Министерство образования и науки Республики Казахстан
РГП ПХВ «Евразийский национальный университет им. Л.Н. Гумилева»

Кафедра уголовно-правовых дисциплин

УТВЕРЖДАЮ
Декан юридического
факультета
д.ю.н., профессор
_____ Сматлаев Б.М.
«___» _____ 2021 г.

Рабочая (модульная) учебная программа (Syllabus)

LAWS 63006 - Уголовно-процессуальные и криминалистические методы противодействия преступности
(код и наименование модуля)

по дисциплине OMRPSKI 6309 - Основы методики расследования преступлений в компьютерной информации
(код и наименование дисциплины)

для обучающихся образовательной программы

7МО4204 – Судебная власть и Уголовная юстиция
(Код и наименование образовательной программы)

2021

	Евразийский национальный университет им. Л.Н. Гумилева	Рабочая (модульная) учебная программа (Syllabus)	Издание: первое

Разработчик
или разработчики _____ к.ю.н., .доцент Баймолдина С.М.
(Ф.И.О., занимаемая должность, ученая степень)

Рассмотрено на заседании кафедры уголовно-правовых дисциплин

протокол № 11 от « 15 » 06 2021 г.

Заведующий кафедрой _____ Сембекова Б.Р.
(подпись) (Ф.И.О.)

Одобрено на заседании Учебно-методической комиссии факультета

« 17 » 06 2020 г. Протокол № 11

Председатель УМК факультета _____ Жадауова Ж.

Ф ЕНУ 703-13-17 Рабочая (модульная) учебная программа (Syllabus). Издание первое

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

1. Краткое описание дисциплины: ознакомление обучающихся с основами методики расследования преступлений в компьютерной информации электронно-цифровых объектов с использованием тактико-криминалистических средств и методов обеспечения, основанных на современных достижениях наук цифровых технологий, научной организации труда.

Цели изучения учебной дисциплины: в разработке методологических основ изучения, ситуаций и ситуаций, связанных с раскрытием и расследованием преступлений в сфере компьютерной информации, их прогнозирование и анализ с целью своевременного предупреждения и разрешения в интересах эффективного производства предварительного следствия, и на основании полученных результатов обосновать необходимость дополнения общей части криминалистики новым частным учением о методике расследования преступлений в сфере компьютерной информации.

Формирование у обучающихся знаний и навыков, позволяющих выявлять и расследовать преступления в сфере компьютерной информации.

Задачи изучения учебной дисциплины: обучающиеся должны знать следующее: криминалистическую и криминологическую характеристику преступлений в сфере компьютерной информации; типичные поводы и основания для возбуждения уголовных дел о преступных посягательствах данного вида; основные сведения и документы, которые должны находится в распоряжении уполномоченного лица для принятия обоснованного решения о возбуждении уголовного дела при расследовании преступлений в сфере компьютерной информации; типичные следственные ситуации первоначального этапа их расследования; алгоритм действий следователя (дознавателя) в случаях, когда информация о мотивах, способе совершения преступного деяния и личности лица, его совершившего, отсутствует, а также других спорных случаях при расследовании ;

2. Пререквизиты

Для освоения данной дисциплины необходимы знания, умения и навыки, приобретённые при изучении следующих дисциплин: Уголовное право РК, Уголовно-процессуальное право РК, Криминалистика, Криминология, Особые уголовно-процессуальные производства.

Постреквизиты

Знания, умения и навыки, полученные при изучении дисциплины необходимы для освоения следующих дисциплин: современные методы борьбы с организованной преступностью, следственные действия, оперативно-розыскная деятельность.

3. Выписка из учебного плана

Курс___2_____
Семестр____3_____
Количество кредитов_____5_____

Виды занятий	Общее количество часов
Лекции	30
Семинарское занятие	15
СРО	105
Итого	150

ТЕМАТИЧЕСКИЙ ПЛАН ДИСЦИПЛИНЫ ПО МОДУЛЯМ

(в академических часах)

№ недели	Наименование модуля и программного материала	Количество часов
1-7	**Модуль 1. Источники теоретических основ криминалистической методики расследования преступлений в сфере компьютерной информации.**	
	Лекции	
	1.1. *Тема занятия:* Становление правоотношений в сфере компьютерной информации и криминализация компьютерных правонарушений. *Краткое содержание:* Понятие и сущность преступлений в сфере компьютерной информации. Состав и структура теоретических основ криминалистической методики расследования преступлений в сфере компьютерной информации (цифровой криминалистики). *Формы и методы обучения: с*лайдовая презентация, объяснительно-иллюстративные методы.	4
	1.2 *Тема занятия:* Методические основы расследования преступлений в сфере компьютерной информации. *Краткое содержание:* Состав, структура и особенности криминалистической характеристики преступлений в сфере компьютерной информации. Механизм следообразования при совершении преступлений в сфере компьютерной информации. Характеристика личности преступников в сфере компьютерной информации. Способы совершения преступлений в сфере компьютерной информации. Основные ситуации первоначального этапа расследования преступлений в сфере компьютерной информации. *Формы и методы обучения:* просмотр видеороликов и обсуждение в группе	4
	1.3 *Тема занятия:* Предварительное исследование компьютерных объектов при расследовании преступлений в сфере компьютерной информации. *Краткое содержание:* Общие положения предварительного исследования объектов кибернетического пространства. Обыск и выемка компьютерных объектов. Особенности осмотра отдельных видов компьютерных объектов *Формы и методы обучения:* просмотр видеороликов и обсуждение в группе	4
	1.4 *Тема занятия:* Получение и проверка вербальной информации, связанной с компьютерными объектами. *Краткое содержание:* Допрос. Следственный эксперимент. Основные возможности компьютерно-технических экспертиз и тактические рекомендации по их назначению. *Формы и методы обучения:* просмотр видеороликов и обсуждение в группе	4
	Практические (семинарские) занятия	
	1.1. *Тема занятия:* Правоотношения в сфере компьютерной информации и криминализация компьютерных правонарушений	2

	План семинарского занятия: Структура теоретических основ криминалистической методики расследования преступлений в сфере компьютерной информации (цифровой криминалистики). *Формы и методы обучения:* Мозговой штурм, работа в группах	
	1.2. Тема занятия: Методические основы расследования преступлений в сфере компьютерной информации. *План семинарского занятия:* Характеристика личности преступников в сфере компьютерной информации. Основные ситуации первоначального этапа расследования преступлений в сфере компьютерной информации. *Формы и методы обучения:* Просмотр видеоролика и обсуждение в группе.	2
	1.3 Тема занятия: Предварительное исследование компьютерных объектов при расследовании преступлений в сфере компьютерной информации. *План семинарского занятия:* Общие положения предварительного исследования объектов кибернетического пространства. Обыск и выемка компьютерных объектов. *Формы и методы обучения:* просмотр видеороликов и обсуждение в группе	2
	1.4 Тема занятия: Получение и проверка вербальной информации, связанной с компьютерными объектами. *План семинарского занятия:* Основные возможности компьютерно-технических экспертиз и тактические рекомендации по их назначению. *Формы и методы обучения:* просмотр видеороликов и обсуждение в группе	2
	СРО	
	1.1. *Тема и задание СРО:* Криминалистическая классификация преступлений в сфере компьютерной информации *Краткое содержание:* подготовить реферат по данной теме *Срок сдачи СРО: в понедельник 2 недели*	10
	1.2 *Тема и задание СРО:* Методические основы расследования преступлений в сфере компьютерной информации. *Краткое содержание:* Способы совершения преступлений в сфере компьютерной информации. Основные ситуации первоначального этапа расследования преступлений в сфере компьютерной информации. *Краткое содержание: п*одготовить эссе по данной теме *Срок сдачи СРО: в понедельник 2 недели*	10
	1.3 Тема и задание СРО: Особенности осмотра отдельных видов компьютерных объектов *Краткое содержание: п*одготовить эссе по данной теме *Срок сдачи СРО: в понедельник 3 недели*	10
	1.4 Тема занятия: Получение и проверка вербальной информации, связанной с компьютерными объектами. *Краткое содержание:* Основные возможности компьютерно-технических экспертиз и тактические рекомендации по их назначению. *Срок сдачи СРО: в понедельник 4 недели*	10
	Итого по модулю 1 16 лекций, 8 семинарских занятий, 40 СРО	**64**

	Модуль 2. Уголовно-правовая, криминалистическая и криминологическая характеристика преступлений в сфере компьютерной информации	
	Лекции	
	2.1. *Тема занятия:* Уголовно-правовая характеристика преступлений в сфере компьютерной информации *Краткое содержание:* Характеристика компьютерной информации. Уголовно-правая характеристика преступлений в сфере компьютерной информации. *Форма и методы обучения:* обзорная форма лекции, слайдовые презентации	4
	2.2. *Тема занятия:* Криминалистическая характеристика преступлений в сфере компьютерной информации *Краткое содержание:* Формирование модели преступления в сфере компьютерной информации. Исследование модели: построение типовых версий. *Форма и методы обучения:* решение кейс-задач	4
	2.3. *Тема занятия:* Проверка типичных версий при расследовании преступлений в сфере компьютерной информации *Краткое содержание:* Некоторые проблемы выявления преступлений в сфере компьютерной информации. Проверка версий при расследовании преступлений в сфере компьютерной информации. Особенности проведения отдельных следственных действий и тактических операций. *Форма и методы обучения:* слайдовая презентация.	4
	Практические (семинарские) занятия	
	2.1. *Тема занятия:* Криминологическая характеристика преступлений в сфере компьютерной информации *План лабораторного занятия:* Криминологическая характеристика преступлений в сфере компьютерной информации. *Форма и методы обучения:* анализ статистических сведений по данным видам преступлений, решение кейсовых задач	2
	2.2. *Тема занятия:* Криминалистическая характеристика неправомерного доступа к компьютерной информации *План лабораторного занятия:* Особенности обстановки совершения неправомерного доступа к компьютерной информации. Характеристика механизма неправомерного доступа к компьютерной информации. *Форма и методы обучения:* просмотр видеоролика и обсуждения.	2
	2.3. *Тема занятия:* Разновидности типичных версий при расследовании преступлений в сфере компьютерной информации *План лабораторного занятия:* Некоторые проблемы выявления преступлений в сфере компьютерной информации. Проверка версий при расследовании преступлений в сфере компьютерной информации. Особенности проведения отдельных следственных действий и тактических операций. *Форма и методы обучения:* работа в малых группах, разработка версий.	2
	СРО	
	2.1. *Тема и задания СРО:* подготовить эссе по данной теме Криминологическая характеристика преступлений в сфере компьютерной информации.	7

	Краткое содержание: Факторы, детерминирующие совершение преступлений в сфере компьютерной информации. *Сроки сдачи СРО:* в понедельник 4 недели	
	2.2. *Тема и задания СРО:* подготовить реферат по данной теме Криминалистические значимые аспекты неправомерного доступа к компьютерной информации *Краткое содержание*: подготовить глоссарий и слайд по данной теме. *Сроки сдачи СРО:* в понедельник 5 недели	8
	2.3. *Тема и задания СРО:* подготовить слайдовую презентацию на тему: Особенности производства основных следственных действий при расследовании неправомерного доступа к компьютерной информации. *Краткое содержание*: Основные способы расследование неправомерного доступа к компьютерной информации. Применение тактических действий и следственных приемов. *Сроки сдачи СРО:* в понедельник 6 недели	8
	Итого по модулю 2 **лекций - 12, семинаров - 6, СРО - 23**	**41**
ИТОГО		**150**

4. Краткая организационно-методическая характеристика дисциплины
Виды контроля учебных достижений:

Рубежный 1 принимается в форме коллоквиума по вопросам или по тестам для этого вида контроля, представленный в УМКД

Рубежный 2 принимается в форме коллоквиума по вопросам или по тестам для этого вида контроля, представленный в УМКД

Итоговый: экзамен в устной форме по экзаменационным билетам, утвержденным на заседании кафедры.

Политика и процедуры курса

Дисциплина является элективной. Объем учебной нагрузки составляет 6 кредитов, из них 30 часов - лекций, 30 часов - семинарские занятия, 120 часов – самостоятельная работа обучающихся.

Требования: обязательное посещение аудиторных занятий, активное участие в обсуждении вопросов, предварительная подготовка к лекциям и семинарским занятиям по рекомендованным источникам, качественное и своевременное выполнение заданий по СРО, участие во всех видах контроля (текущий контроль, контроль СРО, рубежный контроль, промежуточный контроль).

5. Система оценки результатов учебных достижений обучающихся

Знания, умения и навыки студентов оцениваются по следующей системе

Оценка по буквенной системе	Цифровой эквивалент	Баллы (%-ное содержание)	Оценка по традиционной системе
A	4,0	95-100	Отлично
A-	3,67	90-94	
B+	3,33	85-89	Хорошо

B	3,0	80-84	
B-	2,67	75-79	
C+	2,33	70-74	
C	2,0	65-69	Удовлетворительно
C-	1,67	60-64	
D+	1,33	55-59	
D-	1,0	50-54	
FX	0,5	25-49	Неудовлетворительно
F	0	0-24	

Таблица 1

Оценка	Критерий
Оценка A	- ставится в том случае, когда дан полный, развернутый ответ на поставленный вопрос, показана совокупность осознанных знаний об объекте, проявляющаяся в свободном оперировании понятиями, умении выделить существенные и несущественные его признаки, причинно-следственные связи. Знание об объекте демонстрируется на фоне понимания его в системе данной науки и междисциплинарных связей. Ответ формулируется в терминах науки, изложен литературным языком, логичен, доказателен, демонстрирует авторскую позицию обучающихся.
Оценка A-	- ставится в том случае, когда дан полный, развернутый ответ на поставленный вопрос, показана совокупность осознанных знаний об объекте, доказательно раскрыты основные положения темы; в ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. Знание об объекте демонстрируется на фоне понимания его в системе данной науки и междисциплинарных связей. Ответ изложен литературным языком в терминах науки. Могут быть допущены недочеты в определении понятий, исправленные обучающимся самостоятельно в процессе ответа.
Оценка B+	- ставится в том случае, когда обучающимся дан полный, развернутый ответ на поставленный вопрос, доказательно раскрыты основные положения темы в ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. Ответ изложен литературным языком в терминах науки. В ответе допущены недочеты, исправленные обучающимся с помощью преподавателя.
Оценка B	- ставится в том случае, когда дан полный, развернутый ответ на поставленный вопрос, показано умение выделить существенные и несущественные признаки, причинно-следственные связи. Ответ четко структурирован, логичен, изложен литературным языком в терминах науки. Могут быть допущены недочеты или незначительные ошибки, исправленные обучающимся с помощью преподавателя.
Оценка B-	- ставится в том случае, когда дан развернутый ответ на поставленный вопрос, показано умение выделить существенные и несущественные признаки, причинно-следственные связи. Ответ четко структурирован, логичен, изложен в терминах науки. Однако допущены незначительные ошибки или недочеты, исправленные обучающимся с помощью наводящих вопросов.
Оценка C+	- ставится в том случае, когда дан полный, но недостаточно последовательный ответ на поставленный вопрос, но при этом показано

	умение выделить существенные и несущественные признаки и причинно-следственные связи. Ответ логичен и изложен в терминах науки. Могут быть допущены 1-2 ошибки в определении основных понятий, которые обучающийся затруднился исправить самостоятельно.
Оценка C	- ставится в том случае, когда дан недостаточно полный и недостаточно развернутый ответ. Логика и последовательность изложения имеют нарушения. Допущены ошибки в раскрытии понятий, употреблении терминов. Обучающийся не способен самостоятельно выделить существенные и несущественные признаки и причинно-следственные связи. Обучающийся может конкретизировать обобщенные знания, доказав на примерах их основные положения только с помощью преподавателя. Речевое оформление требует поправок, коррекции.
Оценка C-	- ставится в том случае, когда дан неполный ответ, логика, и последовательность изложения имеют существенные нарушения. Допущены грубые ошибки при определении сущности раскрываемых понятий, теорий, явлений, вследствие непонимания обучающимся их существенных и несущественных признаков и связей. В ответе отсутствуют выводы. Умение раскрыть конкретные проявления обобщенных знаний не показано. Речевое оформление требует поправок, коррекции.
Оценка D+	- ставится в том случае, когда дан неполный ответ. Присутствует нелогичность изложения. Обучающий затрудняется с доказательностью. Масса существенных ошибок в определениях терминов, понятий, характеристике фактов, явлений. В ответе отсутствуют выводы. Речь неграмотна. При ответе на дополнительные вопросы Обучающий начинает осознавать существование связи между знаниями только после подсказки преподавателя.
Оценка D	- ставится в том случае, когда дан неполный ответ, представляющий собой разрозненные знания по теме вопроса с существенными ошибками в определениях. Присутствуют фрагментарность, нелогичность изложения. Обучающий не осознает связь данного понятия, теории, явления с другими объектами модуля (дисциплины). Отсутствуют выводы, конкретизация и доказательность изложения. Речь неграмотная. Дополнительные и уточняющие вопросы преподавателя не приводят к коррекции ответа обучающегося не только на поставленный вопрос, но и на другие вопросы модуля (дисциплины).
Оценка FX	- ставится в том случае, если обучающийся обнаружил пробелы в знании основного материала, предусмотренного программой, не освоил более половины программы модуля (дисциплины), в ответах допустил принципиальные ошибки, не выполнил отдельные задания, предусмотренные формами текущего, промежуточного и итогового контроля, не проработал всю основную литературу, предусмотренную программой.
Оценка F	- ставится в том случае, когда обучающийся не смог дать ответ по теме вопроса, не владеет категориями и определениями либо допускает существенные ошибки в определениях, не освоил более половины программы модуля (дисциплины), не выполнил задания, предусмотренные формами текущего, промежуточного и итогового контроля, не проработал всю основную литературу, предусмотренную программой.

6. Учебно-методическая обеспеченность дисциплины

№	Автор, наименование, год издания	Носитель информа-ции	Имеется в наличии (шт.)	
			В библиотеке	На кафедре
Основная литература				
1	Вещественные доказательства: Информационные технологии процессуального доказывания / под общ. ред. В.Я. Колдина. М.: НОРМА, 2018. - 742 с.	учебник	10	+
2	Волеводз, А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества / А.Г. Волеводз. М.: Юрлитинформ, 2017. - 496 с.	учебник	10	+
3	Гаврилин, Ю.В. Расследование неправомерного доступа к компьютерной информации: Учебное пособие / Ю.В. Гаврилин; под ред. проф. Н.Г. Шурухнова. М.: ЮИ МВД РФ, Книжный мир, 2018. - 88 с.	учебник	10	+
4	Гаврилов, М.В. Осмотр при расследовании преступлений в сфере компьютерной информации / М.В. Гаврилов, А.Н. Иванов. М.: Юрлитинформ, 2007. - 168 с.	электрон-ный	10	+
5	Расследование преступлений в сфере компьютерной информации и электронных средств платежа : учебное пособие для вузов / С. В. Зуев [и др.] ; ответственный редактор С. В. Зуев, В. Б. Вехов. — Москва : Издательство Юрайт, 2021. — 243 с. ISBN 978-5-534-13898-6. Эл.ист.: https://urait.ru/bcode/467208	электрон-ный	10	+
Дополнительная литература				
1	Дворецкий, М.Ю. Преступления в сфере компьютерной информации: понятие, система, проблемы квалификации и наказания: монография / М.Ю. Дворецкий. Тамбов: Изд-во ТГУ им. Г.Р. Державина, 2003.-197с.	Учебное пособие	1	+
2	Дикарев, В.И. Защита объектов и информации от несанкционированного доступа / В.И. Дикарев, В.А. Заренков, Д.В. Заренков, Б.В. Койнаш; под ред.	Учебное пособие	1	+

	В.А. Заренкова. СПб: Стройиздат СПб, 2004. - 320 с.			
3	Жмыхов, А.А. Особенности современной компьютерной преступности за рубежом / А.А. Жмыхов // Преступное поведение (новые исследования): Сб. статей; под общей ред. проф. Ю.М. Антоняна. М.: ВНИИ МВД России, 2002. - С. 293-304.	Учебное пособие	1	+

ТЕЗИСЫ ЛЕКЦИЙ

ОСНОВЫ МЕТОДИКИ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

ТЕМА ЛЕКЦИИ: СТАНОВЛЕНИЕ ПРАВООТНОШЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ И КРИМИНАЛИЗАЦИЯ КОМПЬЮТЕРНЫХПРАВОНАРУШЕНИЙ.

ПЛАН:

1) Понятие и сущность преступлений в сферекомпьютерной информации.
2) Состав и структура теоретических основ криминалистической методики расследования преступлений в сфере компьютерной информации (цифровой криминалистики).

Формы и методы обучения: слайдовая презентация, объяснительно-иллюстративные методы.

С возникновением новых информационных технологий и процессов появилась настоятельная потребность в их правовом регулировании. И хотя право является универсальным регулятором общественных отношений, именно в сфере компьютерной информации оно оказалось не вполне готовым к их возникновению.

Не явилось исключением и уголовное право. С развитием информационного общества появилась потребность в защите информации. Проблема защиты компьютерной информации и информационных систем сейчас является одной из самых актуальных во всем мире. Пресечь наиболее опасные проявления человеческого поведения в информационной сфере - задача уголовного законодательства. Но «…киберпреступность становится настолько распространенной, что мы уже проиграли эту битву прежде, чем начали бороться всерьез с этим злом», сказал Рольф Хегэль, руководитель отдела по борьбе с киберпреступностью Европола (Europol's cybercrime unit)[1]. Самые технологически и экономически развитые страны пытаются решить, какие объединенные усилия силовых ведомств можно противопоставить нарастающей угрозе. Так, по заявлению директора Федерального бюро расследования США Роберта Мюллера в мае 2002 г., в десятку приоритетных направлений работы ФБР, наряду с антитеррористической деятельностью и борьбой с коррупцией, теперь входят борьба с преступлениями в сфере компьютерной информации и защита США от кибератак. Самые технологически и экономически развитые страны пытаются решить, какие объединенные усилия силовых ведомств можно противопоставить нарастающей угрозе. Так, по заявлению директора Федерального бюро расследования США Роберта Мюллера в мае 2002 г., в десятку приоритетных направлений работы ФБР, наряду с антитеррористической деятельностью и борьбой с коррупцией, теперь входят борьба с преступлениями в сфере компьютерной информации и защита США от кибератак.

Годовой мировой ущерб от компьютерных преступлений составляет более 5 млрд долл. По данным ООН, уже сегодня ущерб, наносимый компьютерными преступлениями, сопоставим с доходами от незаконного оборота наркотиков и оружия.

Одним из путей совершенствования борьбы с компьютерными преступлениями является согласование определенных материальных норм уголовного права различных государств мира. В течение последних лет международное сообщество проявляет значительный интерес к проблеме борьбы с компьютерной преступностью в разработанных международно-правовых документах.

При этом необходимо подчеркнуть, что понятия «компьютерные преступления» и «преступления в сфере компьютерной информации» не являются синонимами. Понятие компьютерных преступлений шире понятия преступлений в сфере компьютерной информации. Все компьютерные преступления по родовому объекту можно разделить на две группы:

- *преступления против информационной безопасности.* Компьютерная информация выступает здесь предметом преступного посягательства. Например, ст.ст. 272-274 УК РФ, ст.ст. 361-363 УК Украины, §1030 (a)(1) Свода Законов США «Несанкционированный доступ к информации с ограниченным доступом, касающейся национальной безопасности, международных отношений, атомной энергетики», ст. 478.1 УК Австралии «Несанкционированный доступ или модификация охраняемой компьютерной информации или программы» и др.;
- *преступления, где компьютерная информация является орудием или средством совершения другого преступления.* Эти составы находятся в других главах Уголовного кодекса. Например, ст. 212 УК Республики Беларусь «Хищение путем использования компьютерной техники»; §1030(a)(7) Свода Законов США «Вымогательство, угрозы причинения вреда с использованием компьютера»; ст. 206(1)(e) УК Канады «Использование компьютерных данных и технологий в целях извлечения прибыли путем создания финансовых пирамид» и др.

Таким образом, составы преступлений в сфере компьютерной информации объединяет единый родовой объект. Поскольку гл. 28 расположена в разд. IX УК РФ «Преступления против общественной безопасности и общественного порядка», то родовым объектом выступает общественная безопасность.

Но преступления в сфере компьютерной информации посягают не на все отношения общественной безопасности в целом, а лишь на одну ее часть - информационную безопасность. В основе обоих понятий лежит понятие «безопасности».

Информационная безопасность - это «состояние защищенности страны (жизненно важных интересов личности, общества и государства на сбалансированной основе) в информационной сфере от внутренних и внешних угроз».

С 80-х гг. XX в. во многих странах пришли к выводу, что правовая защита компьютерной информации с помощью общих положений национального уголовного законодательства является недостаточной. Многие государства осознали, что эффективное решение проблемы компьютерной преступности требует согласованных международных действий и сотрудничества. Так, на Генеральной Ассамблее ООН в сентябре 1991 г. отмечалось, что «рост преступности в сочетании с процессом приобретения ею транснационального характера ставит под угрозу внутреннюю безопасность государств, посягает на свободу человека жить без страха, а также может подорвать международные

отношения. Все это требует эффективных международных механизмов и более тесного сотрудничества между государствами».

Однако для того чтобы разрабатывать общие международные нормы и новые механизмы, необходим унифицированный подход к пониманию проблемы, выработка единой цели и универсальных принципов. На данный момент анализ зарубежного уголовного законодательства показывает, что отсутствует единообразное понимание того, какие деяния считать компьютерными преступлениями и каково должно быть юридическое определение каждого из них. От различных подходов к понятию и составам компьютерных преступлений возникают сложности в выявлении и наказании преступников, когда само деяние имеет место в одной стране, а его последствие наступает в другой, где такое деяние может быть не уголовно-наказуемым.

Несогласованный подход не способствует эффективному противодействию компьютерным преступлениям. В силу этого международно-правовые механизмы должны играть главную роль в унификации национального уголовного законодательства различных стран в этой сфере, в том числе в выработке общих понятий.

Учитывая, что значительная доля преступлений в сфере компьютерной информации совершается с использованием глобальных компьютерных сетей, в последнее десятилетие активно развивается международное сотрудничество различных стран в борьбе с преступлениями данного вида.

В 1983-85 гг. в Организации экономического сотрудничества и развития (ОЭСР) был создан специальный комитет для обсуждения возможности согласования уголовного законодательства различных стран об ответственности за компьютерные преступления. ОЭСР по результатам работы рекомендовал отнести к уголовно-наказуемым деяниям следующие деяния:

1) введение, изменение, стирание и/или подавление компьютерных данных и/или компьютерных программ, совершаемое умышленно с намерением осуществить незаконный перевод финансовых средств или других ценностей;

2) введение, изменение, стирание и/или подавление компьютерных данных и/или компьютерных программ, совершаемое умышленно с намерением сделать подлог;

3) введение, изменение, стирание и/или подавление компьютерных данных и/или компьютерных программ, или иные другие манипуляции с компьютерными системами, совершаемое умышленно с намерением воспрепятствовать функционированию компьютера и/или телекоммуникационной системы;

4) нарушение исключительного права обладателя охраняемой авторским правом компьютерной программы с намерением воспользоваться программой в коммерческих целях и реализовать ее на рынке;

5) доступ к компьютеру и/или к телекоммуникационной системе и перехват информации, выдаваемой компьютером и/или телекоммуникационной системой, который был получен как следствие осознанного действия без разрешения лица, ответственного за функционирование системы, путем нарушения охранных мер или других бесчестных или злоумышленных действий.

Первым документом Совета Европы, посвященным компьютерной преступности, стала Рекомендация № R 89(9) Комитета Министров стран - членов Совета Европы о преступлениях, связанных с компьютером, принятая 13.09.89, в которой был использован такой термин, как «преступление,

связанное с использованием компьютерных технологий». Данный документ содержал перечень рекомендованных к обязательному включению в национальное уголовное законодательство деяний. Также там приводился перечень тех деяний, по которым не было достигнуто согласия в признании необходимости их криминализации в законодательстве всех стран.

В перечень правонарушений, рекомендованных к обязательному включению во внутригосударственное уголовное законодательство в соответствии с указанной Рекомендацией, отнесены:

a) **Компьютерное мошенничество.** Ввод, изменение, стирание или подавление компьютерных данных или компьютерных программ или иное вмешательство в процесс обработки данных, которое влияет на результат обработки данных, что причиняет экономический ущерб или приводит к утрате собственности другого лица, с намерением получить незаконным путем экономическую выгоду для себя или для другого лица.

b) **Компьютерный подлог.** Введение, изменение, стирание или подавление компьютерных данных или компьютерных программ или иное вмешательство в процесс обработки данных, совершаемое таким способом или при таких условиях, как это устанавливается национальным законодательством, при которых эти деяния квалифицировались бы как подлог, совершенный в отношении традиционного объекта такого правонарушения.

c) **Причинение ущерба компьютерным данным или компьютерным программам.** Противоправное стирание, причинение ущерба, ухудшение качества или подавление компьютерных данных или компьютерных программ.

d) **Компьютерный саботаж.** Введение, изменение, стирание или подавление компьютерных данных или компьютерных программ или создание помех компьютерным системам с намерением воспрепятствовать работе компьютера или телекоммуникационной системы.

e) **Несанкционированный доступ.** Неправомочный доступ к компьютерной системе или сети путем нарушения охранных мер.

f) **Несанкционированный перехват.** Неправомерный и осуществленный с помощью технических средств перехват сообщений, приходящих в компьютерную систему или сеть, исходящих из компьютерной системы или сети и передаваемых в рамках компьютерной системы или сети.

g) **Несанкционированное воспроизведение охраняемой авторским правом компьютерной программы.** Неправомерное воспроизведение, распространение или передача в общественное пользование компьютерной программы, охраняемой законом.

h) **Несанкционированное воспроизведение микросхемы.** Неправомерное воспроизведение охраняемой законом микросхемы изделия на полупроводниках или неправомерное коммерческое использование или импорт с этой целью микросхемы или изделия на полупроводниках, изготовленного с использованием этой микросхемы.

Среди спорных составов преступлений названы:

a) **Изменение компьютерных данных или компьютерных программ.** Неправомерное изменение компьютерных данных или компьютерных программ.

b) **Компьютерный шпионаж.** Приобретение недозволенными методами или раскрытие, передача или использование торговой или коммерческой тайны, не имея на то права или любого другого правового обоснования, с целью

причинить экономический ущерб лицу, имеющему доступ к этой тайне, или получить незаконную экономическую выгоду для себя или для третьего лица.

c) **Несанкционированное использование компьютера.** Неправомерное использование компьютерной системы или сети, которое совершается: или

i) с пониманием того, что лицо, имеющее право на использование системы, подвергает ее значительному риску ущерба или системе или ее функционированию причиняется ущерб, или

ii) с намерением причинить ущерб лицу, имеющему право на использование системы, или системе или ее функционированию, или

iii) причиняет ущерб лицу, имеющему право на использование системы, или системе или ее функционированию.

d) **Несанкционированное использование охраняемой законом компьютерной программы.** Неправомерное использование компьютерной программы, которая охраняется законом и которая воспроизводится без права на воспроизведение, с намерением обеспечить незаконную экономическую прибыль для себя или для другого лица или причинить ущерб обладателю соответствующего права.

Рекомендация № R 89(9) предусмотрела, что в положениях уголовного закона должны содержаться как можно более точные описания уголовно-наказуемых деяний. Этот принцип ясности является чрезвычайно важным, но, к сожалению, не все государства ему следуют (в частности, Россия его не восприняла).

В то же время вышеупомянутая Рекомендация сама не содержала четкой формулировки понятия «преступление, связанное с использованием компьютерных технологий». Оно выводилось из перечня деяний, указанных в Рекомендации и дающих представление о таких преступлениях.

Данный документ послужил ориентиром для многих европейских стран в совершенствовании уголовного законодательства, и в то же время способствовал сближению национального уголовного законодательства различных стран.

Но необходимо учитывать, что данный документ носит лишь рекомендательный характер. И при всем положительном влиянии не по всем принципиальным вопросам европейские государства достигли достаточной степени сближения. На практике это привело к проблемам в согласованной борьбе с преступлениями в сфере компьютерной информации. Кроме этого, недостатком Рекомендации было и то, что в ней не содержались уголовно-процессуальные нормы.

Следующим шагом в развитии международного сотрудничества в борьбе с компьютерными преступлениями явилась разработка в начале 90-х гг. рабочей группой МОУП Интерпол кодификатора компьютерных преступлений. Он был положен в основу автоматизированной информационно-поисковой системы. Данный кодификатор применяется при отправке запросов и сообщений о компьютерных преступлениях по сети МОУП Интерпол.

В соответствии с названным кодификатором все компьютерные преступления классифицированы следующим образом:

1.*QA - Несанкционированный доступ и перехват*: компьютерный абордаж (хакинг), несанкционированный доступ к компьютерной информации или сети, перехват информации и др.

2.*QD - Изменение компьютерных данных*: логическая бомба, троянский конь, «червь», компьютерный вирус и др.

3.*QF* - *Компьютерное мошенничество*: мошенничество с банкоматами, с игровыми автоматами, с платежными средствами, телефонное мошенничество и др.

4.*QR* - *Незаконное копирование*: копирование компьютерных игр, программного обеспечения, топологии полупроводниковых устройств и др.

5.*QS* - *Компьютерный саботаж*: нарушение работы ЭВМ, уничтожение, блокирование информации и др.

6.*QZ* - *Прочие компьютерные преступления*: хищение информации, составляющей коммерческую тайну (компьютерный шпионаж), использование компьютерных досок объявлений для преступной деятельности и др.

По этому перечню можно судить о том, что к преступлениям в сфере компьютерной информации относится весьма широкий спектр деяний. Но, опять же, не все эти деяния восприняты в национальных законах (так, в Уголовном кодексе РФ лишь часть этих деяний отнесена к уголовно-наказуемым).

В рамках Группы Восьми (G-8) в течение 90-х гг. проводилось множество совещаний по проблеме компьютерной преступности. В частности, в июле 2000 г. на Окинаве (Япония) состоялось очередное совещание руководителей глав государств и правительств Группы Восьми. Было признано необходимым «выработать совместный подход в сфере борьбы с преступлениями в области высоких технологий, такими, как киберпреступления, которые могут серьезно угрожать безопасности и доверию в глобальном информационном обществе». И такой общий подход получил отражение в принятой на этом совещании «Окинавской Хартии о глобальном информационном обществе», в которой указано: «Усилия международного сообщества, направленные на развитие глобального информационного общества, должны сопровождаться согласованными действиями по созданию безопасного и свободного от преступности киберпространства…».

В октябре 2000 г. в Берлине проходила конференция стран Группы Восьми по проблемам киберпреступности. Это был очередной раунд переговоров по теме, которая с каждым годом становится все актуальнее. Самые технологически и экономически развитые страны пытались решить, какие объединенные усилия силовых ведомств можно противопоставить нарастающей угрозе. В конференции, помимо высших государственных чиновников и руководителей высокотехнологичных компаний, принимали участие около 100 интернет-экспертов силовых структур и частных организаций.

В ходе конференции представители полиции и органов правосудия многих стран отмечали недостаток в правовом регулировании Интернета. Национальные силовые структуры и международные организации, вроде Интерпола, призывали также не жалеть денег на подготовку и наем высококвалифицированных специалистов, способных эффективно противостоять хакерам. Между тем на практике пока компьютерные преступники в большинстве случаев опережают технологии защиты и противодействия им.

Рост компьютерной преступности и необходимость согласованного подхода государств к выработке уголовно-правовых и уголовно-процессуальных предписаний, направленных на борьбу с ней, в 1997 г. повлекло за собой создание Комитетом Министров Совета Европы Комитета экспертов по преступности в киберпространстве. На протяжении 3 лет Комитет

проводил изучение юридических проблем, возникающих при расследовании компьютерных преступлений. По результатам этой работы в 2000 г. был разработан проект Европейской Конвенции о киберпреступности. 18-22 июня 2001 г. проект был обсужден на заседании Европейского комитета по проблемам преступности. Конвенция была открыта к подписанию до 23.11.01 в Будапеште. Вступает она в силу в первый день месяца, следующего после истечения 3-месячного срока со дня, когда ее ратифицируют 5 государств, включая, по меньшей мере, 3 государства-члена Совета Европы. На 23.03.04 только три страны ратифицировали Конвенцию: Албания, Хорватия, Эстония. Всего ее подписали 33 государства, почти все члены Совета Европы и 4 государства не-члена (США, Япония, Канада, ЮАР). Россия Конвенцию не подписала.

Конвенция является комплексным документом, содержащим нормы различных отраслей права: уголовного, уголовно-процессуального, авторского, гражданского, информационного.

Конвенция по киберпреступности должна исправить недостатки борьбы с высокотехнологичными преступлениями, обеспечив эффективную координацию действий правоохранительных органов разных стран. Насколько эффективной окажется эта координация в действительности, а также стоит ли она той цены, которую придется заплатить гражданам, тайна частной жизни которых благодаря Конвенции находится под угрозой, - другой вопрос. должна исправить недостатки борьбы с высокотехнологичными преступлениями, обеспечив эффективную координацию действий правоохранительных органов разных стран. Насколько эффективной окажется эта координация в действительности, а также стоит ли она той цены, которую придется заплатить гражданам, тайна частной жизни которых благодаря Конвенции находится под угрозой, - другой вопрос.

Конвенция предлагает включить в национальное законодательство стран-участников нормы об уголовной ответственности за преступления в сфере компьютерной информации. В ней не дается определения понятия «преступление в сфере компьютерной информации». Оно заменено термином «киберпреступление» (cybercrime), который раскрывается с помощью перечня, включающего:

(1) деяния, направленные против компьютерной информации (как предмета преступного посягательства) и использующие ее в качестве уникального орудия совершения преступления;

(2) деяния, предметом посягательства которых являются иные охраняемые законом блага, а информация, компьютеры и т.д. являются лишь одним из элементов объективной стороны преступления, выступая в качестве, к примеру, орудия его совершения, составной части способа его совершения или сокрытия.

Объектом киберпреступлений, согласно Конвенции, является широкий спектр охраняемых нормами права общественных отношений, возникающих при осуществлении информационных процессов по поводу производства, сбора, обработки, накопления, хранения, поиска, передачи, распространения и потребления компьютерной информации, а также в иных областях, где используются компьютеры, компьютерные системы и сети. Среди них, учитывая повышенную общественную значимость, выделяются правоотношения, возникающие в сфере обеспечения конфиденциальности, целостности и доступности компьютерных данных и систем, законного

использования компьютеров и компьютерной информации (данных), авторского и смежных прав.

Объективная сторона преступлений в сфере компьютерной информации может быть выявлена через описание 4 групп общественно опасных деяний.

I. Против конфиденциальности, целостности и доступности компьютерных данных и систем:

- противозаконный доступ - получение доступа к компьютерной системе в целом или любой ее части без права на это, который может рассматриваться как преступление, если совершен в обход мер безопасности и с намерением завладеть компьютерными данными или иным бесчестным намерением, или в отношении компьютерной системы, соединенной с другой компьютерной системой (ст. 2);

- противозаконный перехват данных - осуществленный с использованием технических средств перехват без права на это непубличных передач компьютерных данных в компьютерную систему, из нее или внутри такой системы, включая электромагнитные излучения компьютерной системы, несущей такие компьютерные данные, если он совершен в обход мер безопасности и с намерением завладеть компьютерными данными или иным бесчестным намерением, или в отношении компьютерной системы, соединенной с другой компьютерной системой (ст. 3);

- нарушение целостности данных - повреждение, стирание, порчу, изменение или блокирование компьютерных данных без права на это, в том числе исключительно в случаях, повлекших за собой серьезные последствия (ст. 4);

- вмешательство в функционирование системы - создание без права на это серьезных помех функционированию компьютерной системы путем ввода, передачи, повреждения, удаления, порчи, изменения или блокирования компьютерных данных (ст. 5);

- противозаконное использование устройств - (а) производство, продажа, приобретение для использования, импорт, оптовую продажу или иные формы предоставления в пользование: (1) устройств, включая компьютерные программы, разработанных или адаптированных, прежде всего, для целей совершения преступлений; (2) компьютерных паролей, кодов доступа или иных подобных данных, с помощью которых может быть получен доступ к компьютерной системе в целом или любой ее части, с намерением использовать их с целью совершения преступлений; и (б) владение одним из предметов, упоминаемых выше, с намерением использовать его с целью совершения преступлений (ст. 6).

II. Связанные с использованием компьютеров:

- подлог с использованием компьютеров - ввод, изменение, стирание или блокирование компьютерных данных, приводящие к нарушению аутентичности данных с намерением, чтобы они рассматривались или использовались в юридических целях, как будто они остаются подлинными, независимо от того, являются ли эти данные непосредственно читаемыми и понятными (ст. 7);

- мошенничество с использованием компьютеров - лишение другого лица его собственности путем ввода, изменения, стирания или сокрытия компьютерных данных или вмешательства в функционирование компьютера или системы с целью неправомерного получения экономической выгоды для себя или для иного лица (ст. 8).

III. Связанные с содержанием данных (ст. 9):

- правонарушения, связанные с детской порнографией (порнографическими материалами, визуально отображающими участие несовершеннолетнего или кажущегося совершеннолетним лица в сексуально откровенных действиях, а также реалистические изображения, представляющие несовершеннолетних, участвующих в сексуально откровенных действиях), а именно: производство с целью распространения через компьютерные системы; предложение или предоставление через компьютерные системы; распространение или передача через компьютерные системы; приобретение через компьютерную систему для себя или для другого лица; владение детской порнографией, находящейся в компьютерной системе или в среде для хранения компьютерных данных.

IV. Связанные с нарушением авторского и смежных прав (ст. 10):

- нарушения авторского права, предусмотренного нормами внутригосударственного законодательства, с учетом требований Парижского Акта от 24.07.71 к Бернской Конвенции о защите произведений литературы и искусства, Соглашения о связанных с торговлей аспектах прав на интеллектуальную собственность и Договора об авторском праве Всемирной Организации Интеллектуальной Собственности (ВОИС), за исключением любых моральных прав, предоставляемых этими Конвенциями, когда такие действия умышленно совершаются в коммерческом масштабе и с помощью компьютерной системы;

- нарушение прав, связанных с авторским правом (смежных прав), предусмотренных нормами внутригосударственного законодательства, с учетом требований Международной конвенции о защите прав исполнителей, производителей звукозаписей и радиовещательных организации (Римская конвенция). Соглашения о связанных с торговлей аспектах прав интеллектуальной собственности и Договора ВОИС об исполнителях и звукозаписях, за исключением любых предоставляемых этими Конвенциями моральных прав, когда такие действия совершаются умышленно в коммерческом масштабе и с помощью компьютерной системы.

В качестве преступных последствий перечисленных деяний Конвенцией признается нарушение прав законных пользователей компьютерной информации, компьютеров, их систем или сетей. Установление в качестве обязательного признака объективной стороны более тяжких последствий (материального ущерба, противоправного использования полученной компьютерной информации и т.д.) оставлено на усмотрение государств. В целом нормы Конвенции не предусматривают обязательность наступления вредных последствий для каждого из указанных деяний.

Исходя из складывающейся в различных странах практики, ст. 12 Конвенции требует установления ответственности за правонарушения, предусмотренные ею не только для физических лиц, но и для юридических лиц. Условиями наступления ответственности юридического лица являются совершение действия с целью получения выгоды в пользу юридического лица его должностным лицом, занимающим руководящий пост, с использованием его полномочий по представлению юридического лица, принятию решений или осуществлению контроля за его деятельностью. Кроме того, Конвенция предписывает устанавливать ответственность юридических лиц и в случаях совершения противоправных действий иным работником под руководством должностного лица, занимающего руководящий пост, с целью получения выгоды в пользу юридического лица.

Согласно ч. 1 ст. 13 Конвенции установление конкретных санкций за совершение указанных деяний отнесено к ведению государств. По их усмотрению может устанавливаться уголовная ответственность для физических лиц, а также уголовная, гражданско-правовая либо административная ответственность юридических лиц. Предусмотренные внутригосударственным законодательством санкции должны быть эффективны, пропорциональны и убедительны.

Содружество независимых государств также не остается в стороне от выработки международно-правовых документов в сфере борьбы с компьютерными преступлениями. 01.06.01 Главами государств СНГ было подписано Соглашение о сотрудничестве государств - участников СНГ в борьбе с преступлениями в сфере компьютерной информации. Соглашение определяет такие основные понятия, как «преступление в сфере компьютерной информации», «компьютерная информация», «неправомерный доступ».

Согласно Соглашению, стороны признают в соответствии с национальным законодательством в качестве уголовно-наказуемых следующие деяния (если они совершены умышленно):

а) осуществление неправомерного доступа к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети;

б) создание, использование или распространение вредоносных программ;

в) нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации, если это деяние причинило существенный вред или тяжкие последствия;

г) незаконное использование программ для ЭВМ и баз данных, являющихся объектами авторского права, а равно присвоение авторства, если это деяние причинило существенный ущерб.

Определение понятий «существенный вред», «тяжкие последствия» и «существенный ущерб», согласно Соглашению, отнесено к компетенции каждой из сторон.

Кроме данного соглашения в рамках СНГ принят 17.02.96 Модельный Уголовный Кодекс для стран - участников СНГ. Он содержит разд. 12 «Преступления против информационной безопасности». Раздел охватывает деяния, отнесенные к компьютерным преступлениям, в том числе несанкционированный доступ к компьютерной информации (ст. 286), компьютерный саботаж (ст. 288), изготовление и сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети (ст. 291) и др.

Однако практически ни одно из государств - членов СНГ в своем национальном законодательстве в полной мере не реализовало рекомендации, содержащиеся в Модельном Уголовном кодексе. Это привело к тому, что нормы действующих уголовных кодексов стран СНГ не охватывают всего круга противоправных деяний, совершаемых в сфере компьютерной информации, что не соответствует цели защиты личности, общества и государства от таких преступлений.

В рамках ООН пока не разработана политика, конкретно касающаяся криминализации киберпреступлений. На Конгрессах ООН по предупреждению

преступности проходили различные семинары-практикумы, на которых обсуждались проблемы компьютерных преступлений, принимались рекомендации. Но они носят достаточно общий характер либо касаются только методических рекомендаций по расследованию транснациональных организованных преступлений.

Подводя итог, отметим, что именно точное, адекватное определение того или иного явления позволяет увидеть его суть и, если это явление имеет негативные последствия, предложить формы и методы борьбы с ним. Таким образом, первым шагом в борьбе с компьютерной преступностью, на наш взгляд, должно стать создание универсального развитого и детального понятийного аппарата. История сотрудничества в этом вопросе показывает, как сложно и долго идет в международном праве процесс выработки единого подхода к формулировке понятия компьютерного преступления. Так, международное сообщество до сих пор не определилось в выборе между терминами «компьютерное преступление», «киберпреступление», «преступление в сфере компьютерной информации».

Несмотря на многообразие международных документов, посвященных компьютерным преступлениям, не все они обязательны для исполнения для различных государств. Некоторые из них Россия либо не ратифицировала, либо даже не подписала. Кроме того, большинство из них относятся к категории так называемого «мягкого права», предписания которого не являются обязательными для государств-сторон.

И все же главным остается вопрос: почему государства, участвующие в выработке принципиальных документов, касающихся компьютерной преступности, в дальнейшем не предпринимают никаких шагов, чтобы включить данные нормы в свое национальное уголовное законодательство? На наш взгляд, причинами отсутствия должного внимания к компьютерной преступности могут выступать относительно низкий уровень участия в международных электронных коммуникациях, недостаточный уровень опыта в правоохранительной области и заниженные оценки социальных издержек, которые, как ожидается, могут влечь за собой преступления, совершаемые в электронной среде. В рамках глобальной компьютерной сети Интернет уголовно-правовая политика отдельного государства оказывает прямое воздействие на международное сообщество. Преступники могут совершать свои действия в электронной среде с территории определенного государства, где такие деяния не криминализованы, и таким образом они могут находиться под защитой закона такой страны. Даже если в круг конкретных национальных интересов того или иного государства не входит криминализация определенных деяний, оно может рассмотреть вопрос о принятии таких мер, с тем чтобы не превратиться в «правовую крышу» и не поставить себя в условия международной изоляции. Обеспечение международного сотрудничества правоохранительных и судебных органов различных государств невозможно без согласования материальных норм уголовного права в отношении компьютерных преступлений.

ТЕМА ЗАНЯТИЯ: ПРЕДВАРИТЕЛЬНОЕ ИССЛЕДОВАНИЕ КОМПЬЮТЕРНЫХ ОБЪЕКТОВ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ.

ПЛАН

1) Общие положения предварительного исследования объектов кибернетического пространства.
2) Обыск и выемка компьютерных объектов.
3) Особенности осмотра отдельных видов компьютерных объектов

На предварительной стадии экспертного исследования, в ходе выполнения осмотра поступивших объектов, эксперту следует обратить особое внимание на: формулировки поставленных вопросов, при необходимости согласовать вопросы со следователем; комплектность поступивших технических средств, их соответствие описанию в постановлении; решить вопрос о возможности подготовки полной копии исследуемых носителей информации либо согласовать со следователем возможность исследования данных непосредственно на исследуемом носителе; предварительно определиться с необходимым для исследования аппаратно-программным комплексом.

В ходе аналитической стадии большая часть исследования происходит с информационными объектами при постоянном использовании аппаратно-программных экспертных средств, и практически каждое действие эксперта приводит к изменению среды существования этих объектов, а иногда и самих объектов. В этом случае эксперт должен максимально возможно обезопасить как вещественные доказательства в целом, так и все криминалистически значимые информационные объекты. При изучении компьютерных баз данных исследования можно производить либо на полных копиях носителей информации, либо на копиях отдельных информационных объектов, если обеспечивается полный перенос существенных признаков.

Несмотря на разнообразие возможных конкретных экспертных задач, решаемых в ходе производства экспертизы баз данных, в начале аналитической стадии эксперту необходимо выполнить предварительный осмотр информационной среды, присутствующей на полученных носителях. Знание особенностей информационной среды определяет набор наиболее общих диагностических признаков многих информационных объектов и оказывает существенное влияние на дальнейший ход исследования:

· правильность установок даты/времени в «системных» часах (при исследовании CMOS системного блока). Влияет на определение правильности автоматической фиксации временных значений в прикладных и служебных данных на момент их изъятия;

· количество и размер разделов находящихся на устройствах внешней памяти, наличие свободных областей. Определяет наличие областей памяти, недоступных штатными средствами ОС стендового компьютера, а возможно и умышленно сокрытых;

· тип файловых систем разделов и возможности нахождения их на свободных областях. Определяет набор программных средств и методов доступа к элементам файловых систем;

· тип операционных систем, установленных на разделах носителя. Определяет наиболее общие правила управления компьютером (возможные типы файловых систем, возможные средства разграничения доступа, стандарты в размещении элементов файловых систем, правила журналирования работы системы, возможные классы используемых СУБД и прикладных программ работы с БД и т.п.);

· наличие, вид и активность средств разграничения доступа к элементам файловых систем. Влияет на выбор методов получения доступа к закрытым частям файловых систем (оперативные меры, «взлом» или подбор пароля, подключение носителя к информационной среде с полными правами и т.п.);

· перечень установленного программного обеспечения. Определяет круг прикладных задач, которые возможно могли решаться на компьютере с исследуемым носителем информации, их места расположения и возможность обработки файлов баз данных определённого формата.

Определяется место размещения файлов баз данных: просмотром настроек прикладных программ или СУБД; осмотром папок «Рабочего стола» и группы «Документы»; просмотром реестра MS Windows; ручным поиском по характерным именам файлов и каталогов; автоматизированным поиском по именам и типам файлов, по контексту. Отобранные для дальнейшего исследования файлы и папки следует описать стандартным для этих объектов набором частных признаков: место расположение, имя, дата создания, дата изменения, размер.

Одной из важных экспертных задач, решаемых на аналитической стадии, является установление соответствия информационного содержания исследуемой базы данных какой-либо предметной области и её структурных особенностей. Решение данной задачи возможно путём:

· обнаружения на исследуемых носителях одной из известных прикладных программ обработки БД, что предопределяет круг возможных прикладных задач решаемых ею. Структура базы данных этой программы также должна быть стандартной для данной версии программы. Возможно решение и обратной задачи. Совокупность выявленных на предыдущем этапе частных признаков файлов базы данных, являясь специфичной для прикладной программы определённого вида, позволит решать классификационную задачу по установлению этого вида программы обработки БД, а, следовательно, и определить вид стандартной для данной задачи структуры БД.

· В случае обнаружения базы данных неизвестной эксперту структуры вначале следует выяснить содержание и пределы описываемой ею предметной области. Для решения этой подзадачи в зависимости от конкретных условий можно: найти в каталоге с БД или прикладной программой обработки БД файлы с документацией на данную программу и изучить её; запустить прикладную программу обработки конкретной БД и изучить механизм её работы, информацию об обрабатываемых полях и их содержании; универсальной СУБД или программой-просмотрщиком изучить отдельные таблицы (для реляционных БД), обращая внимание на набор наиболее значимых частных признаков БД, содержащихся в её файлах - название полей, их тип, размер, содержание; изучить содержание иных файлов, находящихся в каталоге БД и подкаталогах. Достаточно часто прикладные программы обработки БД содержат в своём составе вспомогательные файлы, содержащие шаблоны подготавливаемых на основе БД деловых документов, иные сервисные файлы, либо сохраняют файлы отчётов текстового содержания или в виде электронных таблиц.

Далее экспертом должна быть решена задача по установлению наличия и видов связей между компонентами базы данных (обычно между различными таблицами одной БД). Для решения данной задачи эксперту следует: при наличии такой возможности, средствами универсальной СУБД или программы-просмотрщика просмотреть явное описание связей базы данных, хранящееся либо в её служебных данных, либо в технической документации; изучить названия таблиц БД и, сопоставив их с моделью предметной области, сделать предположение о месте и возможных связях этих таблиц; изучить названия и содержание полей различных таблиц и, выявив совпадения и сопоставив их с моделью предметной области, сделать предположение о возможных связях этих таблиц по данным полям.

В процессе аналитической стадии исследования компьютерных БД и СУБД периодически могут возникать потребности в переходе на стадию экспертного эксперимента. Экспертный эксперимент состоит в тестовой работе с БД и позволяет получить фактические данные, подтверждающие либо опровергающие построенную версию. Кроме того, экспертный эксперимент позволит: отследить изменения, происходящие в прикладных и служебных файлах АИС в ходе различных операций выполняемых с БД; изучить возможности обработки БД, предоставляемой конкретной прикладной программой; выявить наличие систем разграничения доступа, реализуемых программным путём; выявить права операторов данной АИС; получить образцы отчётов, генерируемых АИС в электронном и бумажном виде, для дальнейшего сравнительного исследования.

Дальнейшее изучение компьютерной БД и СУБД предполагает исследование объектов известной структуры и назначения.

Во многих случаях перед экспертом явно, либо косвенно ставится задача по установлению наличия в БД информации определённого содержания. Выполнение предыдущих этапов исследования делает данную задачу тривиальной. Наиболее эффективным является использование стандартных средств, встроенных в прикладную программу обработки БД (ручной просмотр, фильтры, запросы и отчёты). Для часто решаемых задач в отношении БД определённого вида возможна разработка средствами универсальной СУБД программного модуля под конкретную задачу.

Ещё одной группой объектов подлежащих исследованию на аналитической стадии, являются информационные объекты, генерируемые прикладной программой обработки БД. Они могут содержать признаки, характеризующие факт операции, время, место и средство её осуществления, идентификатор оператора и т.п., либо являться информационными копиями части БД на момент генерации данного отчёта.

Выполнение описанных выше этапов аналитической стадии и стадии экспертного эксперимента предоставляет эксперту набор признаков, позволяющих в зависимости от решаемой задачи перейти либо к стадии сравнительного исследования, либо к стадии оценки результатов исследования.

Стадия сравнительного исследования проводится при решении таких задач, как установление первоначального содержания БД, факта и времени модификации, общего источника происхождения БД, соответствия свойств и содержания данных, представленных на различных носителях информации.

Все существенные признаки, обнаруженные в ходе исследования, необходимо зафиксировать в человеко-читаемом виде на бумажном носителе и предоставить в качестве приложений к заключению эксперта. При распечатке

информации из баз данных в виде деловых документов, желательно использовать средства, встроенные в прикладные программы по обработки БД. Этим достигается перенос на бумажный носитель не только смысловой части данных, но и максимально возможно воспроизводится форма генерируемого программой документа, со всеми присущими ей особенностями.

Часто меняющиеся объекты и средства компьютерных технологий, отсутствие апробированных и сертифицированных методик и средств экспертного исследования вызывает необходимость тщательной фиксации средств, методов и полученных результатов в исследовательской части заключения эксперта. Описанные средства и методы будут являться основанием достоверности и надёжности сделанных выводов.

Типичные следственные ситуации:

• преступление произошло в условиях очевидности — характер и его обстоятельства известны и выявлены потерпевшим собственными силами, преступник известен и задержан;

• известен способ совершения, но механизм преступления в полном объеме неясен, преступник известен, но скрылся;

• налицо только преступный результат, механизм преступления и преступник неизвестны.

В первом случае необходимо установить, имелась ли причинно-следственная связь между несанкционированным проникновением в компьютерную систему и наступившими последствиями, определить размеры ущерба.

Во втором — первоочередная задача, наряду с указанными выше, — розыск и задержание преступника.

В третьей ситуации — установить механизм преступления.

На первоначальном этапе расследования проводятся следующие следственные действия: осмотр места происшествия, обыск, выемка, контроль и запись телефонных и других переговоров, допросы подозреваемых (обвиняемых), свидетелей и потерпевших.

На необходимость изъятия компьютерной информации, помимо признаков состава преступления в сфере движения компьютерной информации, могут указывать:

• наличие у подозреваемого (обвиняемого) или потерпевшего специального образования в области вычислительной техники и информатики, а также компьютерной техники в личном пользовании;

• присутствие в материалах дела документов, изготовленных машинным способом;

• хищение носителей компьютерной информации.

На подготовительном этапе осмотра или обыска необходимо получить достоверные данные о виде и конфигурации используемой ЭВМ. Часто решающее значение имеет внезапность обыска (неотложность осмотра), поскольку компьютерную информацию можно быстро уничтожить. Любые обнаруженные носители информации должны быть изъяты и изучены.

Тактика поиска компьютерной информации на рабочем этапе следственного действия избирается исходя из, во-первых, степени защищенности данных, во-вторых — функционального состояния компьютера и периферийных устройств на момент производства следственного действия.

Деятельность следователя по преодолению защиты компьютера от несанкционированного доступа — одна из самых ответственных.

На дальнейшем этапе расследования может проводиться два вида компьютерно-технических экспертиз:

• техническая экспертиза компьютеров и их комплектующих в целях изучения конструктивных особенностей и состояния компьютера, его периферийных устройств, магнитных носителей, компьютерных сетей, а также причин возникновения сбоев в работе;

• экспертиза данных и программного обеспечения, осуществляемая в целях изучения информации, хранящейся в компьютере и на магнитных носителях.

Объекты компьютерно-технической экспертизы:

• компьютеры в сборке, их системные блоки;

• периферийные устройства, коммуникационные устройства компьютеров и вычислительных сетей;

• магнитные носители информации; распечатки программных и текстовых файлов;

• словари поисковых признаков систем (тезаурусы), классификаторы и иная техническая документация, например технические задания и отчеты;

• электронные записные книжки, пейджеры, иные электронные носители текстовой или цифровой информации, техническая документация к ним.

По делам данной категории могут назначаться и другие экспертизы:

• трасологические — для анализа следов взлома;

• дактилоскопические — следов рук, как на внешних, так и на внутренних поверхностях компьютеров и их комплектующих;

• судебно-экономические экспертизы (финансово-экономические и бухгалтерские) назначаются в случаях, когда, преступления в сфере движения компьютерной информации связаны с преступлениями в кредитно- финансовой сфере;

• технико-криминалистические экспертизы документов, когда компьютер используется как средство для изготовления поддельных документов, фальшивых денежных билетов;

• фоноскопические экспертизы — при использовании средств прослушивания переговоров.

ТЕМА ЛЕКЦИИ: МЕТОДИЧЕСКИЕ ОСНОВЫ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

ПЛАН

1) Состав, структура и особенности криминалистической характеристики преступлений в сфере компьютерной информации.
2) Механизм следообразования при совершении преступлений в сфере компьютерной информации.
3) Характеристика личности преступников в сфере компьютерной информации.
4) Способы совершения преступлений в сфере компьютерной информации.
5) Основные ситуации первоначального этапа расследования преступлений в сфере компьютерной информации.

Формы и методы обучения: просмотр видеороликов и обсуждение в группе

При внедрении высоких технологий практически во все сферы жизни и хозяйственной деятельности неправомерный доступ к охраняемой законом компьютерной информации перестал быть самоцелью правонарушителей. Компьютерные технологии все чаще становятся не только орудием, но и способом и средством совершения так называемых традиционных преступлений: хищений путем растраты и присвоения, мошенничества, причинения имущественного ущерба путем обмана или злоупотребления доверием, изготовления фальшивых денег и документов, поддельных пластиковых платежных карт, нарушений авторских прав на программы для ЭВМ и базы данных и многих других.

В результате распространения глобальных сетей компьютерные преступления стали транснациональными. Интернет широко используется при совершении хищений чужого имущества, изготовлении и распространении порнографии, ложных сообщений об актах терроризма, вымогательства под угрозой блокирования или уничтожения баз данных, принадлежащих крупным корпорациям и общественным организациям, при распространении компрометирующих материалов в отношении физических и юридических лиц и т.д.

Предметом преступного посягательства является компьютерная информация, г.е. документированные сведения о лицах, предметах, фактах, событиях, явлениях и процессах, хранящиеся на машинных носителях, в ЭВМ, системе или сети ЭВМ либо управляющие ЭВМ.

ЭВМ - это комплекс электронных устройств, позволяющий осуществлять предписанные программой (или пользователем) информационные процессы: сбор, обработку, накопление, хранение, поиск и распространение информации. Систему ЭВМ можно определить как комплекс, в котором хотя бы одна ЭВМ является элементом системы либо несколько ЭВМ составляют систему. Целью системы является повышение эффективности работы ЭВМ. Сеть ЭВМ представляет собой компьютеры, объединенные между собой линиями (сетями) электросвязи, т.е. технологическими системами, обеспечивающими один или несколько видов передач (телефонную, телеграфную, факсимильную, передачу данных и других видов документальных сообщений, включая обмен информацией между ЭВМ, телевизионное, звуковое и иные виды радио- и проводного вещания). К машинным носителям компьютерной информации относятся устройства памяти ЭВМ, периферийные устройства связи, сетевые устройства и сети электросвязи.

На материальных носителях информация находится непосредственно в файлах, которые имеют стандартные свойства: тип информации (текст, графика, программный код, числа и пр.), местонахождение информации на физическом носителе, имя, объем информации, время создания и изменения, атрибуты информации (архивная, скрытая, только для чтения и пр.). При передаче файлов и сообщений (информации) в других формах (в виде сигналов) по системам, например, электросвязи, они не теряют своих индивидуальных свойств. Именно поэтому в числе носителей сведений, составляющих государственную тайну, указаны и физические поля, в которых сведения находят свое отображение в виде символов, образов, сигналов, технических решений и процессов.

Компьютерная информация может быть массовой, если она предназначена для неограниченного круга лиц, или конфиденциальной, если принадлежит

определенному собственнику или ее распространение и доступ к ней ограничены специальной нормой права, например персональные данные о субъектах, государственная, коммерческая, врачебная тайна и т.п. Доступ к такой информации ограничен и требует специального допуска. Если последний отсутствует, доступ к такой информации является неправомерным.

Состав преступления образует не всякий неправомерный доступ, а лишь такой, при котором наступили вредные последствия для обладателя информации, затруднившие или сделавшие невозможным для потерпевшего использование компьютерной информации. К таковым относятся: уничтожение, блокирование, модификация или копирование информации.

Способ совершения преступления включает подготовку, непосредственное совершение преступления и его сокрытие. Непосредственное совершение — это, например:

1) неправомерный доступ к компьютерной информации, направленный на нарушение конфиденциальности информации, — получение возможности знакомиться и осуществлять операции с чужой информацией, находящейся в ЭВМ, системах ЭВМ и их сетях, а также на магнитных носителях;

2) создание, использование и распространение вредоносных программ, приводящих к нарушению целостности или конфиденциальности информации;

3) нарушение порядка использования технических средств, повлекшее нарушение целостности и конфиденциальности информации.

Преступления, в частности, совершаются путем:

— модификации компьютерных программ с целью проводки подложных электронных документов для создания резерва денежных средств с их последующим перечислением на счета юридических и физических лиц, обналичиванием и изъятием;

- изменения программ по начислению заработной платы и зачисления ее на лицевые счета сотрудников с автоматическим списанием части наличных сумм на свой счет и на счета соучастников;

— произведения незаконных начислений денежных выплат с последующим их хищением путем подделки подписи получателей в оформленных платежных документах;

— создания файлов с вымышленными вкладчиками, зачисления и проводки по их счетам фиктивных денежных сумм с последующим переводом на свой счет и их хищением;

— получения в базах данных кредитно-финансовых учреждений номеров банковских карт и ПИН-кодов с последующим использованием в расчетах денежных средств клиентов банка;

— искажения реквизитов электронных платежных документов, касающихся адресата получателя денег, с переводом их на свой счет или счета соучастников;

— занижения суммы выручки торговых предприятий путем установки специальных вредоносных программ на контрольно-кассовые аппараты, являющиеся ЭВМ, для совершения налоговых преступлений и хищений;

— внесения ложных сведений в электронные базы данных, управляющие учетом, для завышения расхода топлива, сырья, материалов и сокрытия недостачи, образовавшейся в результате хищения, и др.

Основными средствами неправомерного доступа и преодоления информационной защиты являются: хищение ключей и паролей, использование несовершенства защиты информации, использование визуальных, оптических и

акустических средств наблюдения за ЭВМ, использование недостатков программного обеспечения, операционных систем, несанкционированное подключение к основной и вспомогательной аппаратуре ЭВМ, внешним запоминающим устройствам, периферийным устройствам, линиям связи и пр.

Способ совершения таких преступлений заключается в постановке задачи, определении цели программы, выборе средств и языка реализации программы, написании текста программы, ее отладке и запуске, а также ее использовании, т.е. в создании вредоносной программы. Вредоносной является любая программа, специально разработанная или модифицированная для несанкционированного собственником информационной системы уничтожения, блокирования, модификации либо копирования информации, нарушения обычной работы ЭВМ.

Программы могут создаваться непосредственно на ЭВМ в подвергшейся воздействию компьютерной системе, а также в любом другом месте, где субъект имеет доступ к персональному компьютеру и обладает необходимыми для разработки программы оборудованием, временем и средствами. Наказуемо и применение разработанной, в том числе иным лицом, вредоносной программы при эксплуатации ЭВМ и обработке информации.

Способом совершения преступления является и распространение вредоносных программ, которое выражается в предоставлении доступа к воспроизведенной в любой материальной форме программе для ЭВМ или базе данных. Оно может осуществляться путем перезаписи на магнитные носители и продажи с рук или через торговые предприятия, сдачи в прокат, взаймы, путем обмена, дарения и т.п. Распространение может осуществляться и сетевыми способами. Все эти действия могут выполняться одним лицом или несколькими, действующими как в группе по предварительному сговору, так и индивидуально.

Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети совершается путем выполнения действий или бездействия, нарушающих порядок их использования, установленный инструкциями по эксплуатации компьютерного оборудования. Выделяются активный и пассивный способ совершения этого преступления. Правила эксплуатации устанавливаются разработчиками оборудования, а также собственником и владельцем информационных ресурсов. Их нарушение в равной мере недопустимо, если это повлекло вредные последствия в виде уничтожения, блокирования или модификации компьютерной информации. Ответственность за такую деятельность предусматривается только для лиц, имеющих официальный доступ к ЭВМ, их системе или сети.

Для всех преступлений в сфере компьютерной информации характерно, что место и время совершения противоправных действий нс совпадает с местом и временем неправомерного доступа к информации и наступления вредных последствий. Это означает, что действия, совершаемые в одной местности, могут повлечь доступ к информации в нескольких других местах, значительно удаленных, а вредные последствия могут наступить в третьем. Наиболее ярким примером этого могут являться хищения путем нсзаконного электронного перевода денежных средств со счетов граждан путем использования номеров их банковских счетов с обналичиванием денег через подставных лиц в иной местности.

Субъекты преступлений в сфере компьютерной информации весьма специфичны. Способ совершения посягательства, как правило, отражает

особенности и мотивы преступников. Следственная практика показывает: чем сложнее в техническом отношении способ проникновения в компьютерную систему или сеть, тем легче выделить подозреваемого, поскольку круг специалистов, обладающих соответствующими способностями, обычно весьма ограничен. Зачастую преступники имеют высшее или среднее специальное техническое образование, занимают административные и бухгалтерские должности либо относятся к инженерно-техническому персоналу, многие по роду службы правомерно пользуются служебной компьютерной техникой и постоянно имеют свободный доступ к ней. Наряду с этим распространены случаи совершения таких преступлений несовершеннолетними, а также группами, в том числе организованными (каждое третье преступление совершено организованной преступной группой с распределением ролей и соответствующей подготовкой). Уже регистрируются случаи использования «компьютерных взломщиков» организованными группами, совершающими тяжкие преступления, в том числе финансовые, а также террористическими организациями.

По делам о преступлениях в сфере компьютерной информации установлению подлежат следующие обстоятельства:

— факт неправомерного доступа к компьютерной информации;

— физические или юридические лица, потерпевшие от преступления;

— место совершения преступления;

— время совершения преступления, а также время наступления вредных последствий;

— орудия преступления, т.е. компьютерные и телекоммуникационные средства, а также программное обеспечение, которые использовались преступником;

— способ совершения преступления;

— вредные последствия преступления, их оценка обладателем компьютерной информации, характер и размер вреда, возможно — наступление тяжких последствий;

— субъект преступления, наличие у него доступа к ЭВМ, системе ЭВМ или их сети, наличие преступной группы, распределение ролей между ее участниками;

— виновность каждого субъекта преступления, форма вины, мотив преступной деятельности;

— обстоятельства, характеризующие личность каждого субъекта;

— обстоятельства, исключающие преступность и наказуемость деяния;

— обстоятельства, смягчающие и отягчающие наказание;

— обстоятельства, которые могут повлечь за собой освобождение от уголовной ответственности и наказания;

— причины и условия, способствовавшие совершению преступления.

ТЕМА ЛЕКЦИИ: **ПОЛУЧЕНИЕ И ПРОВЕРКА ВЕРБАЛЬНОЙ ИНФОРМАЦИИ,СВЯЗАННОЙ С КОМПЬЮТЕРНЫМИ ОБЪЕКТАМИ**

ПЛАН

1) Допрос.
2) Следственный эксперимент.
3) Основные возможности компьютерно-технических экспертиз и тактические рекомендации по их назначению.

Формы и методы обучения: просмотр видеороликов и обсуждение в группе

При расследовании преступлений в сфере компьютерной информации допросы свидетелей осуществляются с использованием тактических рекомендаций, разработанных в криминалистике. Особое значение здесь приобретает подготовка к допросу и всестороннее изучение личности допрашиваемого. При этом следует учесть, что свидетелями по данной категории дел чаще всего выступают лица с высшим образованием, обладающие высоким интеллектом, в совершенстве владеющие специальной терминологией, зачастую не вполне понятной следователю, в связи с этим следователю необходимо детализировать показания допрашиваемого постановкой уточняющих вопросов, раскрывающих содержание тех или иных терминов и определений, употребляемых допрашиваемым. Для участия в допросе может быть приглашен специалист в области вычислительной техники (необходимо, как минимум, предварительное согласование с ним формулировок задаваемых вопросов).

Основными тактическими задачами допроса потерпевших и свидетелей при расследовании дел рассматриваемой категории являются: выявление элементов состава преступления в наблюдавшихся ими действиях, установление обстоятельств, места и времени совершения значимых для расследования действий, способа и мотивов его совершения и сопутствующих обстоятельств, признаков внешности лиц, участвовавших в нем, определение предмета преступного посягательства, размера причиненного ущерба, детальные признаки похищенного, установление свидетелей и лиц, причастных к совершению преступления.

Для решения указанных задач в процессе допроса свидетеля необходимо выяснить:

1. Не проявлял ли кто-либо интереса к компьютерной информации, программному обеспечению, компьютерной технике данного предприятия, организации, учреждения, фирмы или компании?

2. Не появлялись ли в помещении, где расположена компьютерная техника, посторонние лица, не зафиксированы ли случаи работы сотрудников с информацией, не относящейся к их компетенции?

3. Не было ли сбоев в работе программ, хищений носителей информации и отдельных компьютерных устройств?

4. Зафиксированы ли сбои в работе компьютерного оборудования, электронных сетей, средств защиты компьютерной информации?

5. Как часто проверяются программы на наличие вирусов, каковы результаты последних проверок?

6. Как часто обновляется программное обеспечение, каким путем, где и кем оно приобретается?

7. Каким путем, где и кем приобретается компьютерная техника, как осуществляется ее ремонт и модернизация?

8. Каков на данном объекте порядок работы с информацией, как она поступает, обрабатывается и передается по каналам связи?

9. Кто еще является абонентом компьютерной сети, к которой подключены компьютеры данного предприятия, организации, учреждения или фирмы, каким образом осуществляется доступ в сеть, кто из пользователей имеет право на работу в сети, каковы их полномочия?

10. Как осуществляется защита компьютерной информации, применяемые средства и методы защиты и др.?

11. Могли ли возникшие последствия стать результатом неосторожного действия лица или неисправности работы ЭВМ, системы ЭВМ, сбоев программного обеспечения и т.п.?

12. Каков характер изменений информации?

13. Кто является собственником (владельцем или законным пользователем) скопированной (уничтоженной, модифицированной, блокированной) информации и др.?

При расследовании неправомерного доступа к компьютерной информации на первоначальном этапе возникает необходимость допрашивать в качестве свидетелей граждан различных категорий, для каждой из которых существует свой предмет допроса.

В зависимости от занимаемой должности свидетелей, потерпевших их допрос может иметь некоторые особенности.

В процессе допросов операторов ЭВМ следует выяснить правила ведения журналов операторов, порядок приема-сдачи смен, режим работы операторов, порядок идентификации операторов; правила эксплуатации, хранения, уничтожения компьютерных распечаток (листингов), категорию лиц, имеющих к ним доступ; порядок доступа в помещение, где находится компьютерная техника, категорию работников, допущенных к работе с ней, и др.

В процессе допроса программистов выясняется: перечень используемого программного обеспечения и его классификации (лицензионное, собственное), пароли защиты программ, отдельных устройств компьютера, частота их смен; технические характеристики компьютерной сети (при ее наличии), кто является администратором сети; порядок приобретения и сопровождения программного обеспечения; наличие в рабочих программах специальных файлов-протоколов, регистрирующих вхождение компьютеров пользователей, каково их содержание и др.

У сотрудника, отвечающего за информационную безопасность, или администратора компьютерной сети выясняется: наличие специальных технических средств защиты информации; порядок доступа пользователей в компьютерную сеть; порядок идентификации пользователей компьютеров, распорядок рабочего дня пользователей компьютерной сети; порядок доступа сотрудников к компьютерной технике во внерабочее время, порядок присвоения и смены паролей пользователей; характеристика мер по защите информации.

У сотрудников, занимающихся техническим обслуживанием вычислительной техники, выясняется: перечень и технические характеристики средств компьютерной техники, установленных в организации, а также перечень

защитных технических средств, периодичность технического обслуживания, проведения профилактических и ремонтных работ; сведения о произошедших в последнее время случаях выхода аппаратуры из строя; случаи незаконного подключения к телефонным линиям связи, установка какого-либо дополнительного электрооборудования.

У начальника вычислительного центра или руководителей предприятия (организации) следует выяснить: действуют ли в учреждении специальные службы по эксплуатации сетей и службы безопасности, их состав и обязанности; сертифицированы ли программы системной защиты; организационную структуру вычислительного центра; сертифицированы ли технические устройства вычислительной техники; действуют ли внутриведомственные правила эксплуатации ЭВМ и сети, каков порядок ознакомления с ними и контроля за их исполнением; какие сотрудники учреждения (организации) были уволены в течение интересующего периода времени и по каким мотивам; были ли ранее случаи незаконного проникновения в помещение, где установлена компьютерная техника; были ли случаи несанкционированного доступа к компьютерной информации, вирусных атак и др.

У руководителя организации, работника юридического отдела или иного лица, уполномоченного представлять интересы потерпевшего юридического лица (в ходе допроса в качестве представителя потерпевшего), выясняется: стаж работы в должности; основания для представления интересов организации в правоохранительных органах (доверенность, подписанная руководителем организации, которая приобщается к уголовному делу); откуда стало известно о произошедшем; излагаются обстоятельства, ставшие известными представителю потерпевшего; выясняются лица, могущие разъяснить следователю технические вопросы, возникающие при расследовании уголовного дела; правовая регламентация статуса информации, подвергшейся воздействию в результате преступления.

Свидетелями при расследовании неправомерного доступа к компьютерной информации могут быть лица, наблюдавшие событие преступления (особенно при непосредственном доступе) или его отдельные моменты, а также видевшие преступников непосредственно в момент совершения преступления или после него.

При этом должно быть выяснено:

1. При каких обстоятельствах свидетель наблюдал преступников (процесс совершения преступления)?
2. В чем состоял способ совершения преступления?
3. Какую роль выполнял каждый из соучастников неправомерного доступа к компьютерной информации?
4. Знает ли свидетель, какую цель преследовал обвиняемый, совершая неправомерный доступ к компьютерной информации?
5. Имели ли место подобные проявления ранее, если да, то как на них реагировали руководители предприятия, организации, учреждения, фирмы, компании?
6. Как свидетель характеризует обвиняемого и его окружение?
7. Что способствовало совершению преступления?

ТЕМА ЛЕКЦИИ: УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

ПЛАН

1) Характеристика компьютерной информации.
2) Уголовно-правовая характеристика преступлений в сфере компьютерной информации.

Форма и методы обучения: обзорная форма лекции, слайдовые презентации

Составы компьютерных преступлений (т.е. перечень признаков, характеризующих общественно опасное деяние как конкретное преступление) приведены в 7 главе УК РК, которая называется **«Уголовные правонарушения в сфере информатизации и связи»** и содержит следующие статьи:

Статья 205. Неправомерный доступ к информации, в информационную систему или сеть телекоммуникаций

1. Умышленный неправомерный доступ к охраняемой законом информации, содержащейся на электронном носителе, в информационную систему или сеть телекоммуникаций, повлекший существенное нарушение прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства, –

наказывается штрафом в размере до ста шестидесяти месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до ста шестидесяти часов, либо арестом на срок до сорока суток, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до двух лет или без такового.

2. То же деяние, совершенное в отношении критически важных объектов информационно-коммуникационной инфраструктуры, –

наказывается штрафом в размере до двухсот месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до двухсот часов, либо арестом на срок до пятидесяти суток, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до двух лет или без такового.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, повлекшие по неосторожности тяжкие последствия, -

наказываются штрафом в размере до двух тысяч месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до шестисот часов, либо ограничением свободы на срок до двух лет, либо лишением свободы на тот же срок, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

Сноска. Статья 205 с изменениями, внесенными законами РК от 28.12.2017 № 128-VI (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования); от 12.07.2018 № 180-VI (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

Статья 206. Неправомерные уничтожение или модификация информации

1. Умышленные неправомерные уничтожение или модификация охраняемой законом информации, хранящейся на электронном носителе, содержащейся в информационной системе или передаваемой по сетям телекоммуникаций, а равно ввод в информационную систему заведомо ложной информации, если это повлекло существенное нарушение прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства, –

наказываются штрафом в размере до двухсот месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до двухсот часов, либо арестом на срок до пятидесяти суток, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до двух лет или без такового.

2. Те же деяния, совершенные:

1) в отношении критически важных объектов информационно-коммуникационной инфраструктуры;

2) группой лиц по предварительному сговору, –

наказываются штрафом в размере до двух тысяч месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до шестисот часов, либо ограничением свободы на срок до двух лет, либо лишением свободы на тот же срок, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

3. Деяния, предусмотренные частями первой или второй настоящей статьи:

1) совершенные преступной группой;

2) повлекшие тяжкие последствия, –

наказываются лишением свободы на срок от трех до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

Сноска. Статья 206 с изменениями, внесенными законами РК от 28.12.2017 № 128-VI (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования); от 12.07.2018 № 180-VI (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

Статья 207. Нарушение работы информационной системы или сетей телекоммуникаций

1. Умышленные действия (бездействие), направленные на нарушение работы информационной системы или сетей телекоммуникаций, –

наказываются штрафом в размере до двух тысяч месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до шестисот часов, либо ограничением свободы на срок до двух лет, либо лишением свободы на тот же срок, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до двух лет или без такового.

2. Те же деяния, совершенные:

1) в отношении критически важных объектов информационно-коммуникационной инфраструктуры;

2) группой лиц по предварительному сговору, –

наказываются штрафом в размере до четырех тысяч месячных расчетных показателей либо исправительными работами в том же размере, либо

привлечением к общественным работам на срок до одной тысячи часов, либо ограничением свободы на срок до четырех лет, либо лишением свободы на тот же срок, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

3. Деяния, предусмотренные частями первой или второй настоящей статьи:

1) совершенные преступной группой;

2) повлекшие тяжкие последствия, –

наказываются лишением свободы на срок от пяти до десяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет или без такового.

Сноска. Статья 207 с изменениями, внесенными законами РК от 28.12.2017 № 128-VI (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования); от 12.07.2018 № 180-VI (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

Статья 208. Неправомерное завладение информацией

1. Умышленное неправомерное копирование или иное неправомерное завладение охраняемой законом информацией, хранящейся на электронном носителе, содержащейся в информационной системе или передаваемой по сетям телекоммуникаций, если это повлекло существенное нарушение прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства, –

наказывается штрафом в размере до двухсот месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до ста восьмидесяти часов, либо арестом на срок до пятидесяти суток, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до двух лет или без такового.

2. То же деяние, совершенное:

1) в отношении критически важных объектов информационно-коммуникационной инфраструктуры;

2) группой лиц по предварительному сговору, –

наказывается штрафом в размере до двух тысяч месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до шестисот часов, либо ограничением свободы на срок до двух лет, либо лишением свободы на тот же срок, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

3. Деяния, предусмотренные частями первой или второй настоящей статьи:

1) совершенные преступной группой;

2) повлекшие тяжкие последствия, –

наказываются лишением свободы на срок от трех до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

Сноска. Статья 208 с изменениями, внесенными законами РК от 28.12.2017 № 128-VI (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования); от 12.07.2018 № 180-VI (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

Статья 209. Принуждение к передаче информации

1. Принуждение к передаче охраняемой законом информации, хранящейся на электронном носителе, содержащейся в информационной системе или передаваемой по сетям телекоммуникаций, под угрозой применения насилия либо уничтожения или повреждения имущества, а равно под угрозой распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, оглашение которых может причинить существенный вред интересам потерпевшего или его близких, –

наказывается штрафом в размере до двух тысяч месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до шестисот часов, либо ограничением свободы на срок до двух лет, либо лишением свободы на тот же срок, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до двух лет или без такового.

2. То же деяние:

1) сопряженное с применением физического насилия над лицом или его близкими;

2) совершенное группой лиц по предварительному сговору;

3) совершенное с целью получения информации из критически важных объектов информационно-коммуникационной инфраструктуры, –

наказывается лишением свободы на срок от трех до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

3. Деяния, предусмотренные частями первой или второй настоящей статьи:

1) совершенные преступной группой;

2) повлекшие тяжкие последствия, –

наказываются лишением свободы на срок от пяти до десяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет или без такового.

Сноска. Статья 209 с изменениями, внесенными законами РК от 28.12.2017 № 128-VI (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования); от 12.07.2018 № 180-VI (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

Статья 210. Создание, использование или распространение вредоносных компьютерных программ и программных продуктов

1. Создание компьютерной программы, программного продукта или внесение изменений в существующую программу или программный продукт с целью неправомерного уничтожения, блокирования, модификации, копирования, использования информации, хранящейся на электронном носителе, содержащейся в информационной системе или передаваемой по сетям телекоммуникаций, нарушения работы компьютера, абонентского устройства, компьютерной программы, информационной системы или сетей телекоммуникаций, а равно умышленные использование и (или) распространение такой программы или программного продукта –

наказываются штрафом в размере до трех тысяч месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до восьмисот часов, либо ограничением свободы на срок до трех лет, либо лишением свободы на тот же срок, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

2. Те же деяния, совершенные:

1) группой лиц по предварительному сговору;

2) лицом с использованием своего служебного положения;

3) в отношении критически важных объектов информационно-коммуникационной инфраструктуры, -

наказываются ограничением свободы на срок от трех до семи лет либо лишением свободы на тот же срок, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

3. Деяния, предусмотренные частями первой или второй настоящей статьи:

1) совершенные преступной группой;

2) повлекшие тяжкие последствия, –

наказываются лишением свободы на срок от пяти до десяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет или без такового.

Сноска. Статья 210 с изменениями, внесенными законами РК от 28.12.2017 № 128-VI (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования); от 12.07.2018 № 180-VI (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

Статья 211. Неправомерное распространение электронных информационных ресурсов ограниченного доступа

1. Неправомерное распространение электронных информационных ресурсов, содержащих персональные данные граждан или иные сведения, доступ к которым ограничен законами Республики Казахстан или их собственником или владельцем, –

наказывается штрафом в размере до двухсот месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до ста восьмидесяти часов, либо арестом на срок до пятидесяти суток, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

2. То же деяние, совершенное:

1) группой лиц по предварительному сговору;

2) из корыстных побуждений;

3) лицом с использованием своего служебного положения, –

наказывается привлечением к общественным работам на срок до одной тысячи двухсот часов либо ограничением свободы на срок до пяти лет, либо лишением свободы на тот же срок, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

3. Деяния, предусмотренные частями первой или второй настоящей статьи:

1) совершенные преступной группой;

2) повлекшие тяжкие последствия, –

наказываются лишением свободы на срок от трех до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет или без такового.

Сноска. Статья 211 с изменениями, внесенными Законом РК от 12.07.2018 № 180-VI (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

Статья 212. Предоставление услуг для размещения интернет-ресурсов, преследующих противоправные цели

1. Заведомо противоправное оказание услуг по предоставлению аппаратно-программных комплексов, функционирующих в открытой информационно-коммуникационной сети, для размещения интернет-ресурсов, преследующих противоправные цели, –

наказывается штрафом в размере до двух тысяч месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до шестисот часов, либо ограничением свободы на срок до двух лет, либо лишением свободы на тот же срок, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до двух лет.

2. То же деяние, совершенное группой лиц по предварительному сговору или преступной группой, –

наказывается лишением свободы на срок от трех до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

Сноска. Статья 212 с изменениями, внесенными Законом РК от 12.07.2018 № 180-VI (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

Статья 213. Неправомерные изменение идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента, а также создание, использование, распространение программ для изменения идентификационного кода абонентского устройства

1. Изменение идентификационного кода абонентского устройства сотовой связи, создание дубликата карты идентификации абонента сотовой связи, если эти действия совершены без согласия производителя или законного владельца, –

наказываются штрафом в размере до ста шестидесяти месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до ста шестидесяти часов, либо арестом на срок до сорока суток.

2. Неправомерные создание, использование, распространение программ, позволяющих изменять идентификационный код абонентского устройства сотовой связи или создавать дубликат карты идентификации абонента сотовой связи, –

наказываются штрафом в размере до двух тысяч месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до шестисот часов, либо ограничением свободы на срок до двух лет, либо лишением свободы на тот же срок.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные преступной группой, –

наказываются лишением свободы на срок до пяти лет.

Сноска. Статья 213 с изменениями, внесенными Законом РК от 12.07.2018 № 180-VI.

Эти деяния направлены против той части установленного порядка общественных отношений, который регулирует изготовление, использование, распространение и защиту компьютерной информации.

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.

Видовым объектом данных преступлений является совокупность общественных отношений по обеспечению информационной безопасности.

Непосредственными объектами преступного посягательства являются,

- базы и банки данных,
- отдельные файлы конкретных компьютерных систем и сетей,
- компьютерные технологии и программные средства, включая те, которые обеспечивают защиту компьютерной информации от неправомерного доступа.

Под ***информацией*** понимаются сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Документированная информация это зафиксированные на материальном носителе сведения с реквизитами, которые позволяют их идентифицировать.

Под ***компьютерной информацией*** понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

Компьютерная информация считается документированной, но хранящейся в ЭВМ или управляющей ею в соответствии с программой и (или) предписаниями пользователя.

К машинным носителям компьютерной информации относятся:

- блоки памяти ЭВМ,
- ее периферийные системы,
- компьютерные средства связи,
- сетевые устройства,
- сети электросвязи.

Ответственность наступает в случае, если неправомерный доступ к компьютерной информации привел к таким опасным последствиям, как уничтожение, блокирование, модификация либо копирование компьютерной информации.

Уничтожением считается такое изменение информации, которое лишает ее первоначального качества, вследствие чего она перестает отвечать своему прямому назначению.

Под ***блокированием*** понимается временная или постоянная невозможность доступа к информации со стороны законного пользователя, а под ***модификацией*** ее видоизменение с появлением новых, нежелательных свойств.

Копирование это воспроизведение точного или относительно точного аналога оригинала.

К ***вредоносным*** программам для ЭВМ, прежде всего, относятся так называемые компьютерные вирусы, т.е. программы, могущие внедряться в чужие информационные ресурсы, размножаться и при определенных условиях повреждать компьютерные системы, хранящуюся в них информацию и программное обеспечение. Свое название они получили потому, что многие их свойства аналогичны свойствам природных вирусов. Компьютерный вирус может самовоспроизводиться во всех системах определенного типа. Некоторые из них сравнительно безопасны, поскольку не уничтожают информацию, однако большинство приносит существенный вред.

Имеются также иные вредоносные программы, облегчающие доступ к информационным ресурсам, используемые обычно для хищений денежных средств в компьютерных банковских системах и совершения других злоупотреблений в сфере компьютерной информации.

Непосредственный объект данного преступления это общественные отношения по безопасному использованию ЭВМ, ее программного обеспечения и информационного содержания. Этим преступлениям свойственна высокая латентность; особенно трудно выявлять создателей вредоносных программ.

ТЕМА ЛЕКЦИИ: КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

ПЛАН

1) Формирование модели преступления в сфере компьютерной информации.
2) Исследование модели: построение типовых версий.

Форма и методы обучения: решение кейс-задач

Особенностями первоначального этапа расследования преступлений в области компьютерной информации являются:

а) широкое использование при проведении следственных и оперативно-розыскных действий лиц, сведущих в области применения информационных технологий;

б) особый алгоритм расследования;

в) специфические приемы работы (осмотры, изъятие, хранение и т.п.) с машинными носителями в ходе производства следственных действий;

г) особенности тактики отдельных следственных действий.

д) особенности взаимодействия с оперативными подразделениями.

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, совершенные с использованием компьютерных технологий, представляют серьезную угрозу для любой располагающей компьютерной техникой организации. Таким образом. необходимо подробное изучения особенностей их раскрытия и расследования.

1. Типичные следственные ситуации и версии предварительного этапа расследования преступлений в сфере компьютерной информации

Для рассматриваемых преступлений характерны такие ситуации начала расследования:

1. Собственник компьютерной системы обнаружил нарушение ее целостности и (или) конфиденциальности, установил виновное лицо и заявил о случившемся в правоохранительные органы.

2. Собственник самостоятельно выявил названные нарушения, однако не смог установить злоумышленника и заявил о случившемся.

3. Сведения о нарушении целостности и (или) конфиденциальности информации и виновном субъекте стали известны или непосредственно обнаружены компетентным органом, владелец компьютерной системы этот факт скрывает.

4. Правоохранительным органом обнаружены признаки противоправного вторжения в компьютерную систему, виновное лицо и владелец информации неизвестны.

Общие версии, которые выдвигаются на первоначальном этапе расследования следующие: преступление действительно имело место при тех обстоятельствах, которые вытекают из первичных материалов; ложное заявление о преступлении либо имела место инсценировка преступления.

Частные версии выдвигаются в отношении личности преступника, мотивов и способов совершения преступления, размера причиненного ущерба и т.д.

Например, версия по поводу личности преступника может звучать следующим образом: неправомерный доступ совершен сотрудником потерпевшей организации или лицом, не имеющим отношений с потерпевшей организацией. В первом случае выдвигается версия об инсайдере (внутренний неправомерный доступ), вторая - неправомерный доступ совершен хакером (неправомерный доступ снаружи). Однако надо иметь в виду, что если признаки преступления указывают на то, что НДКИ был совершен хакером (снаружи), то скорее всего он стал возможным в результате сговора с сотрудником потерпевшей организации, поскольку для хакера обнаружить уязвимости в информационной системе - это сложная задача с учетом новейших программных средств, а вот сотрудник потерпевшей организации знаком со всеми ее проблемами.

2. Обстоятельства, подлежащие установлению и доказыванию по делам о преступления в сфере компьютерной информации

При расследовании неправомерного доступа к компьютерной информации обстоятельства содеянного устанавливаются в такой очередности:

1) факт неправомерного доступа к информации в компьютерной системе или сети;

2) место несанкционированного проникновения в эту систему или сеть;

3) время совершения преступления;

4) способ несанкционированного доступа;

5) степень надежности средств защиты компьютерной информации;

6) лица, совершившие неправомерный доступ, их виновность и мотивы преступления;

7) вредные последствия содеянного.

Факт неправомерного доступа к информации обнаруживают, как правило, пользователи компьютерной системы или сети. Такие факты иногда устанавливаются в ходе оперативно-розыскной деятельности органов внутренних дел. Их можно выявить и в ходе прокурорских проверок, ревизий, судебных экспертиз, следственных действий по расследуемым делам.

Признаками несанкционированного доступа или подготовки к нему могут служить:

а) появление в компьютере искаженных данных;

б) длительное необновление кодов, паролей и других защитных средств компьютерной системы;

в) увеличение числа сбоев в работе ЭВМ;

г) участившиеся жалобы пользователей компьютерной системы или сети.

Таким фактам могут предшествовать или сопутствовать:

1) осуществление без необходимости сверхурочных работ;

2) немотивированные отказы отдельных сотрудников, обслуживающих компьютерную систему или сеть, от очередного отпуска;

3) приобретение работником для личного пользования дорогостоящего компьютера;

4) чистые дискеты или диски, принесенные на работу кем-то из сотрудников компьютерной системы под предлогом копирования программ для компьютерных игр;

5) участившиеся случаи перезаписи отдельных данных без серьезных на то причин;

6) необоснованный интерес некоторых работников к содержанию чужих принтерных распечаток;

7) повторный ввод в компьютер одной и той же информации и др.

Необходимо выяснить также признаки неправомерного доступа, выражающиеся в отступлениях от установленного порядка обработки документов. Имеются в виду:

а) нарушения принятых правил оформления документов и изготовления машинограмм;

б) лишние документы, подготовленные для обработки на ЭВМ;

в) несоответствие информации, содержащейся в первичных документах, данным машинограмм;

г) преднамеренные утрата или уничтожение первичных документов и машинных носителей информации, внесение искажений в данные их регистрации. Следует, однако, помнить, что перечисленные признаки могут быть результатом не только злоупотреблений, но и других причин, например халатности персонала, случайных ошибок и сбоев компьютерной техники.

Место несанкционированного проникновения в компьютерную систему или сеть удается установить с определенными трудностями, поскольку таких

мест может быть несколько. На практике чаще обнаруживается место неправомерного доступа к компьютерной информации с целью хищения денежных средств, но для этого также приходится выявлять все места работы компьютеров, имеющих единую телекоммуникационную связь.

Гораздо проще это место устанавливается тогда, когда расследуется несанкционированный доступ к единичному компьютеру. Но и тут нужно учитывать, что информация на машинных носителях может храниться в других помещениях.

Во много раз труднее определить место непосредственного применения технических средств удаленного несанкционированного доступа, которые не входят в данную компьютерную систему или сеть. К его установлению необходимо привлекать соответствующих специалистов. Необходимо выяснить также место хранения информации на машинных носителях, добытой преступником в результате неправомерного доступа к компьютерной системе или сети.

Время несанкционированного доступа можно определить с помощью программ общесистемного назначения. В работающем компьютере они обычно фиксируют текущее время. Если данная программа функционирует, то при несанкционированном входе в систему или сеть время работы на компьютере любого пользователя и производства конкретной операции автоматически фиксируется в оперативной памяти. Тогда время несанкционированного доступа можно определить в ходе следственного осмотра компьютера, его распечаток или дискет, производимого с участием специалиста, чтобы информация, находящаяся в оперативной памяти ЭВМ или на дискете, не была случайно стерта. В качестве специалистов могут выступать, например, сотрудники информационных центров МВД.

Время несанкционированного доступа устанавливается и путем допроса свидетелей из числа сотрудников данной компьютерной системы. Выясняется, когда именно каждый из них работал на ЭВМ, если это не было зафиксировано в автоматическом режиме.

Способы преступных манипуляций в сфере компьютерной информации могут быть разделены на две большие группы. Первая группа осуществляется без использования компьютерных устройств в качестве инструмента для проникновения извне в информационные системы или воздействия на них. Это могут быть:

а) хищение машинных носителей информации в виде блоков и элементов ЭВМ;

б) использование визуальных, оптических и акустических средств наблюдения за ЭВМ;

в) считывание и расшифровка различных электромагнитных излучений компьютера и обеспечивающих систем;

г) фотографирование информации в процессе ее обработки;

д) изготовление бумажных дубликатов входных и выходных документов, копирование распечаток;

е) использование оптических и акустических средств наблюдения за лицами, имеющими отношение к необходимой злоумышленнику информации, фиксация их разговоров;

ж) осмотр и изучение не полностью утилизированных отходов деятельности компьютерных систем;

з) вступление в прямой контакт с лицами, имеющими отношение к необходимой злоумышленнику информации, получение от них под разными предлогами нужных сведений и др.

Для таких действий, как правило, характерна достаточно локальная следовая картина. Она определяется тем, что место совершения преступных действий и дислокация объекта преступного посягательства расположены вблизи друг от друга или совпадают. Приемы их исследования достаточно традиционны.

Вторая группа преступных действий осуществляется с использованием компьютерных и коммуникационных устройств. Тогда несанкционированный доступ реализуется с помощью различных способов: подбором пароля, использованием чужого имени, отысканием и применением пробелов в программе, а также других мер преодоления защиты компьютерной информации. Конкретный способ несанкционированного доступа можно установить путем допроса свидетелей из числа лиц, обслуживающих компьютерную систему, и ее разработчиков. При этом следует учитывать выявленную следовую картину. У них необходимо выяснить как преступник мог проникнуть в защищенную систему, например узнать идентификационный номер законного пользователя, код, пароль для доступа, получить сведения о других средствах защиты системы или сети ЭВМ.

Чрезвычайно важны и другие действия, направленные на фиксацию факта нарушения целостности (конфиденциальности) компьютерной системы и его последствий, следов преступных манипуляций виновного субъекта, отразившихся в ЭВМ и на машинных носителях информации, в линиях связи и др.

Способ несанкционированного доступа надежнее установить путем производства судебной информационно-технической экспертизы. Перед экспертом ставится вопрос: "Каким способом был осуществлен несанкционированный доступ в данную компьютерную систему?" Для этого эксперту нужно представить всю проектную документацию на взломанную компьютерную систему, а также данные о ее сертификации. При производстве такой экспертизы не обойтись без использования компьютерного оборудования той же системы, которую взломал преступник, либо специальных технических и программных средств.

В ряде случаев целесообразен следственный эксперимент для проверки возможности преодоления средств защиты компьютерной системы одним из предполагаемых способов. Одновременно может быть проверена возможность появления на экране дисплея конфиденциальной информации или ее распечатки вследствие ошибочных, неумышленных действий оператора либо случайного технического сбоя в электронном оборудовании.

Выясняя надежность средств зашиты компьютерной информации, прежде всего следует установить, предусмотрены ли в данной системе или сети ЭВМ меры защиты от несанкционированного доступа, в том числе к определенным файлам. Это возможно в ходе допросов разработчиков и пользователей системы, а также при изучении проектной документации и инструкций по эксплуатации системы. Изучая инструкции, нужно обращать особое внимание на разделы о мерах защиты информации, порядке допуска пользователей к конкретным данным, разграничении их полномочий, организации контроля за доступом. Важно разобраться в аппаратных, программных, криптографических, организационных и других методах защиты информации, поскольку для

обеспечения высокой степени надежности компьютерных систем, обрабатывающих документированную информацию с ограниченным доступом, обычно используется комплекс мер по обеспечению их безопасности от несанкционированного доступа.

Так, законодательством предусмотрена обязательная сертификация средств защиты систем и сетей ЭВМ, а кроме того обязательное лицензирование всех видов деятельности в области проектирования и производства названных средств. Поэтому в процессе расследования необходимо выяснить: 1) есть ли лицензия на производство средств защиты информации, задействованных в данной компьютерной системе, от несанкционированного доступа и 2) соответствуют ли их параметры выданному сертификату. Ответ на последний вопрос может дать информационно-техническая экспертиза, с помощью которой выясняется: соответствуют ли средства защиты информации от несанкционированного доступа, использованные в данной компьютерной системе, выданному сертификату? Правда, ответственность за выявленные отклонения, позволившие несанкционированный доступ к компьютерной информации, ложится на пользователя системы, а не на разработчика средств ее защиты.

При установлении лиц, совершивших несанкционированный доступ к конфиденциальной компьютерной информации, следует учитывать, что он является технологически весьма сложным. Осуществить его могут только специалисты, обладающие достаточно высокой квалификацией. Поэтому поиск подозреваемых рекомендуется начинать с технического персонала взломанных компьютерных систем или сетей. Это в первую очередь их разработчики, а также руководители, операторы, программисты, инженеры связи, специалисты по защите информации, другие сотрудники.

Следственная практика свидетельствует, что чем технически сложнее способ проникновения в компьютерную систему или сеть, тем легче установить подозреваемого, ибо круг специалистов, обладающих соответствующими способностями, весьма ограничен.

Доказыванию виновности конкретного субъекта в несанкционированном доступе к компьютерной информации способствует использование различных следов, обнаруживаемых при осмотре ЭВМ и ее компонентов. Это, например, следы пальцев, записи на внешней упаковке дискет и др. Для их исследования назначаются криминалистические экспертизы дактилоскопическая, почерковедческая и др.

Для установления лиц, обязанных обеспечивать надлежащий режим доступа к компьютерной системе или сети, следует прежде всего ознакомиться с должностными инструкциями, определяющими полномочия сотрудников, ответственных за защиту конфиденциальной информации. Их необходимо допросить для выяснения, кто запускал нештатную программу и фиксировалось ли это каким-либо способом. Нужно также выяснить, кто особо увлекается программированием, учится или учился на курсах программистов, интересуется системами защиты информации.

У субъектов, заподозренных в неправомерном доступе к компьютерной информации, производится обыск в целях обнаружения: ЭВМ различных конфигураций, принтеров, средств телекоммуникационной связи с компьютерными сетями, записных книжек, в том числе электронных, с уличающими записями, дискет и дисков с информацией, могущей иметь значение для дела, особенно если это коды, пароли, идентификационные номера

пользователей данной компьютерной системы, а также сведения о них. При обыске нужно изымать также литературу и методические материалы по компьютерной технике и программированию. К производству обыска и осмотру изъятых предметов рекомендуется привлекать специалиста по компьютерной технике, незаинтересованного в исходе дела.

Доказать виновность и выяснить мотивы лиц, осуществивших несанкционированный доступ к компьютерной информации, можно лишь по результатам всего расследования. Решающими здесь будут показания свидетелей, подозреваемых, обвиняемых, потерпевших, заключения судебных экспертиз, главным образом информационно-технологических и информационно-технических, а также результаты обысков. В ходе расследования выясняется:

1) с какой целью совершен несанкционированный доступ к компьютерной информации;

2) знал ли правонарушитель о системе ее защиты;

3) желал ли преодолеть эту систему и какими мотивами при этом руководствовался.

Вредные последствия неправомерного доступа к компьютерной системе или сети могут заключаться в хищении денежных средств или материальных ценностей, завладении компьютерными программами, а также информацией путем изъятия машинных носителей либо копирования. Это может быть также незаконное изменение, уничтожение, блокирование информации, выведение из строя компьютерного оборудования, внедрение в компьютерную систему вредоносного вируса, ввод заведомо ложных данных и др.

Хищения денежных средств чаще всего совершаются в банковских электронных системах путем несанкционированного доступа к их информационным ресурсам, внесения в последние изменений и дополнений. Такие посягательства обычно обнаруживают сами работники банков, устанавливаются они и в ходе оперативно-розыскных мероприятий. Сумма хищения определяется посредством судебно-бухгалтерской экспертизы.

Факты неправомерного завладения компьютерными программами вследствие несанкционированного доступа к той или иной системе и их незаконного использования выявляют, как правило, потерпевшие. Максимальный вред причиняет незаконное получение информации из различных компьютерных систем, ее копирование и размножение с целью продажи либо использования в других преступных целях (например, для сбора компрометирующих данных на кандидатов на выборные должности различных представительных и исполнительных органов государственной власти).

Похищенные программы и базы данных могут быть обнаружены в ходе обысков у обвиняемых, а также при оперативно-розыскных мероприятиях. Факты незаконного изменения, уничтожения, блокирования информации, выведения из строя компьютерного оборудования, "закачки" в информационную систему заведомо ложных сведений выявляются прежде всего самими пользователями компьютерной системы или сети. Следует учитывать, что не все эти негативные последствия наступают в результате умышленных действий. Их причиной могут стать случайные сбои в работе компьютерного оборудования, происходящие довольно часто.

При определении размера вреда, причиненного несанкционированным доступом, учитываются не только прямые затраты на ликвидацию негативных последствий, но и упущенная выгода. Такие последствия устанавливаются в

ходе следственного осмотра компьютерного оборудования и носителей информации с анализом баз и банков данных. Помогут здесь и допросы технического персонала, владельцев информационных ресурсов. Вид и размер ущерба обычно определяются посредством комплексной экспертизы, проводимой с участием специалистов в области информатизации, средств вычислительной техники и связи, экономики, финансовой деятельности и товароведения.

На заключительном этапе расследования формируется целостное представление об обстоятельствах, которые облегчили несанкционированный доступ к компьютерной информации. Здесь важно последовательное изучение различных документов, особенно относящихся к защите информации. Весьма значимы материалы ведомственного (служебного) расследования.

К этим обстоятельствам относятся:

1) неэффективность методов защиты компьютерной информации от несанкционированного доступа;

2) совмещение функций разработки и эксплуатации программного обеспечения в рамках одного структурного подразделения;

3) неприменение в технологическом процессе всех имеющихся средств и процедур регистрации операций, действий программ и обслуживающего персонала;

4) нарушение сроков изменения паролей пользователей, а также сроков хранения копий программ и компьютерной информации.

3. Особенности организации и проведения допроса свидетеля, потерпевшего по делам о преступлениях в сфере компьютерной информации

При расследовании преступлений в сфере компьютерной информации допросы свидетелей осуществляются с использованием тактических рекомендаций, разработанных в криминалистике. Особое значение здесь приобретает подготовка к допросу и всестороннее изучение личности допрашиваемого. При этом следует учесть, что свидетелями по данной категории дел чаще всего выступают лица с высшим образованием, обладающие высоким интеллектом, в совершенстве владеющие специальной терминологией, зачастую не вполне понятной следователю, в связи с этим следователю необходимо детализировать показания допрашиваемого постановкой уточняющих вопросов, раскрывающих содержание тех или иных терминов и определений, употребляемых допрашиваемым. Для участия в допросе может быть приглашен специалист в области вычислительной техники (необходимо, как минимум, предварительное согласование с ним формулировок задаваемых вопросов).

Основными тактическими задачами допроса потерпевших и свидетелей при расследовании дел рассматриваемой категории являются: выявление элементов состава преступления в наблюдавшихся ими действиях, установление обстоятельств, места и времени совершения значимых для расследования действий, способа и мотивов его совершения и сопутствующих обстоятельств, признаков внешности лиц, участвовавших в нем, определение предмета преступного посягательства, размера причиненного ущерба, детальные признаки похищенного, установление свидетелей и лиц, причастных к совершению преступления.

Для решения указанных задач в процессе допроса свидетеля необходимо выяснить:

1. Не проявлял ли кто-либо интереса к компьютерной информации, программному обеспечению, компьютерной технике данного предприятия, организации, учреждения, фирмы или компании?

2. Не появлялись ли в помещении, где расположена компьютерная техника, посторонние лица, не зафиксированы ли случаи работы сотрудников с информацией, не относящейся к их компетенции?

3. Не было ли сбоев в работе программ, хищений носителей информации и отдельных компьютерных устройств?

4. Зафиксированы ли сбои в работе компьютерного оборудования, электронных сетей, средств защиты компьютерной информации?

5. Как часто проверяются программы на наличие вирусов, каковы результаты последних проверок?

6. Как часто обновляется программное обеспечение, каким путем, где и кем оно приобретается?

7. Каким путем, где и кем приобретается компьютерная техника, как осуществляется ее ремонт и модернизация?

8. Каков на данном объекте порядок работы с информацией, как она поступает, обрабатывается и передается по каналам связи?

9. Кто еще является абонентом компьютерной сети, к которой подключены компьютеры данного предприятия, организации, учреждения или фирмы, каким образом осуществляется доступ в сеть, кто из пользователей имеет право на работу в сети, каковы их полномочия?

10. Как осуществляется защита компьютерной информации, применяемые средства и методы защиты и др.?

11. Могли ли возникшие последствия стать результатом неосторожного действия лица или неисправности работы ЭВМ, системы ЭВМ, сбоев программного обеспечения и т.п.?

12. Каков характер изменений информации?

13. Кто является собственником (владельцем или законным пользователем) скопированной (уничтоженной, модифицированной, блокированной) информации и др.?

При расследовании неправомерного доступа к компьютерной информации на первоначальном этапе возникает необходимость допрашивать в качестве свидетелей граждан различных категорий, для каждой из которых существует свой предмет допроса.

В зависимости от занимаемой должности свидетелей, потерпевших их допрос может иметь некоторые особенности.

В процессе допросов операторов ЭВМ следует выяснить правила ведения журналов операторов, порядок приема-сдачи смен, режим работы операторов, порядок идентификации операторов; правила эксплуатации, хранения, уничтожения компьютерных распечаток (листингов), категорию лиц, имеющих к ним доступ; порядок доступа в помещение, где находится компьютерная техника, категорию работников, допущенных к работе с ней, и др.

В процессе допроса программистов выясняется: перечень используемого программного обеспечения и его классификации (лицензионное, собственное), пароли защиты программ, отдельных устройств компьютера, частота их смен; технические характеристики компьютерной сети (при ее наличии), кто является администратором сети; порядок приобретения и сопровождения программного

обеспечения; наличие в рабочих программах специальных файлов-протоколов, регистрирующих вхождение компьютеров пользователей, каково их содержание и др.

У сотрудника, отвечающего за информационную безопасность, или администратора компьютерной сети выясняется: наличие специальных технических средств защиты информации; порядок доступа пользователей в компьютерную сеть; порядок идентификации пользователей компьютеров, распорядок рабочего дня пользователей компьютерной сети; порядок доступа сотрудников к компьютерной технике во внерабочее время, порядок присвоения и смены паролей пользователей; характеристика мер по защите информации.

У сотрудников, занимающихся техническим обслуживанием вычислительной техники, выясняется: перечень и технические характеристики средств компьютерной техники, установленных в организации, а также перечень защитных технических средств, периодичность технического обслуживания, проведения профилактических и ремонтных работ; сведения о произошедших в последнее время случаях выхода аппаратуры из строя; случаи незаконного подключения к телефонным линиям связи, установка какого-либо дополнительного электрооборудования.

У начальника вычислительного центра или руководителей предприятия (организации) следует выяснить: действуют ли в учреждении специальные службы по эксплуатации сетей и службы безопасности, их состав и обязанности; сертифицированы ли программы системной защиты; организационную структуру вычислительного центра; сертифицированы ли технические устройства вычислительной техники; действуют ли внутриведомственные правила эксплуатации ЭВМ и сети, каков порядок ознакомления с ними и контроля за их исполнением; какие сотрудники учреждения (организации) были уволены в течение интересующего периода времени и по каким мотивам; были ли ранее случаи незаконного проникновения в помещение, где установлена компьютерная техника; были ли случаи несанкционированного доступа к компьютерной информации, вирусных атак и др.

У руководителя организации, работника юридического отдела или иного лица, уполномоченного представлять интересы потерпевшего юридического лица (в ходе допроса в качестве представителя потерпевшего), выясняется: стаж работы в должности; основания для представления интересов организации в правоохранительных органах (доверенность, подписанная руководителем организации, которая приобщается к уголовному делу); откуда стало известно о произошедшем; излагаются обстоятельства, ставшие известными представителю потерпевшего; выясняются лица, могущие разъяснить следователю технические вопросы, возникающие при расследовании уголовного дела; правовая регламентация статуса информации, подвергшейся воздействию в результате преступления.

Свидетелями при расследовании неправомерного доступа к компьютерной информации могут быть лица, наблюдавшие событие преступления (особенно при непосредственном доступе) или его отдельные моменты, а также видевшие преступников непосредственно в момент совершения преступления или после него.

При этом должно быть выяснено:

1. При каких обстоятельствах свидетель наблюдал преступников (процесс совершения преступления)?

2. В чем состоял способ совершения преступления?

3. Какую роль выполнял каждый из соучастников неправомерного доступа к компьютерной информации?

4. Знает ли свидетель, какую цель преследовал обвиняемый, совершая неправомерный доступ к компьютерной информации?

5. Имели ли место подобные проявления ранее, если да, то как на них реагировали руководители предприятия, организации, учреждения, фирмы, компании?

6. Как свидетель характеризует обвиняемого и его окружение?

7. Что способствовало совершению преступления?

4. Особенности производства обыска по делам о преступлениях в сфере компьютерной информации

Обыск по делам данной категории является важным следственным действием, направленным на установление обстоятельств расследуемого события.

Надо обратить внимание, что обыск является ключевым следственным действием и отправной точкой для сбора доказательств по уголовному делу. Обыск проводится лишь после установления всех соучастников преступления, одновременно несколькими следственно-оперативными группами и сам факт возбуждения уголовного дела держится в тайне от лиц, совершивших преступление.

При наличии средств компьютерной техники в нескольких помещениях, по мнению авторов учебника, рекомендуется организовать групповой обыск одновременно во всех помещениях, где установлены ЭВМ.

В процессе подготовки к обыску помещений (до выезда на место проведения) необходимо:

1. Выяснить, какая вычислительная техника имеется в обыскиваемом помещении и ее количество.

2. Установить, используются ли в комплекте с вычислительной техникой устройства автономного или бесперебойного питания и к чему может привести отключение электроэнергии. Здесь надо знать, что практически на всех предприятиях есть источники бесперебойного питания для ЭВМ.

3. Пригласить специалиста по компьютерным системам, так как его познания будут необходимы во время подготовки к обыску, а также для оперативного анализа информации и квалифицированного ее изъятия с компьютера.

4. Подготовить соответствующую компьютерную технику, которая будет использоваться для считывания и хранения изъятой информации.

5. Изучить личность владельца компьютера, его профессиональные навыки по владению компьютерной техникой.

6. Определить время поиска и меры, обеспечивающие конфиденциальность обыска (наиболее удачными являются утренние часы – с 6.00 до 8.00, так как в это время техника, скорее всего, выключена).

7. Спрогнозировать характер возможно находящейся в компьютере информации.

Важным этапом подготовки данного следственного действия видится подбор и инструктаж членов следственно-оперативной группы. В состав СОГ помимо следователя могут входить оперативные работники, количество
которых определяется задачами следственного действия и объемом предстоящей работы. Так, для осмотра больших площадей, например предприятия, в котором имеется одна или несколько локальных сетей ЭВМ, подвергшихся неправомерному воздействию, могут привлекаться значительные силы.

Некоторое число оперативных работников может привлекаться для охраны места проведения следственного действия. Для этих же целей могут привлекаться сотрудники милиции, служб безопасности организации, представители общественности.

При подборе и расстановке лиц, участвующих в следственном действии следователь должен учитывать знание ими средств компьютерной техники и личный опыт по проведению осмотров и обысков по делам, связанным с преступлениями в сфере компьютерной информации.

В состав СОГ включают и специалистов. Как отмечалось ранее, по делам рассматриваемой категории к участию в следственном действии чаще всего привлекают специалистов-криминалистов, а также специалистов по средствам компьютерной техники. Специалисты активно используются следователем в процессе подготовки следственного действия.

Все участники СОГ обязательно инструктируются следователем и специалистами. В ходе инструктажа до участников доводятся: особенности расследуемого преступления; информация о предметах и документах, подлежащих отысканию и изъятию; информация о порядке работы и обращения со средствами компьютерной техники; порядок действий на месте и тактические приемы производства следственного действия; способы зашифровки источников используемой оперативной информации; обязанности участников следственного действия и т.д.

Субъект, производящий осмотр, не может непосредственно осмотреть содержимое машинного носителя, так как последнее представляет собой некоторую намагниченную область машинного носителя. Для этого необходимо использовать технические устройства и программные средства, позволяющие субъекту, производящему осмотр, наглядно, объективно и полно воспринимать и оценивать информацию, находящуюся на машинном носителе. Подбор технических средств осуществляется исходя из требований к обеспечению сохранности следов преступления, средств компьютерной техники, компьютерной информации.

По прибытии к месту проведения обыска необходимо быстро и неожиданно войти в обыскиваемое помещение так, чтобы предотвратить уничтожение информации на ЭВМ. Здесь следователь должен учесть, что понятые должны быть приглашены до того, как следователь предъявит постановление о производстве обыска, поскольку если возникнет заминка с поиском понятых, лицо, у которого производится обыск, может воспользоваться этим и уничтожить следы преступления. Поскольку начинать обыск до приглашения понятых нельзя, то и входить в обыскиваемое помещение тоже нельзя.

На предварительной стадии обыска, сразу после входа в помещение, необходимо организовать охрану компьютеров и не допускать к ним присутствующих в помещении.

На обзорной стадии следователь должен выполнить рекомендации, аналогичные рекомендациям по прибытию на место происшествия.

В ходе производства обыска всей следственно-оперативной группе и иным участникам необходимо знать следующее:

При обыске не следует забывать о возможностях сбора традиционных доказательств – рукописных записей, распечаток принтеров и пр., поскольку лица, совершающие преступления в сфере компьютерной информации, часто дублируют сохраненную информацию на бумажном носителе. Так, по месту жительства подозреваемого К. в ходе обыска была обнаружена и изъята записная книжка,

при осмотре которой обнаружили логин и пароль, незаконно используя который, К. выходил в сеть Интернет и пользовался услугами сети бесплатно.

В ходе обысков по делам данной категории могут быть обнаружены и изъяты следующие виды важных документов, которые могут стать вещественными доказательствами по делу:

1) журналы учета рабочего времени, доступа к вычислительной технике, ее сбоев и ремонта, регистрации пользователей компьютерной системы или сети, проведения регламентных работ;

2) лицензионные соглашения и договоры на пользование программными продуктами и их разработку;

3) книги паролей, приказов и других документов, регламентирующих работу учреждения и использование компьютерной информации. Эти документы нередко ведутся в электронной форме, поэтому к ознакомлению с ними необходимо привлекать специалиста. При изучении журналов, книг, соглашений и другой документации следователь может выяснить законность использования того или иного программного обеспечения, систему организации работы учреждения и обработки в нем информации, доступа к ней и компьютерной технике, круг лиц, имевших на это право;

4) документы, носящие следы совершенного преступления: шифрованные, рукописные записи, телефонные счета, телефонные книги, которые доказывают факты контакта преступников между собой, в том числе и по компьютерным сетям, пароли и коды доступа в сети, дневники связи, сведения о процедурах входа-выхода и пр.;

5) 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;

6) документы, описывающие аппаратуру и программное обеспечение (пояснение к аппаратным средствам и программному обеспечению) или доказывающие нелегальность их приобретения (например, ксерокопии описания программного обеспечения в случаях, когда таковые предоставляются изготовителем);

7) документы, устанавливающие правила работы с ЭВМ, нормативные акты, регламентирующие правила работы с данной ЭВМ, системой, сетью, доказывающие, что преступник их знал и умышленно нарушал;

8) личные документы подозреваемого или обвиняемого – записные книжки, учебники по программированию и т.д.

5. Взаимодействие следователя с оперативными подразделениями на первоначальном этапе расследования преступлений в сфере компьютерной информации.

19 октября 1992 года в структуре МВД образовано Бюро специальных технических мероприятий, одним из направлений деятельности которого является борьба с преступлениями в сфере компьютерных технологий.

С 2001 года в составе БСТМ функционирует Управление «К».

Основные направления работы Управления «К» БСТМ МВД России:

- выявление и пресечение фактов неправомерного доступа к компьютерной информации;
- борьба с изготовлением, распространением и использованием вредоносных программ для ЭВМ;

- противодействие мошенническим действиям с использованием возможностей электронных платежных систем;
- борьба с распространением порнографических материалов с участием несовершеннолетних через сеть Интернет.
- пресечение противоправных действий в информационно-телекоммуникационных сетях, включая сеть Интернет:
- выявление и пресечение преступлений, связанных с незаконным использованием ресурсов сетей сотовой и проводной связи;
- противодействие мошенническим действиям, совершаемым с использованием информационно-телекоммуникационных сетей, включая сеть Интернет;
- противодействие и пресечение попыток неправомерного доступа к коммерческим каналам спутникового и кабельного телевидения.
- борьба с незаконным оборотом радиоэлектронных и специальных технических средств.
- выявление и пресечение фактов нарушения авторских и смежных прав в сфере информационных технологий.
- борьба с международными преступлениями в сфере информационных технологий:
- противодействие преступлениям в сфере информационных технологий, носящим международный характер;
- взаимодействие с национальными контактными пунктами зарубежных государств.
- международное сотрудничество в области борьбы с преступлениями, совершаемыми с использованием информационных технологий.

ТЕМА ЛЕКЦИИ: ПРОВЕРКА ТИПИЧНЫХ ВЕРСИЙ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

ПЛАН

1) Некоторые проблемы выявления преступлений в сфере компьютерной информации.
2) Проверка версий при расследовании преступлений в сфере компьютерной информации.
3) Особенности проведения отдельных следственных действий и тактических операций.

Форма и методы обучения: слайдовая презентация.

Преступления, связанные с криминальным использованием ЭВМ, их систем и сетей, совершаются различными способами, основными из которых являются: неправомерный доступ к чужой компьютерной информации (хищение или копирование информации, копирование документов, изготовление их дубликатов и проч.); изготовление и распространение вредоносных программ, приводящих к нарушению целостности и конфиденциальности информации (ее уничтожению, блокированию, модификации и др.); нарушение правил эксплуатации ЭВМ, ведущее к нарушению целостности и конфиденциальности информации.

Все эти преступления весьма специфичны с точки зрения способов, средств их совершения и их субъектов. Совершаются такие преступления в обстановке особой интеллектуальной профессиональной деятельности с использованием компьютерной техники. Субъектами преступлений, как правило, являются лица, владеющие специальными знаниями в области управления ЭВМ.

Криминалистическая характеристика этих преступлений проявляется в своеобразии предмета преступного посягательства, способов их совершения и типовых чертах их субъектов.

В начале расследования данных преступлений обычно возникают следующие типовые ситуации:

1) заявление о неправомерном доступе к чужой информации или нарушении ее целостности и конфиденциальности поступило от собственника информационной системы, обнаружившего этот факт, при этом есть сведения о причастном лице;

2) та же ситуация, но данных о причастности к указанным противоправным действиям какого-либо лица в заявлении не имеется;

3) факт указанных противоправных действий обнаружен оперативно-розыскными органами и соответствующим образом зафиксирован.

Во всех описанных ситуациях основные первоначальные задачи обычно сводятся к установлению: данных, позволяющих судить о способе совершения преступления; порядка регламентации конкретной информационной системы ее собственником; круга лиц, работающих с системой и имеющих к ней доступ; и т. д.

Для решения названных задач чаще всего проводятся такие первоначальные следственные действия, как допросы собственников данных информационных систем и свидетелей; осмотр ЭВМ и машинных носителей; выемка и осмотр необходимой документации. При этом осмотры и выемки должны проводиться с участием специалистов в области компьютерной техники. Участие специалистов в расследовании преступлений в сфере компьютерной информации является их специфической методической особенностью.

Рассмотренные действия обычно позволяют выявить и других необходимых свидетелей, которых нужно допросить; определить круг лиц, причастных к данному деянию, а также примерный размер ущерба, причиненного владельцу информационной системы.

Если правонарушитель задержан на месте преступления или сразу после него, он должен быть обыскан, допрошен. Необходимо провести обыск у него дома и на работе.

Дальнейшие следственные действия связаны с изъятием ЭВМ, ее устройств, их осмотром и, если необходимо, экспертным исследованием, допросами новых свидетелей, предъявлением обвинения и допросом обвиняемого.

Рассматриваемые преступления объединяют общие объект и предмет преступного посягательства, используемые орудия и средства, сходство способов преступлений и следовой картины произошедших событий, а также личностных свойств субъектов.

Непосредственным объектом преступлений в сфере компьютерной информации выступают общественные отношения по обеспечению информационной безопасности. Последняя представляет собой состояние защищенности информации, хранимой и обрабатываемой в автоматизированной системе, от негативного воздействия на нее с точки зрения нарушения ее

физической и логической целостности (уничтожения, искажения) или несанкционированного использования.

Предметом посягательства при совершении рассматриваемых преступлений является компьютерная информация. Последняя (как вид информации вообще) представляет собой сведения, знания, предназначенные для использования в ЭВМ или управления ею, находящиеся в ЭВМ или на машинном носителе, имеющие собственника, установившего правила использования этой информации.

Компьютерная информация, будучи разновидностью информации вообще, имеет свою специфику:

1) объемна и быстро обрабатываема — современные компьютеры способны производить более 4 млрд элементарных операций в секунду и могут быть оснащены накопителями на жестких магнитных дисках (НЖМД) емкостью 500 байт и более, что составляет около 150 млн страниц (неформатированного текста);

2) легко удаляема, причем при удалении отдельного файла физически он продолжает оставаться на носителе информации до момента записи на его место новой информации либо физического разрушения ее носителя;

3) обезличена, т.е. между ней и лицом, которое ее создает и использует, нет жесткой связи;

4) может находиться лишь на машинном носителе (НЖМД, дискете, магнитной ленте, компакт-диске, карте памяти и др.), в самой ЭВМ (оперативных и постоянных запоминающих устройствах), системе ЭВМ, сети ЭВМ, при этом ее содержание не зависит от типа используемого материального носителя (так, при копировании информации с дискеты на жесткий диск оба файла — оригинал и копия — с точки зрения содержания будут тождественны);

5) может создаваться, изменяться, копироваться, применяться (использоваться) только с помощью ЭВМ при наличии соответствующих периферийных устройств для ее ввода, чтения (чте- ния/записи), передачи, при этом компьютерная информация может быть перенесена на новый носитель с удалением на первоисточнике, а может быть скопирована и оставлена на первоисточнике (число подобных копий может быть неограниченным);

6) легко передается по телекоммуникационным каналам связи компьютерных сетей, причем практически любой объем информации можно передать на любое расстояние, при этом ей свойственна способность к сжатию; специальные программы (архиваторы WinRar, WinZip, Arj и др.) позволяют сжимать информацию до нескольких раз, а при разархивировании происходит ее восстановление в первоначальный вид без изменения содержания; доступ к одному и тому же файлу, содержащему информацию, могут иметь одновременно несколько пользователей.

Подготовка к совершению преступлений в сфере компьютерной информации имеет место в большинстве случаев. Можно выделить следующие основные ее направления.

1. Изучение специальных вопросов, которые могут касаться изучения особенностей работы и уязвимостей программных продуктов, аппаратно-программных средств и сетей передачи данных, способов преодоления защиты информации и др. Много полезной информации преступники получают путем изучения литературы и тематических сайтов в сети Интернет.

2. Подыскание объекта посягательства и сбор сведений о нем осуществляются исходя из ценности информации, хранимой или

обрабатываемой в информационной системе, используемых в ней средств защиты информации и других обстоятельств.

3. Подбор соучастников, распределение ролей между ними и их инструктаж.

4. Подбор специальных (аппаратных, программных) средств, предназначенных для преодоления защиты информации. Каждой категории средств защиты (организационно-тактических, программно-технических) соответствует свой набор средств их преодоления.

5. Установление аутентификационных данных (имя, пароль, код доступа и пр.) для доступа к интересующей информации методами социальной инженерии (посредством выведывания их под различными предлогами у законных пользователей информационных ресурсов. Распространением программ, копирующих и направляющих преступнику данные законных пользователей, а также визуального наблюдения и др.

Способы совершения преступлений в зависимости от формы контакта с компьютерной техникой можно разделить на непосредственные и опосредованные.

Непосредственный доступ осуществляется при прямом контакте преступника с объектом, содержащим соответствующую информацию. При этом возможно проникновение в закрытые зоны и помещения, где производится обработка информации.

Опосредованный доступ осуществляется при удаленном контакте преступника с объектом, содержащим соответствующую информацию. Способы с помощью опосредованного доступа можно разделить на две группы:

1) использующие системы и сети передачи данных, в том числе: непосредственное соединение с объектом с использованием современных средств передачи данных (модем, Bluetooth, Wi-Fi и т.п.); соединение с объектом с использованием локальных сетей передачи данных; соединение с объектом с использованием глобальных сетей передачи данных.

2) способы, использующие перехват: информации путем подключения к сетям передачи данных; электромагнитного излучения; аудиосигналов и видеоизображений.

Также в зависимости от степени участия человека в непосредственном процессе совершения преступления способы совершения можно разделить на командные и программные.

К командным способам относятся способы, при которых преступник непосредственно запускает программы на выполнение.

К программным способам относятся способы, при которых негативные последствия наступают в результате работы программ, запущенных без непосредственного участия преступника.

Следы преступления в данном случае весьма специфичны. Наряду с такими традиционными следами, как следы рук и микрочастицы на вычислительной технике и машинных носителях, а также рукописные записи, распечатки и пр., при подготовке и совершении преступлений в сфере компьютерной информации возникают следы, являющиеся результатами не непосредственного контакта с материальными объектами, а опосредованного отражения материальных объектов, процессов и результатов ввода, обработки и передачи информации.

Компьютерные следы представляют собой компьютерную информацию на машинном носителе или в средстве вычислительной техники, причинно связанную с событием преступления. Она остается на машинных носителях в

виде либо информации, отражающей свойства материальных объектов, либо результатов работы пользователя, либо сведений о процессах ее ввода, обработки и передачи.

В качестве информации, отражающей свойства материальных объектов, как правило, выступают файлы (наборы файлов, фрагменты файлов) содержащие фото и видео изображения, аудиозаписи, полученные путем преобразования видео и аудио сигналов в цифровую форму.

В качестве результатов работы пользователя можно рассматривать файлы (наборы файлов, фрагменты файлов), содержащие информацию, введенную пользователем с использованием таких устройств ввода как клавиатура, манипулятор мышь и т.п. и/или обработанную с помощью компьютерных программ.

К сведениям о процессах ввода, обработки и передачи компьютерной информации можно отнести метаданные файлов, протоколы работы программ, файлы, появляющиеся в процессе работы программ, информация, содержащаяся в файловых системах и др.

Компьютерные следы могут быть выявлены соответствующими специалистами в средствах вычислительной техники и машинных носителях.

Особое значение для установления лиц, совершивших преступления посредством использования сети Интернет, имеет следующая информация:

• IP-адрес компьютера, с которого произведен неправомерный доступ;

• данные о фирме-провайдере, устанавливаемые через специальный сервис (www. ripe.net) путем ввода IP-адреса интересующего компьютера;

• сведения об устройствах, с помощью которых осуществлялась связь с провайдером (номер телефона, MAC-адрес сетевой карты и т.п.);

• сведения о работе абонента в сети со стороны провайдера (дата и время начала и окончания сеансов связи, объем отправленной и полученной информации, возможно, перечень посещенных сетевых ресурсов и пр.);

• сведения о работе абонента в сети с определенного компьютера;

• регистрационные данные на абонента электронной почты, интернет-пейджера и пр.

Компьютерные следы — это отражение события преступления в информационном поле; будучи материальными по своей природе, они не являются результатом непосредственного контакта со следообразующим объектом; они обладают способностью к дублированию, т.е. переносу (копированию) на другие носители информации без какого-либо изменения их существенных характеристик, легко изменяемы и удаляемы.

Способы сокрытия преступлений в сфере компьютерной информации можно разделить на следующие группы:

• удаление оставленных следов (воссоздание обстановки, предшествующей совершению преступления, уничтожение следов рук, обуви, удаление компьютерных следов и т.п.);

• подмена следов (в том числе подмена информации в компьютерных следах).

Наиболее распространенными способами сокрытия компьютерных следов преступления являются следующие:

• удаление информации о действиях преступника из протоколов работы программ;

• удаление файлов, создающихся или изменяющихся в процессе совершения преступления;

• использование анонимных прокси-серверов, межсетевых экранов, специализированного программного обеспечения, позволяющих подменять информацию об IP-адресе, MAC-адресе;

• использование ремейлеров и программ-анонимизаторов, позволяющих осуществлять переадресацию электронной почты, направляя ее с другого компьютера либо изменять данные об обратном адресе и службе электронной почты отправителя;

• использование учетных записей, созданных от чужого (вымышленного) имени.

О лицах, совершающих преступления в сфере компьютерной информации, можно привести следующие данные. Их возраст колеблется в широких границах — от 15 до 45 лет. Большинство лиц рассматриваемой категории составляют мужчины. Хотя совершить такое преступление может и человек, обладающий минимально необходимыми познаниями для работы в качестве пользователя ЭВМ, большой процент среди преступников составляют лица, обладающие специальными знаниями, умениями и навыками, обладающими интеллектуальными способностями среднего, либо выше среднего уровня, имеющими среднее специальное и высшее образование. Как правило, на личном или рабочем компьютере такого лица расположены подборки с информацией, посвященной различным технологиям совершения преступных деяний и соответствующее им программное обеспечение.

Достаточно часто преступления в сфере компьютерной информации совершаются устойчивыми преступными группами, для которых характерны мобильность, высокая техническая оснащенность, четкое распределение ролей, ярко выраженная корыстная мотивация, хорошо продуманная система сокрытия следов преступных деяний.

Преступники, совершающие рассматриваемые преступления, как правило, руководствуются следующими мотивами: корысть, месть, личные неприязненные отношения с сослуживцами и руководством по месту работы, стремление скрыть другое преступление, хулиганские побуждения и озорство, исследование компьютерной информации и/или систем ее обработки, демонстрация личных интеллектуальных способностей или превосходства.

ТЕМАТИЧЕСКИЙ ПЛАН СЕМИНАРСКИХ ЗАНЯТИЙ ДИСЦИПЛИНЫ

Наименование модуля и программного материала	Количество часов
Модуль 1. Источники теоретических основ криминалистической методики расследования преступлений в сфере компьютерной информации.	
Практические (семинарские) занятия	
1.1. *Тема занятия:* Правоотношения в сфере компьютерной информации и криминализация компьютерных правонарушений	2
План семинарского занятия: Структура теоретических основ криминалистической методики расследования преступлений в сфере компьютерной информации (цифровой криминалистики). *Формы и методы обучения:* Мозговой штурм, работа в группах	
1.2. Тема занятия: Методические основы расследования преступлений в сфере компьютерной информации. *План семинарского занятия:* Характеристика личности преступников в сфере компьютерной информации. Основные ситуации первоначального этапа расследования преступлений в сфере компьютерной информации. *Формы и методы обучения:* Просмотр видеоролика и обсуждение в группе.	2
1.3 Тема занятия: Предварительное исследование компьютерных объектов при расследовании преступлений в сфере компьютерной информации. *План семинарского занятия:* Общие положения предварительного исследования объектов кибернетического пространства. Обыск и выемка компьютерных объектов. *Формы и методы обучения:* просмотр видеороликов и обсуждение в группе	2
1.4 Тема занятия: Получение и проверка вербальной информации, связанной с компьютерными объектами. *План семинарского занятия:* Основные возможности компьютерно-технических экспертиз и тактические рекомендации по их назначению. *Формы и методы обучения:* просмотр видеороликов и обсуждение в группе	2
Итого по модулю: 8 семинарских занятий	**8**
Модуль 2. Уголовно-правовая, криминалистическая и криминологическая характеристика преступлений в сфере компьютерной информации	
Практические (семинарские) занятия	
2.1. *Тема занятия:* Криминологическая характеристика преступлений в сфере компьютерной информации *План лабораторного занятия:* Криминологическая характеристика преступлений в сфере компьютерной информации. *Форма и методы обучения:* анализ статистических сведений по данным видам преступлений, решение кейсовых задач	2

2.2. *Тема занятия:* Криминалистическая характеристика неправомерного доступа к компьютерной информации *План лабораторного занятия:* Особенности обстановки совершения неправомерного доступа к компьютерной информации. Характеристика механизма неправомерного доступа к компьютерной информации. *Форма и методы обучения:* просмотр видеоролика и обсуждения.	2
2.3. *Тема занятия:* Разновидности типичных версий при расследовании преступлений в сфере компьютерной информации *План лабораторного занятия:* Некоторые проблемы выявления преступлений в сфере компьютерной информации. Проверка версий при расследовании преступлений в сфере компьютерной информации. Особенности проведения отдельных следственных действий и тактических операций. *Форма и методы обучения:* работа в малых группах, разработка версий.	3
Итого по модулю 2 **семинаров - 6**	**7**
Итого	15

Министерство образования и науки Республики Казахстан
РГП ПХВ «Евразийский национальный университет им. Л.Н. Гумилева»

Кафедра уголовно-правовых дисциплин

УТВЕРЖДАЮ
Декан юридического
факультета
д.ю.н., профессор
_____ Сматлаев Б.М.
«___» _____ 2021 г.

Рабочая (модульная) учебная программа (Syllabus)

LAWS 63006 - Уголовно-процессуальные и криминалистические методы противодействия преступности
(код и наименование модуля)

по дисциплине OMRPSKI 6309 - Основы методики расследования преступлений в компьютерной информации
(код и наименование дисциплины)

для обучающихся образовательной программы

7МО4204 – Судебная власть и Уголовная юстиция
(Код и наименование образовательной программы)

2021

	Евразийский национальный университет им. Л.Н. Гумилева	Рабочая (модульная) учебная программа (Syllabus)	Издание: первое

Разработчик
или разработчики _____ к.ю.н., .доцент Баймолдина С.М.
(Ф.И.О., занимаемая должность, ученая степень)

Рассмотрено на заседании кафедры уголовно-правовых дисциплин

протокол № 11 от « 15 » 06 2021 г.

Заведующий кафедрой _____ Сембекова Б.Р.
(подпись) (Ф.И.О.)

Одобрено на заседании Учебно-методической комиссии факультета

« 17 » 06 2020 г. Протокол № 11

Председатель УМК факультета _____ Жадауова Ж.

Ф ЕНУ 703-13-17 Рабочая (модульная) учебная программа (Syllabus). Издание первое

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

1. Краткое описание дисциплины: ознакомление обучающихся с основами методики расследования преступлений в компьютерной информации электронно-цифровых объектов с использованием тактико-криминалистических средств и методов обеспечения, основанных на современных достижениях наук цифровых технологий, научной организации труда.

Цели изучения учебной дисциплины: в разработке методологических основ изучения, ситуаций и ситуаций, связанных с раскрытием и расследованием преступлений в сфере компьютерной информации, их прогнозирование и анализ с целью своевременного предупреждения и разрешения в интересах эффективного производства предварительного следствия, и на основании полученных результатов обосновать необходимость дополнения общей части криминалистики новым частным учением о методике расследования преступлений в сфере компьютерной информации.

Формирование у обучающихся знаний и навыков, позволяющих выявлять и расследовать преступления в сфере компьютерной информации.

Задачи изучения учебной дисциплины: обучающиеся должны знать следующее: криминалистическую и криминологическую характеристику преступлений в сфере компьютерной информации; типичные поводы и основания для возбуждения уголовных дел о преступных посягательствах данного вида; основные сведения и документы, которые должны находится в распоряжении уполномоченного лица для принятия обоснованного решения о возбуждении уголовного дела при расследовании преступлений в сфере компьютерной информации; типичные следственные ситуации первоначального этапа их расследования; алгоритм действий следователя (дознавателя) в случаях, когда информация о мотивах, способе совершения преступного деяния и личности лица, его совершившего, отсутствует, а также других спорных случаях при расследовании ;

2. Пререквизиты

Для освоения данной дисциплины необходимы знания, умения и навыки, приобретённые при изучении следующих дисциплин: Уголовное право РК, Уголовно-процессуальное право РК, Криминалистика, Криминология, Особые уголовно-процессуальные производства.

Постреквизиты

Знания, умения и навыки, полученные при изучении дисциплины необходимы для освоения следующих дисциплин: современные методы борьбы с организованной преступностью, следственные действия, оперативно-розыскная деятельность.

3. Выписка из учебного плана

Курс___2_____
Семестр____3_____
Количество кредитов_____5_____

Виды занятий	Общее количество часов
Лекции	30
Семинарское занятие	15
СРО	105
Итого	150

ТЕМАТИЧЕСКИЙ ПЛАН ДИСЦИПЛИНЫ ПО МОДУЛЯМ

(в академических часах)

№ недели	Наименование модуля и программного материала	Количество часов
1-7	**Модуль 1. Источники теоретических основ криминалистической методики расследования преступлений в сфере компьютерной информации.**	
	Лекции	
	1.1. *Тема занятия:* Становление правоотношений в сфере компьютерной информации и криминализация компьютерных правонарушений. *Краткое содержание:* Понятие и сущность преступлений в сфере компьютерной информации. Состав и структура теоретических основ криминалистической методики расследования преступлений в сфере компьютерной информации (цифровой криминалистики). *Формы и методы обучения: с*лайдовая презентация, объяснительно-иллюстративные методы.	4
	1.2 *Тема занятия:* Методические основы расследования преступлений в сфере компьютерной информации. *Краткое содержание:* Состав, структура и особенности криминалистической характеристики преступлений в сфере компьютерной информации. Механизм следообразования при совершении преступлений в сфере компьютерной информации. Характеристика личности преступников в сфере компьютерной информации. Способы совершения преступлений в сфере компьютерной информации. Основные ситуации первоначального этапа расследования преступлений в сфере компьютерной информации. *Формы и методы обучения:* просмотр видеороликов и обсуждение в группе	4
	1.3 *Тема занятия:* Предварительное исследование компьютерных объектов при расследовании преступлений в сфере компьютерной информации. *Краткое содержание:* Общие положения предварительного исследования объектов кибернетического пространства. Обыск и выемка компьютерных объектов. Особенности осмотра отдельных видов компьютерных объектов *Формы и методы обучения:* просмотр видеороликов и обсуждение в группе	4
	1.4 *Тема занятия:* Получение и проверка вербальной информации, связанной с компьютерными объектами. *Краткое содержание:* Допрос. Следственный эксперимент. Основные возможности компьютерно-технических экспертиз и тактические рекомендации по их назначению. *Формы и методы обучения:* просмотр видеороликов и обсуждение в группе	4
	Практические (семинарские) занятия	
	1.1. *Тема занятия:* Правоотношения в сфере компьютерной информации и криминализация компьютерных правонарушений	2

	План семинарского занятия: Структура теоретических основ криминалистической методики расследования преступлений в сфере компьютерной информации (цифровой криминалистики). *Формы и методы обучения:* Мозговой штурм, работа в группах	
	1.2. Тема занятия: Методические основы расследования преступлений в сфере компьютерной информации. *План семинарского занятия:* Характеристика личности преступников в сфере компьютерной информации. Основные ситуации первоначального этапа расследования преступлений в сфере компьютерной информации. *Формы и методы обучения:* Просмотр видеоролика и обсуждение в группе.	2
	1.3 Тема занятия: Предварительное исследование компьютерных объектов при расследовании преступлений в сфере компьютерной информации. *План семинарского занятия:* Общие положения предварительного исследования объектов кибернетического пространства. Обыск и выемка компьютерных объектов. *Формы и методы обучения:* просмотр видеороликов и обсуждение в группе	2
	1.4 Тема занятия: Получение и проверка вербальной информации, связанной с компьютерными объектами. *План семинарского занятия:* Основные возможности компьютерно-технических экспертиз и тактические рекомендации по их назначению. *Формы и методы обучения:* просмотр видеороликов и обсуждение в группе	2
	СРО	
	1.1. *Тема и задание СРО:* Криминалистическая классификация преступлений в сфере компьютерной информации *Краткое содержание:* подготовить реферат по данной теме *Срок сдачи СРО: в понедельник 2 недели*	10
	1.2 *Тема и задание СРО:* Методические основы расследования преступлений в сфере компьютерной информации. *Краткое содержание:* Способы совершения преступлений в сфере компьютерной информации. Основные ситуации первоначального этапа расследования преступлений в сфере компьютерной информации. *Краткое содержание: п*одготовить эссе по данной теме *Срок сдачи СРО: в понедельник 2 недели*	10
	1.3 Тема и задание СРО: Особенности осмотра отдельных видов компьютерных объектов *Краткое содержание: п*одготовить эссе по данной теме *Срок сдачи СРО: в понедельник 3 недели*	10
	1.4 Тема занятия: Получение и проверка вербальной информации, связанной с компьютерными объектами. *Краткое содержание:* Основные возможности компьютерно-технических экспертиз и тактические рекомендации по их назначению. *Срок сдачи СРО: в понедельник 4 недели*	10
	Итого по модулю 1 16 лекций, 8 семинарских занятий, 40 СРО	**64**

	Модуль 2. Уголовно-правовая, криминалистическая и криминологическая характеристика преступлений в сфере компьютерной информации	
	Лекции	
	2.1. *Тема занятия:* Уголовно-правовая характеристика преступлений в сфере компьютерной информации *Краткое содержание:* Характеристика компьютерной информации. Уголовно-правая характеристика преступлений в сфере компьютерной информации. *Форма и методы обучения:* обзорная форма лекции, слайдовые презентации	4
	2.2. *Тема занятия:* Криминалистическая характеристика преступлений в сфере компьютерной информации *Краткое содержание:* Формирование модели преступления в сфере компьютерной информации. Исследование модели: построение типовых версий. *Форма и методы обучения:* решение кейс-задач	4
	2.3. *Тема занятия:* Проверка типичных версий при расследовании преступлений в сфере компьютерной информации *Краткое содержание:* Некоторые проблемы выявления преступлений в сфере компьютерной информации. Проверка версий при расследовании преступлений в сфере компьютерной информации. Особенности проведения отдельных следственных действий и тактических операций. *Форма и методы обучения:* слайдовая презентация.	4
	Практические (семинарские) занятия	
	2.1. *Тема занятия:* Криминологическая характеристика преступлений в сфере компьютерной информации *План лабораторного занятия:* Криминологическая характеристика преступлений в сфере компьютерной информации. *Форма и методы обучения:* анализ статистических сведений по данным видам преступлений, решение кейсовых задач	2
	2.2. *Тема занятия:* Криминалистическая характеристика неправомерного доступа к компьютерной информации *План лабораторного занятия:* Особенности обстановки совершения неправомерного доступа к компьютерной информации. Характеристика механизма неправомерного доступа к компьютерной информации. *Форма и методы обучения:* просмотр видеоролика и обсуждения.	2
	2.3. *Тема занятия:* Разновидности типичных версий при расследовании преступлений в сфере компьютерной информации *План лабораторного занятия:* Некоторые проблемы выявления преступлений в сфере компьютерной информации. Проверка версий при расследовании преступлений в сфере компьютерной информации. Особенности проведения отдельных следственных действий и тактических операций. *Форма и методы обучения:* работа в малых группах, разработка версий.	2
	СРО	
	2.1. *Тема и задания СРО:* подготовить эссе по данной теме Криминологическая характеристика преступлений в сфере компьютерной информации.	7

	Краткое содержание: Факторы, детерминирующие совершение преступлений в сфере компьютерной информации. *Сроки сдачи СРО:* в понедельник 4 недели	
	2.2. *Тема и задания СРО:* подготовить реферат по данной теме Криминалистические значимые аспекты неправомерного доступа к компьютерной информации *Краткое содержание*: подготовить глоссарий и слайд по данной теме. *Сроки сдачи СРО:* в понедельник 5 недели	8
	2.3. *Тема и задания СРО:* подготовить слайдовую презентацию на тему: Особенности производства основных следственных действий при расследовании неправомерного доступа к компьютерной информации. *Краткое содержание*: Основные способы расследование неправомерного доступа к компьютерной информации. Применение тактических действий и следственных приемов. *Сроки сдачи СРО:* в понедельник 6 недели	8
	Итого по модулю 2 **лекций - 12, семинаров - 6, СРО - 23**	**41**
ИТОГО		**150**

4. Краткая организационно-методическая характеристика дисциплины
Виды контроля учебных достижений:

Рубежный 1 принимается в форме коллоквиума по вопросам или по тестам для этого вида контроля, представленный в УМКД

Рубежный 2 принимается в форме коллоквиума по вопросам или по тестам для этого вида контроля, представленный в УМКД

Итоговый: экзамен в устной форме по экзаменационным билетам, утвержденным на заседании кафедры.

Политика и процедуры курса

Дисциплина является элективной. Объем учебной нагрузки составляет 6 кредитов, из них 30 часов - лекций, 30 часов - семинарские занятия, 120 часов – самостоятельная работа обучающихся.

Требования: обязательное посещение аудиторных занятий, активное участие в обсуждении вопросов, предварительная подготовка к лекциям и семинарским занятиям по рекомендованным источникам, качественное и своевременное выполнение заданий по СРО, участие во всех видах контроля (текущий контроль, контроль СРО, рубежный контроль, промежуточный контроль).

5. Система оценки результатов учебных достижений обучающихся

Знания, умения и навыки студентов оцениваются по следующей системе

Оценка по буквенной системе	Цифровой эквивалент	Баллы (%-ное содержание)	Оценка по традиционной системе
A	4,0	95-100	Отлично
A-	3,67	90-94	
B+	3,33	85-89	Хорошо

B	3,0	80-84	
B-	2,67	75-79	
C+	2,33	70-74	
C	2,0	65-69	Удовлетворительно
C-	1,67	60-64	
D+	1,33	55-59	
D-	1,0	50-54	
FX	0,5	25-49	Неудовлетворительно
F	0	0-24	

Таблица 1

Оценка	Критерий
Оценка A	- ставится в том случае, когда дан полный, развернутый ответ на поставленный вопрос, показана совокупность осознанных знаний об объекте, проявляющаяся в свободном оперировании понятиями, умении выделить существенные и несущественные его признаки, причинно-следственные связи. Знание об объекте демонстрируется на фоне понимания его в системе данной науки и междисциплинарных связей. Ответ формулируется в терминах науки, изложен литературным языком, логичен, доказателен, демонстрирует авторскую позицию обучающихся.
Оценка A-	- ставится в том случае, когда дан полный, развернутый ответ на поставленный вопрос, показана совокупность осознанных знаний об объекте, доказательно раскрыты основные положения темы; в ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. Знание об объекте демонстрируется на фоне понимания его в системе данной науки и междисциплинарных связей. Ответ изложен литературным языком в терминах науки. Могут быть допущены недочеты в определении понятий, исправленные обучающимся самостоятельно в процессе ответа.
Оценка B+	- ставится в том случае, когда обучающимся дан полный, развернутый ответ на поставленный вопрос, доказательно раскрыты основные положения темы в ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. Ответ изложен литературным языком в терминах науки. В ответе допущены недочеты, исправленные обучающимся с помощью преподавателя.
Оценка B	- ставится в том случае, когда дан полный, развернутый ответ на поставленный вопрос, показано умение выделить существенные и несущественные признаки, причинно-следственные связи. Ответ четко структурирован, логичен, изложен литературным языком в терминах науки. Могут быть допущены недочеты или незначительные ошибки, исправленные обучающимся с помощью преподавателя.
Оценка B-	- ставится в том случае, когда дан развернутый ответ на поставленный вопрос, показано умение выделить существенные и несущественные признаки, причинно-следственные связи. Ответ четко структурирован, логичен, изложен в терминах науки. Однако допущены незначительные ошибки или недочеты, исправленные обучающимся с помощью наводящих вопросов.
Оценка C+	- ставится в том случае, когда дан полный, но недостаточно последовательный ответ на поставленный вопрос, но при этом показано

	умение выделить существенные и несущественные признаки и причинно-следственные связи. Ответ логичен и изложен в терминах науки. Могут быть допущены 1-2 ошибки в определении основных понятий, которые обучающийся затруднился исправить самостоятельно.
Оценка C	- ставится в том случае, когда дан недостаточно полный и недостаточно развернутый ответ. Логика и последовательность изложения имеют нарушения. Допущены ошибки в раскрытии понятий, употреблении терминов. Обучающийся не способен самостоятельно выделить существенные и несущественные признаки и причинно-следственные связи. Обучающийся может конкретизировать обобщенные знания, доказав на примерах их основные положения только с помощью преподавателя. Речевое оформление требует поправок, коррекции.
Оценка C-	- ставится в том случае, когда дан неполный ответ, логика, и последовательность изложения имеют существенные нарушения. Допущены грубые ошибки при определении сущности раскрываемых понятий, теорий, явлений, вследствие непонимания обучающимся их существенных и несущественных признаков и связей. В ответе отсутствуют выводы. Умение раскрыть конкретные проявления обобщенных знаний не показано. Речевое оформление требует поправок, коррекции.
Оценка D+	- ставится в том случае, когда дан неполный ответ. Присутствует нелогичность изложения. Обучающий затрудняется с доказательностью. Масса существенных ошибок в определениях терминов, понятий, характеристике фактов, явлений. В ответе отсутствуют выводы. Речь неграмотна. При ответе на дополнительные вопросы Обучающий начинает осознавать существование связи между знаниями только после подсказки преподавателя.
Оценка D	- ставится в том случае, когда дан неполный ответ, представляющий собой разрозненные знания по теме вопроса с существенными ошибками в определениях. Присутствуют фрагментарность, нелогичность изложения. Обучающий не осознает связь данного понятия, теории, явления с другими объектами модуля (дисциплины). Отсутствуют выводы, конкретизация и доказательность изложения. Речь неграмотная. Дополнительные и уточняющие вопросы преподавателя не приводят к коррекции ответа обучающегося не только на поставленный вопрос, но и на другие вопросы модуля (дисциплины).
Оценка FX	- ставится в том случае, если обучающийся обнаружил пробелы в знании основного материала, предусмотренного программой, не освоил более половины программы модуля (дисциплины), в ответах допустил принципиальные ошибки, не выполнил отдельные задания, предусмотренные формами текущего, промежуточного и итогового контроля, не проработал всю основную литературу, предусмотренную программой.
Оценка F	- ставится в том случае, когда обучающийся не смог дать ответ по теме вопроса, не владеет категориями и определениями либо допускает существенные ошибки в определениях, не освоил более половины программы модуля (дисциплины), не выполнил задания, предусмотренные формами текущего, промежуточного и итогового контроля, не проработал всю основную литературу, предусмотренную программой.

6. Учебно-методическая обеспеченность дисциплины

№	Автор, наименование, год издания	Носитель информа-ции	Имеется в наличии (шт.)	
			В библиотеке	На кафедре
Основная литература				
1	Вещественные доказательства: Информационные технологии процессуального доказывания / под общ. ред. В.Я. Колдина. М.: НОРМА, 2018. - 742 с.	учебник	10	+
2	Волеводз, А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества / А.Г. Волеводз. М.: Юрлитинформ, 2017. - 496 с.	учебник	10	+
3	Гаврилин, Ю.В. Расследование неправомерного доступа к компьютерной информации: Учебное пособие / Ю.В. Гаврилин; под ред. проф. Н.Г. Шурухнова. М.: ЮИ МВД РФ, Книжный мир, 2018. - 88 с.	учебник	10	+
4	Гаврилов, М.В. Осмотр при расследовании преступлений в сфере компьютерной информации / М.В. Гаврилов, А.Н. Иванов. М.: Юрлитинформ, 2007. - 168 с.	электрон-ный	10	+
5	Расследование преступлений в сфере компьютерной информации и электронных средств платежа : учебное пособие для вузов / С. В. Зуев [и др.] ; ответственный редактор С. В. Зуев, В. Б. Вехов. — Москва : Издательство Юрайт, 2021. — 243 с. ISBN 978-5-534-13898-6. Эл.ист.: https://urait.ru/bcode/467208	электрон-ный	10	+
Дополнительная литература				
1	Дворецкий, М.Ю. Преступления в сфере компьютерной информации: понятие, система, проблемы квалификации и наказания: монография / М.Ю. Дворецкий. Тамбов: Изд-во ТГУ им. Г.Р. Державина, 2003.-197с.	Учебное пособие	1	+
2	Дикарев, В.И. Защита объектов и информации от несанкционированного доступа / В.И. Дикарев, В.А. Заренков, Д.В. Заренков, Б.В. Койнаш; под ред.	Учебное пособие	1	+

	В.А. Заренкова. СПб: Стройиздат СПб, 2004. - 320 с.			
3	Жмыхов, А.А. Особенности современной компьютерной преступности за рубежом / А.А. Жмыхов // Преступное поведение (новые исследования): Сб. статей; под общей ред. проф. Ю.М. Антоняна. М.: ВНИИ МВД России, 2002. - С. 293-304.	Учебное пособие	1	+

Список обязательной и дополнительной литературы и источников к курсу и теме

Основная литература:

1. Вещественные доказательства: Информационные технологии процессуального доказывания , В.Я. Колдин, Москва, М.: НОРМА, 2018, 742 с.;

2. Расследование преступлений в сфере компьютерной информации и электронных средств платежа : учебное пособие для вузов , С. В. Зуев [и др.] ; ответственный редактор С. В. Зуев, В. Б., Москва, Москва : Издательство Юрайт, 2021, 243 с.;

3. Преступления в сфере компьютерной информации: понятие, система, проблемы квалификации и наказания: монография , Дворецкий, М.Ю. , Тамбов, Тамбов: Изд-во ТГУ им. Г.Р. Державина, 2003, 197 с..

Основные вопросы:

1) Становление правоотношений в сфере компьютерной информации и криминализация компьютерных правонарушений.
2) Понятие и сущность преступлений в сфере компьютерной информации.
3) Состав и структура теоретических основ криминалистической методики расследования преступлений в сфере компьютерной информации (цифровой криминалистики).
4) Методические основы расследования преступлений в сфере компьютерной информации.
5) Состав, структура и особенности криминалистической характеристики преступлений в сфере компьютерной информации. Механизм следообразования при совершении преступлений в сфере компьютерной информации.
6) Характеристика личности преступников в сфере компьютерной информации.
7) Способы совершения преступлений в сфере компьютерной информации.
8) Основные ситуации первоначального этапа расследования преступлений в сфере компьютерной информации.
9) Формы и методы обучения: просмотр видеороликов и обсуждение в группе
10) Предварительное исследование компьютерных объектов при расследовании преступлений в сфере компьютерной информации.
11) Общие положения предварительного исследования объектов кибернетического пространства.
12) Обыск и выемка компьютерных объектов.
13) Особенности осмотра отдельных видов компьютерных объектов
14) Формы и методы обучения: просмотр видеороликов и обсуждение в группе
15) Получение и проверка вербальной информации, связанной с компьютерными объектами.
16) Допрос.
17) Следственный эксперимент.
18) Основные возможности компьютерно-технических экспертиз и тактические рекомендации по их назначению.

19) Уголовно-правовая характеристика преступлений в сфере компьютерной информации
20) Характеристика компьютерной информации.

21) Уголовно-правовая характеристика преступлений в сфере компьютерной информации.
22) Криминалистическая характеристика преступлений в сфере компьютерной информации
23) Формирование модели преступления в сфере компьютерной информации.
24) Исследование модели: построение типовых версий.
25) Проверка типичных версий при расследовании преступлений в сфере компьютерной информации.
26) Некоторые проблемы выявления преступлений в сфере компьютерной информации.
27) Проверка версий при расследовании преступлений в сфере компьютерной информации.
28) Особенности проведения отдельных следственных действий и тактических операций.

Основные вопросы:

1) Становление правоотношений в сфере компьютерной информации и криминализация компьютерных правонарушений.
2) Понятие и сущность преступлений в сфере компьютерной информации.
3) Состав и структура теоретических основ криминалистической методики расследования преступлений в сфере компьютерной информации (цифровой криминалистики).
4) Методические основы расследования преступлений в сфере компьютерной информации.
5) Состав, структура и особенности криминалистической характеристики преступлений в сфере компьютерной информации. Механизм следообразования при совершении преступлений в сфере компьютерной информации.
6) Характеристика личности преступников в сфере компьютерной информации.
7) Способы совершения преступлений в сфере компьютерной информации.
8) Основные ситуации первоначального этапа расследования преступлений в сфере компьютерной информации.
9) Формы и методы обучения: просмотр видеороликов и обсуждение в группе
10) Предварительное исследование компьютерных объектов при расследовании преступлений в сфере компьютерной информации.
11) Общие положения предварительного исследования объектов кибернетического пространства.
12) Обыск и выемка компьютерных объектов.
13) Особенности осмотра отдельных видов компьютерных объектов
14) Формы и методы обучения: просмотр видеороликов и обсуждение в группе
15) Получение и проверка вербальной информации, связанной с компьютерными объектами.
16) Допрос.
17) Следственный эксперимент.
18) Основные возможности компьютерно-технических экспертиз и тактические рекомендации по их назначению.

19) Уголовно-правовая характеристика преступлений в сфере компьютерной информации
20) Характеристика компьютерной информации.

21) Уголовно-правовая характеристика преступлений в сфере компьютерной информации.
22) Криминалистическая характеристика преступлений в сфере компьютерной информации
23) Формирование модели преступления в сфере компьютерной информации.
24) Исследование модели: построение типовых версий.
25) Проверка типичных версий при расследовании преступлений в сфере компьютерной информации.
26) Некоторые проблемы выявления преступлений в сфере компьютерной информации.
27) Проверка версий при расследовании преступлений в сфере компьютерной информации.
28) Особенности проведения отдельных следственных действий и тактических операций.

Ссылки на электронные и мультимедийные ресурсы

https://mvd.ru/upload/site119/folder_widepage/006/580/771/rassled_prest_komp/Lekt

Основы метоики расследования компьютерных преступлений.docx
https://api45o.ilovepdf.com/v1/download/7pbc9ntkl3ypjhygm8xb7lp0m9xvyszmb0kcrtl