расследование отдельных категорий уголовных правонарушений (изнасилование). Караганда 2015.		
			Алаяқтық жолмен жасалған қылмыстарды сотқа дейінгі тергеп-тексеру. Әдістемелік нұсқаулықтар мен процессуалдық құжаттардың үлгілері. Оқу-тәжірибелік құрал. Караганда, 2015.	Досудебное расследование уголовных правонарушений (убиство). Учебно-практическое пособие (под общей редакцей д.ю.н., профессора Токубаева З.С.) Караганда 2015.	20	1
		13. А.К.Қалиев, Т.Н.Сүйлеменов, А.Ж.Бейсенбаев, А.Т.Шакжанов.			20	1
		14. Калиев А.К., Ногайбаева А.С., Хасенов Е.А.			40	1
		15. Калиев А.К., Сулейменов Т.Н., Бейсенбаев А.Ж., Шакжанов А.Т., Жаксыбаев Б.Е.	Сотқа дейінгі тергеп-тексеру барысындағы іс жүргізу құжаттарының үлгілері. Қарағанды:		40	1
		16. Бейсенбаев	2016.			1

		А.Ж. 17. Кондратьев И.В., Шульгин Е.П. 18. Т.З.Аймағанбетов, А.Қ.Қалиев, Т.Н.Сүлейменов, А.Ж.Бейсенбаев, А.Т.Шакжанов, А.С.Ноғайбаева, Б.Е.Жақсыбаев, Қ.М.Алимбеков, Е.А.Хасенов, Ж.С.Кемпирова 19. Ногайбаева А.С., Хасенов Е.А.	Қылмыстық құқық бұзушылықтың жекелей санаттың сотқа дейінгі тергеп тексеру. Тәжірибелік-оқу құралы. Қарағанды 2017. Қарап-тексеру жүргізуді ұйымдастыру бойынша тергеушілер мен анықтаушыларға жадынама. Қарағанды 2017.	Досудебное расследование отдельных видов уголовных правонарушений. Учебно- практическое пособие. Караганда 2017. Предварительное следствие по присвоению или растрате вверенного чужого имущества. Учебно- практическое пособие. Караганда 2017. Организационная деятельность следователя (дознавателя) по проведению следствнных осмотров. Учебно-практическое пособие. Караганда 2017. Квалификация процессуальных решений лица, осуществляющего досудебное расследование (образцы процессуальных документов). Караганда, 2017.	20	1 1
.4	Фондовая лекция, авторский курс лекций					
	Учебно-практические издания:					
	Тестовые	1. Авторский	ҚБСО пәні	Вопросы тестов для	-	1

.	материалы	коллектив кафедры 2.Авторский коллектив кафедры	бойынша тергеу-криминалистикалық мамандығы 3 курс тыңдаушылары на арналған тест тапсырмалары ҚБСО пәні бойынша жедел-іздестіру мамандығы 3 курс тыңдаушылары на арналған тест тапсырмалары	слушателей 3 курса следственно-криминалистической специализации Вопросы тестов для слушателей 3 курса оперативно-розыскной специализации	-	1
.	Электронный учебник	Тяжина А.О. Хан А.Л. Калиев А.К.	Қылмыстық істер бойынша сотқа дейінгі өндіріс: электрондық оқу құрал.-Қарағанды, 2010ж.		-	5
	Учебно-методические издания:					
.	Методические рекомендации по выполнению дипломных работ	Авторский коллектив кафедры	Дипломдық жұмыстарды дайындау, ресімдеу және қорғауға ұсыну жөніндегі ереже және әдістемелік нұсқаулар	Положение и методические указания по подготовке, оформлению и представ-лению к защите дипломных работ	5	2
.	Методические рекомендации по по организации и проведению ознакомительной практики слушателей	Авторский коллектив кафедры	ҚР ІІМ органдарының тергеу бөлімдерінде тергеу-кримина-листикалық мамандығы 2 курс тыңдаушыларының танысу	Программа и методические указания по организации и проведению ознакомительной практики слушателей 2 курса следственно-криминалисти-ческой специализации в следственных подразде-лениях МВД РК	5	2

	2 курса		тәжірибесін ұйымдастыру және жүргізу бойынша әдістемелік нұсқаулар мен бағдарлама			
.	Методические рекомендации по по организации и проведению дополнительной практики слушателей 3 курса	Авторский коллектив кафедры	ҚР ІІМ органдарының тергеу бөлімдерінде тергеу-кримина-листикалық мамандығы 3 курс тыңдаушыларының қосымша тәжірибесін жоспарланған сабақтардан тыс тәжірибе ұйымдастыру және жүргізу бойынша әдістемелік нұсқаулар мен бағдарлама	Программа и методические указания по организации и проведению дополнительной практики во внеучебное время слушателей 3 курса следственно-криминалистической специализации в следствен-ных подразделениях МВД РК	5	2
.	Методические рекомендации по организации и проведению стажировки	Авторский коллектив кафедры	ҚР ІІМ органдарының тергеу бөлімдерінде тергеу-кримина-листикалық мамандығы 4 курс тыңдаушыларының тағылым-дамасын ұйымдастыру және жүргізу бойынша әдістемелік нұсқаулар мен бағдарлама	Программа и методические указания по организации и проведению стажировки слушателей 4 курса след-ственно-криминалистической специализации в следствен-ных подразделениях МВД РК	5	2
.	Методические рекомендации по оформлению и	Авторский коллектив кафедры	Магистрлік диссертацияны дайындау, ресімдеу және қорғау тәртібі жөніндегі	Методические рекомендации по подготовке, оформлению и защите магистерских диссертаций	5	2

	выполнению магистерских диссертаций		әдістемелік ұсынымдар			
	Учебно-методические комплексы:					
.	Учебно-методические комплексы специальности	Авторский коллектив кафедры			-	1
.	Учебно-методические комплексы дисциплины	Авторский коллектив кафедры			-	1
	Электронный учебно-методический комплекс:					
.	Учебно-методические комплекс, разработанный для представления на электронном носителе и воспроизведения с помощью компьютера	Авторский коллектив кафедры			-	1
.	Тесты в электронном виде (программы тестирования)	Авторский коллектив кафедры	ҚБСО пәні бойынша тергеу-криминалистикалық мамандығы 3 курс тыңдаушылары на арналған тест тапсырмалары ҚБСО пәні бойынша жедел-іздестіру мамандығы 3	Вопросы тестов для слушателей 3 курса следственно-криминалистической специализации Вопросы тестов для слушателей 3 курса оперативно-розыскной специализации	-	1

			курс тыңдаушылары на арналған тест тапсырмалары			
.	Тексты учебных пособий	1. Сарсенбаев Т.Е. Смирнов С.В. Хан А.Л. 2. Сарсенбаев Т.Е. Смирнов С.В. Хан А.Л. 3.Авторский коллектив под редакцией Т.Е.Сарсенбаева	Бөтеннің мүлкін ұрлауға қатысты қылмыстық істі тергеу:оқу тәжірибелік құрал.-Қарағанды: 2010ж. Қылмыстық іс жүргізу актілерінің үлгілері (сотқа дейінгі саты) : Тәжірибелік оқу құралы.-Қарағанды: Болашақ Баспа: 2010ж.	Расследование уголовного дела: кража чужого имущества: учебно-практическое пособие.-Астана: Акрам групп, 2006г.	- - -	1 1 -