МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра уголовного права

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«17» 01 2022 г.

ПРОТИВОДЕЙСТВИЕ ПОСЯГАТЕЛЬСТВАМ В УГОЛОВНО-ИСПОЛНИТЕЛЬНОЙ СИСТЕМЕ, СОВЕРШАЕМЫХ ПРИ ПОМОЩИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Методические указания для самостоятельной работы для студентов всех форм обучения специальности 40.05.02 Правоохранительная деятельность

Курск 2022

УДК 343.9.01

Составители: А.А. Гребеньков, М. И. Синяева, А.Б. Баумштейн

Рецензент
Доктор юридических наук, профессор С.В. Шевелева

Противодействие посягательствам в уголовно-исполнительной системе, совершаемых при помощи информационно-телекоммуникационных сетей: методические указания для самостоятельной работы для студентов всех форм обучения специальности 40.05.02 Правоохранительная деятельность / Юго-Зап. гос. ун-т.: сост. А.А. Гребеньков, М. И. Синяева, А.Б. Баумштейн. - Курск, 2022. - 54 с.

Методические рекомендации соответствуют Федеральному государственному образовательному стандарту по направлению подготовки 40.04.01.

Включают общие положения, широкий набор различных видов работы обучающихся при освоении дисциплины «Противодействие посягательствам в уголовно-исполнительной системе, совершаемых при помощи информационно-телекоммуникационных сетей»: содержание лекционных, практических занятий и самостоятельной работы студентов, формы контроля и требования к оценке знаний по дисциплине, список рекомендуемой литературы и информационное обеспечение дисциплины. Обеспечивают необходимые задания и критерии оценки, как для аудиторной, так и самостоятельной работы студентов, которая играет особую роль в подготовке специалистов.

Методические указания помогают сформировать студентам знания и навыки в области юриспруденции, развить у студентов перспективное мышление и творческие способности к исследовательской деятельности, усвоить необходимые компетенции, формируемые в результате изучения дисциплины «Противодействие посягательствам в уголовно-исполнительной системе, совершаемых при помощи информационно-телекоммуникационных сетей».

Предназначены для студентов всех форм обучения специальности 40.05.02.

Текст печатается в авторской редакции

Подписано в печать 17.01.2022 . Формат 60х84 1/16.
Усл. печ. л. 3,1 . Уч.-изд. л. 2,8 . Тираж 100 экз. Заказ 592. Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94

ОГЛАВЛЕНИЕ

1. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЕ ПОЛОЖЕНИЯ

1.1. Общие положения

Цель дисциплины. Подготовка выпускника, способного осуществлять деятельность, требующую углубленной фундаментальной и профессиональной подготовки, в том числе научно-исследовательскую работу, обладающего глубокими теоретическими знаниями и практическими навыками, касающимися особенностей квалификации преступлений, совершаемых с использованием новых информационных технологий и их криминологической характеристики, способного применять эти знания и навыки в рамках дальнейшей его практической деятельности.

Предмет дисциплины — изучение закономерностей возникновения, существования и изменения преступления и состава Противодействие посягательствам в уголовно-исполнительной системе, совершаемых при помощи информационно-телекоммуникационных сетей как явления социальной жизни любого общества.

Основные задача дисциплины:

— обучение студента навыкам обоснования и принятия решений, а также совершения действий, связанных с реализацией уголовно-правовых норм в сфере противодействия посягательств, совершаемым при помощи информационно-телекоммуникационных сетей;

— овладение необходимыми для успешной профилактики, предупреждения, выявления, пресечения преступлений, совершаемым при помощи информационно-телекоммуникационных сетей, знаниями норм и правовых институтов;

— обучение студента самостоятельной работе над нормативными актами, научной и учебной литературой, необходимой для сбора, анализа и оценки информации, имеющей значение для реализации правовых норм в сфере правоохранительной деятельности;

— формирование навыков проведения прикладных научных исследований в сфере противодействия посягательствам, совершаемым при помощи информационно-телекоммуникационных сетей;

— овладение умением критически анализировать действующее законодательство; обобщать следственную и судебную практику

применения законодательства в сфере противодействия посягательств, совершаемым при помощи информационно-телекоммуникационных сетей;

— овладение методикой пополнения и закрепления правовых знаний и умений в сфере противодействия посягательствам, совершаемым при помощи информационно-телекоммуникационных сетей на практике;

— сформировать понимание методологических основ и специфики методов, используемых в уголовно-правовой и криминологической теории, а также информационном праве в связи с проблематикой преступлений, совершаемых при помощи информационно-телекоммуникационных сетей.

Перечень компетенций, которые формирует дисциплина

ПК-3.2

Осуществляет мероприятия по пресечению преступлений и правонарушений на режимной территории исправительных учреждений

ПК-7.3

Применяет меры профилактического, воспитательного и иного воздействия, направленные на профилактику правонарушений и преступлений в отношении лиц, отбывающих уголовные наказания

ПК-8.2

Пресекает угрозы, возникающие в пенитенциарных правоотношениях

В результате изучения данного курса студенты должны:

Знать:

- нормы уголовного права, касающиеся преступлений, совершаемых при помощи ИТС, криминологические особенности преступлений, совершаемых при помощи ИТС, необходимые для пресечения преступлений на режимной территории ИУ
- нормы уголовного права, касающиеся преступлений, совершаемых при помощи ИТС, криминологические особенности преступлений, совершаемых при помощи ИТС, необходимые для профилактики преступлений в отношении лиц, отбывающих уголовные наказания
- основные угрозы, связанные с преступлениями, совершаемыми при помощи ИТС, возникающие в пенитенциарных правоотношениях

Уметь:

- пресекать преступления, совершаемые при помощи ИТС, на режимной территории ИУ
- предупреждать преступления, совершаемые при помощи ИТС, в отношении лиц, отбывающих уголовные наказания
- выявлять угрозы, связанные с преступлениями, совершаемыми при помощи ИТС, возникающие в пенитенциарных правоотношениях

Владеть:

- навыками осуществления мероприятий по пресечению преступлений, совершаемых при помощи ИТС, на режимной территории ИУ
- навыками применения мер профилактического, воспитательного и иного воздействия для предупреждения преступлений, совершаемых при помощи ИТС
- навыками пресечения угроз, связанных с преступлениями, совершаемыми при помощи ИТС, возникающих в пенитенциарных правоотношениях

1.2. Объем дисциплины и виды учебной работы

Объем дисциплины и виды учебной работы определены учебным планом специальности 40.05.02 Правоохранительная деятельность, утвержденного Ученым советом университета «25» июня 2021 г., протокол №9.

Распределение часов по темам лекционных (практических, семинарских, лабораторных) занятий и самостоятельной работы студентов представлено в таблице 1 и таблице 2.

Таблица 1 – Содержание дисциплины и её трудоёмкость (для очной формы обучения)

№ п/п	Наименование темы	Вид проводимого занятия			СРС
		Лк	Лр	Пр	
1	Понятие и общая характеристика преступлений, связанных с использованием ИТС.	4	0	8	16
2	Общая характеристика компьютерных преступлений	2	0	4	8
3	Неправомерный доступ к компьютерной информации	2	0	4	8

4	Создание, использование и распространение вредоносных компьютерных программ	2	0	4	8
5	Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и ИТС и посягательства на критическую информационную инфраструктуру	2	0	4	8
6	Хищения с использованием новых информационных технологий	6	0	12	23,9
7	Преступления против личности, совершаемые с применением информационных технологий	2	0	2	7
8	Преступления против здоровья населения и общественной нравственности, совершаемые с применением информационных технологий	4	0	4	14
9	Преступления против конституционного строя и безопасности государства, совершаемые с применением информационных технологий	2	0	2	7
10	Преступления против общественной безопасности, совершаемые с применением информационных технологий	4	0	4	14
11	Частные вопросы организации деятельности сотрудников УИС по пресечению угроз и преступлений, связанных с использованием ИТС	2	0	2	7
12	Частные вопросы организации деятельности сотрудников УИС по профилактике преступлений, связанных с использованием ИТС	4	0	4	12,85
	Итого	36	0	54	133,75
Форма контроля		зачет, экзамен			
ВСЕГО по дисциплине		252 часов / 7 ЗЕ			

Таблица 2 – Содержание дисциплины и её трудоёмкость (для заочной формы обучения)

№ п/п	Наименование темы	Вид проводимого занятия			СРС
		Лк	Лр	Пр	
1	Понятие и общая характеристика преступлений, связанных с использованием ИТС.	1	0	1	22,78
2	Общая характеристика компьютерных преступлений	1	0	1	18
3	Неправомерный доступ к компьютерной информации	1	0	1	18

4	Создание, использование и распространение вредоносных компьютерных программ	1	0	1	18
5	Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и ИТС и посягательства на критическую информационную инфраструктуру	1	0	1	18
6	Хищения с использованием новых информационных технологий	1	0	1	18
7	Преступления против личности, совершаемые с применением информационных технологий	0	0	1	18
8	Преступления против здоровья населения и общественной нравственности, совершаемые с применением информационных технологий	0	0	1	18
9	Преступления против конституционного строя и безопасности государства, совершаемые с применением информационных технологий	0	0	1	18
10	Преступления против общественной безопасности, совершаемые с применением информационных технологий	0	0	1	18
11	Частные вопросы организации деятельности сотрудников УИС по пресечению угроз и преступлений, связанных с использованием ИТС	0	0	1	18
12	Частные вопросы организации деятельности сотрудников УИС по профилактике преступлений, связанных с использованием ИТС	0	0	1	18
	Итого	6	0	12	220,78
Форма контроля		зачет, экзамен			
ВСЕГО по дисциплине		252 часов / 7 ЗЕ			

1.3. Методические рекомендации по организации изучения дисциплины

В рамках изучения дисциплины «Противодействие посягательствам в уголовно-исполнительной системе, совершаемых при помощи информационно-телекоммуникационных сетей» работа студентов организуется в следующих формах:

- *работа с конспектом лекций и дополнительной литературой по темам курса;*
- *работа с раздаточным материалом – «Скрин-шот»;*

- *изучение вопросов, выносимых за рамки лекционных занятий (дискуссионные вопросы для дополнительного изучения);*
- *подготовка к практическому занятию;*
- *выполнение групповых и индивидуальных домашних заданий, в том числе:*

– *проведение собеседования по теме лекции;*

– *подготовка краткого доклада (резюме, эссе) по теме практического занятия и разработка мультимедийной презентации к нему;*

– *выполнение практических заданий (решение задач, выполнение расчетных и лабораторных работ);*

– *подготовка к тестированию;*

- *самоконтроль.*

Рекомендуемый ниже режим самостоятельной работы позволит студентам глубоко разобраться во всех изучаемых вопросах, активно участвовать в дискуссиях на семинарских занятиях и в итоге успешно сдать зачет (экзамен).

1. *Лекция* является фундаментальным источником знаний и должна способствовать глубокому усвоению материала, активизировать интерес студента к изучаемой дисциплине.

На лекции излагаются только основные, наиболее важные положения изучаемой темы. Одной только лекции недостаточно для успешного ответа на практическом занятии.

Работу с конспектом лекций целесообразно проводить непосредственно после её прослушивания. Она предполагает перечитывание конспекта, внесение в него, по необходимости, уточнений, дополнений, разъяснений и изменений. Ознакомление с дополнительной литературой по теме, проведение обзора мнений других ученных по изучаемой теме. Необходимым является глубокое освоение содержания лекции и свободное владение им, в том числе использованной в ней терминологии (понятий), категорий и законов. Студенту рекомендуется не ограничиваться при изучении темы только конспектом лекций или одним учебником; необходимо не только конспектировать лекции, но и читать дополнительную литературу, изучать методические рекомендации, издаваемые кафедрой.

2. *«Скрин-шот»* - специальный раздаточный материал, подготовленный преподавателем, который предназначен для повышения эффективности учебного процесса за счет:

- привлечения дополнительного внимания студента на наиболее важных и сложных проблемах курса;

- освобождения от необходимости ведения рутинных записей по ходу лекции и возможности более адекватной фиксации ключевых положений лекции;

- представления всего необходимого иллюстративного и справочно-информационного материала по теме лекции;

- более глубокой переработки материалов курса при подготовке к зачету или экзамену.

Самостоятельная работа с раздаточным материалом «*Скрин-шот»* может проводиться вместо работы с конспектом лекций, если композиция каждой страницы материала построена лектором таким образом, что достаточно свободного места для конспектирования материалов лекции, комментариев и выражения собственных мыслей студента по материалам услышанного или прочитанного.

В случае, когда студенты ведут отдельные конспекты лекций, работа с раздаточным материалом «*Скрин-шот»* проводится вместе с работой с конспектом лекций по каждой теме.

3. В связи с большим объемом изучаемого материала, интересом, который он представляет для современного образованного человека, некоторые вопросы выносятся за рамки лекций. Это предусмотрено рабочим учебным планом подготовки студентов. *Изучение вопросов, выносимых за рамки лекционных занятий* (дискуссионных вопросов), предполагает самостоятельное изучение студентами дополнительной литературы и её конспектирование по этим вопросам.

4. По каждой теме, выносимой на практические занятия, даётся примерный план её изучения (вопросы, на которые следует подготовиться к занятию). В ходе *практических занятий* проводится разъяснение теоретических положений курса, уточнения междисциплинарных связей.

Подготовка к практическому занятию предполагает большую самостоятельную работу и включает в себя:

- Знакомство с планом практического занятия и подбор материала к нему по указанным источникам (конспект лекции, основная, справочная и дополнительная литература, электронные и Интернет-ресурсы).
- Запоминание подобранного по плану материала.
- Освоение терминов, перечисленных в глоссарии.

- Ответы на вопросы, приведенные к каждой теме.
- Обдумывание вопросов для обсуждения. Выдвижение собственных вариантов ответа.
- Выполнение заданий преподавателя (подготовка рефератов, тесты, контрольные работы, консультации, самостоятельная работа).
- Подготовка (выборочно) индивидуальных заданий.

Задания, приведенные в планах занятий, выполняются всеми студентами в обязательном порядке.

5. В*ыполнение групповых и индивидуальных домашних заданий* является обязательной формой самостоятельной работы студентов. Целесообразно к каждому занятию, выбрав из изучаемой темы наиболее проблемные и спорные вопросы, заблаговременно поручить подготовку по ним докладов одному или двум студентам. Продолжительность доклада — не более 5-7 минут. Такая форма работы приучает студентов не только к самостоятельной работе с источниками, но и к публичным выступлениям.

По дисциплинам предполагается подготовка индивидуальных или групповых (на усмотрение преподавателя) *докладов (сообщений, рефератов, эссе, творческих заданий)* на практических занятиях и разработку мультимедийной презентации к нему.

Доклад — продукт самостоятельной работы студента, представляющий собой публичное выступление по представлению полученных результатов решения определенной учебно-практической, учебно-исследовательской или научной темы.

Эссе — средство, позволяющее оценить умение обучающегося письменно излагать суть поставленной проблемы, самостоятельно проводить анализ проблемы с использованием концепций и аналитического инструментария соответствующей дисциплины, делать выводы, обобщающие авторскую позицию по поставленной проблеме.

Реферат — продукт самостоятельной работы студента, представляющий собой краткое изложение в письменном виде полученных результатов теоретического анализа определенной научной (учебно-исследовательской) темы, где автор раскрывает суть исследуемой проблемы, приводит различные точки зрения, а также собственные взгляды на нее, приводит список используемых источников.

Творческое задание — частично регламентированное задание, имеющее нестандартное решение и позволяющее диагностировать

умения, интегрировать знания различных областей, аргументировать собственную точку зрения. Может выполняться в индивидуальном порядке или группой обучающихся.

Преподаватель сам формирует задание или студенты имеют возможность самостоятельно выбрать одну из предполагаемых преподавателем тем и выступить на семинарском занятии. Доклад (резюме, эссе и т.д.) как форма самостоятельной учебной деятельности студентов представляет собой рассуждение на определенную тему на основе обзора нескольких источников в целях доказательства или опровержения какого-либо тезиса. Информация источников используется для аргументации, иллюстрации и т.д. своих мыслей. Цель написания такого рассуждения не дублирование имеющейся литературы на эту тему, а подготовка студентов к проведению собственного научного исследования, к правильному оформлению его описания в соответствии с требованиями.

Работа студентов по подготовке доклада (сообщения, рефератов, эссе, творческих заданий) заключается в следующем:

- подбор научной литературы по выбранной теме;
- работа с литературой, отбор информации, которая соответствует теме и помогает доказать тезисы;
- анализ проблемы, фактов, явлений;
- систематизация и обобщение данных, формулировка выводов;
- оценка теоретического и практического значения рассматриваемой проблемы;
- аргументация своего мнения, оценок, выводов, предложений;
- выстраивание логики изложения;
- указание источников информации, авторов излагаемых точек зрения;
- правильное оформление работы (ссылки, список использованной литературы, рисунки, таблицы) по стандарту.

Самостоятельность студента при подготовке доклада (сообщение, эссе) проявляется в выборе темы, ракурса её рассмотрения, источников для раскрытия темы, тезисов, аргументов для их доказательства, конкретной информации из источников, способа структурирования и обобщения информации, структуры изложения, а также в обосновании выбора темы, в оценке её актуальности, практического и теоретического значения, в выводах.

Выступление с докладом (резюме, эссе) на семинаре не должно превышать 7-10 минут. После устного выступления автор отвечает на вопросы аудитории (студентов, преподавателя) по теме и содержанию своего выступления.

Цель и задачи данного вида самостоятельной работы студентов определяют требования, предъявляемые к докладу (резюме, эссе), и критерии его оценки: 1) логическая последовательность изложения; 2) аргументированность оценок и выводов, доказанность тезиса; 3) ясность и простота изложения мыслей (отсутствие многословия и излишнего наукообразия); 4) самостоятельность изложения материала источников; 5) корректное указание в тексте доклада источников информации, авторов проводимых точек зрения; 6) стилистическая правильность и выразительность (выбор языковых средств, соответствующих научному стилю речи); 7) уместное использование иллюстративных средств (цитат, сносок, рисунков, таблиц, слайдов).

Изложение материалов доклада может сопровождаться *мультимедийной презентацией*. Разработка мультимедийной презентации выполняется по требованию преподавателя или по желанию студента.

Презентация должна быть выполнена в программе Power Point или аналогичных и включать такое количество слайдов, какое необходимо для иллюстрирования материала доклада в полном объеме.

Основные методические требования, предъявляемые к презентации:

- логичность представления с согласованность текстового и визуального материала;
- соответствие содержания презентации выбранной теме и выбранного принципа изложения / рубрикации информации (хронологический, классификационный, функционально-целевой и др.).
- соразмерность (необходимая и достаточная пропорциональность) текста и визуального ряда на каждом слайде (не менее 50% - 50%, или на 10-20% более в сторону визуального ряда).
- комфортность восприятия с экрана (цвет фона; размер и четкость шрифта).

- эстетичность оформления (внутреннее единство используемых шаблонов предъявления информации; упорядоченность и выразительность графических и изобразительных элементов).
- допускается наличие анимационных и звуковых эффектов.

Оценка доклада (резюме, эссе) производится в рамках действующей в ЮЗГУ балльно - рейтинговой оценки успеваемости и качества знаний студентов. Итоговая оценка является суммой баллов, выставляемых преподавателем с учетом мнения других студентов по каждому из перечисленных выше методических требований к докладу и презентации.

Также формой самостоятельной работы студентов является *выполнение практических заданий (решения задач, оформление отчетов о самостоятельной работе*), содержание которых определяется содержанием настоящих методических указаний. Часть практических заданий может быть выполнена студентами на аудиторных практических занятиях под руководством преподавателя. После того, как преподавателем объявлено, что рассмотрение данной темы на аудиторных занятиях завершено, студент переходит к самостоятельному выполнению практических заданий, пользуясь настоящими методическими указаниями, конспектом лекций по соответствующей теме, записями, сделанными на практических занятиях, дополнительной литературой по теме. Все практические задания для самостоятельного выполнения студентами, приведенные в настоящих методических указаниях обязательны для выполнения в полном объеме.

5. Подготовка к тестированию предусматривает повторение лекционного материала и основных терминов, а также самостоятельное выполнение заданий в тестовой форме, приведенных в настоящих методических указаниях.

Тестовый подход, при всех его общеизвестных недостатках, также следует использовать при проведении практических занятий. Перед тем, как предложить тесты студентам, преподавателю следует самому внимательно их проверить, уточнив, остались ли вопросы и ответы корректны в связи с регулярными изменениями в законодательстве.

6. *Самоконтроль* является обязательным элементом самостоятельной работы студента по дисциплинам. Он позволяет

формировать умения самостоятельно контролировать и адекватно оценивать результаты своей учебной деятельности и на этой основе управлять процессом овладения знаниями. Овладение умениями самоконтроля формирует навыки планирования учебного труда, способствует углублению внимания, памяти и выступает как важный фактор развития познавательных способностей.

Самоконтроль включает:

1. Ответ на вопросы для самоконтроля для самоанализа глубины и прочности знаний и умений по дисциплине.

2. Критическую оценку результатов своей познавательной деятельности.

Самоконтроль учит ценить свое время, позволяет вовремя заменить и исправлять свои ошибки.

Формы самоконтроля могут быть следующими:

- *устный пересказ текста лекции и сравнение его с содержанием конспекта лекции;*
- *ответ на вопросы, приведенные к каждой теме (см. раздел 2 настоящих методических указаний);*
- *составление плана, тезисов, формулировок ключевых положений текста по памяти;*
- *ответы на вопросы и выполнение заданий для самопроверки (настоящие методические указания предполагают вопросы для самоконтроля по каждой изучаемой теме);*
- *самостоятельное тестирование по предложенным в настоящих методических указаниях тестовых заданий.*

Самоконтроль учебной деятельности позволяет студенту оценивать эффективность и рациональность применяемых методов и форм умственного труда, находить допускаемые недочеты и на этой основе проводить необходимую коррекцию своей познавательной деятельности.

Наконец, желательна периодическая проверка остаточных знаний по предыдущим темам, которую можно провести в форме контрольной работы.

При возникновении сложностей по усвоению программного материала необходимо посещать консультации по дисциплине, задавать уточняющие вопросы на лекциях и практических занятиях, уделять время самостоятельной подготовке (часы на самостоятельное изучение), осуществлять все формы самоконтроля.

1.4. Формы контроля знаний

1.4.1. Текущий контроль изучения дисциплины

Текущий контроль изучения дисциплины осуществляется на основе балльно-рейтинговой системы (БРС) контроля оценки знаний в соответствии со следующими этапами:

1. Студент очной формы обучения на каждой контрольной точке может получить максимально 16 баллов (из них: 4 балла – за посещаемость, 12 баллов – за успеваемость).

2. Студент заочной формы обучения может получить максимально 50 баллов (из них: 14 баллов – за посещаемость, 36 баллов – за успеваемость).

1.4.2. Текущий контроль

Текущий контроль изучения дисциплины осуществляется с помощью экзамена. Контрольно-измерительные материалы к экзамену утверждаются зав. кафедрой.

В результате освоения дисциплины студент получает оценку в соответствии с набранными в сумме баллами (таблица 3).

Таблица 3 – Соответствие баллов оценке

Оценка	Неудовлетворительно	Удовлетворительно	Хорошо	Отлично
Набранная сумма баллов	менее 50	50-69	70-84	85-100

Оценка	Не зачтено	Зачтено
Набранная сумма баллов	менее 50	50-100

Для промежуточной аттестации студентов очно формы обучения, проводимой в форме тестирования, используется следующая методика оценивания знаний, умений, навыков и (или) опыта деятельности. В каждом варианте КИМ - 16 заданий (15 вопросов и одна задача).

Каждый верный ответ оценивается следующим образом:

- задание в закрытой форме – 2 балла,
- задание в открытой форме – 2 балла,
- задание на установление правильной последовательности – 2 балла,
- задание на установление соответствия – 2 балла,
- решение задачи – 6 баллов.

Максимальное количество баллов за тестирование - 36 баллов.

Для промежуточной аттестации студентов заочной формы обучения, проводимой в форме тестирования, используется следующая методика оценивания знаний, умений, навыков и (или)

опыта деятельности. В каждом варианте КИМ - 16 заданий (15 вопросов и одна задача).

Каждый верный ответ оценивается следующим образом:

- задание в закрытой форме – 3 балла,
- задание в открытой форме – 3 балла,
- задание на установление правильной последовательности – 3 балла,
- задание на установление соответствия – 3 балла,
- решение задачи – 15 баллов.

Максимальное количество баллов за тестирование –60 баллов.

ПЛАНЫ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

ТЕМА 1. ПОНЯТИЕ И ОБЩАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С ИСПОЛЬЗОВАНИЕМ ИТС

Глоссарий

Киберпреступность — общее наименование компьютерных правонарушений (взломы файлов, похищение секретов и денег со счетов банков), а также компьютерное хулиганство (введение вирусов и т.п.).

Хакер — лицо, совершающее различного рода незаконные действия в сфере информатики: несанкционированное проникновение в чужие компьютерные сети и получение из них информации; незаконные снятие защиты с программных продуктов и их копирование и т.д.

Высокие технологии — технологии, развивающиеся в ходе НТР. К ним обычно относят: информатику, программное обеспечение, искусственный интеллект, робототехнику, телекоммуникации, биотехнологию.

Преступность — в криминологии и правовой статистике совокупность всех фактически совершенных противоправных деяний, за каждое из которых предусмотрено уголовное наказание, как массовое явление.

Личность преступника — основывающаяся на структуре основных сущностных свойств и черт преступника совокупность интеллектуально духовных качеств, его психического и физического состояния.

Структура (план)

1.1. Сфера высоких технологий и ИТС и её значение для современного мира.
1.2. Виды преступлений в сфере высоких технологий и использования ИТС.
1.3. Типовые особенности личности преступника.
1.4. Общественная опасность преступлений в сфере высоких технологий и использования ИТС.

1.5. Ознакомление студентов с процедурой проведения текущего контроля по дисциплине.

Практическое занятие

В ходе практического занятия рассматриваются следующие вопросы: сфера высоких технологий и её значение для современного мира. Виды преступлений в сфере высоких технологий. Типовые особенности личности преступника. Общественная опасность преступлений в сфере высоких технологий. Ознакомление студентов с процедурой проведения текущего контроля по дисциплине. Понятия «информация» и «компьютерная информация». Общие принципы информационной безопасности и защиты компьютерной информации в Российской Федерации. Объект преступлений в сфере компьютерной информации

Вопросы для самоконтроля

Чем обусловлена актуальность изучения преступности в сфере высоких технологий в современный период?
Какие виды преступности относятся к высокотехнологичным?
Каково состояние киберпреступности и перспективы борьбы с ней?
В чём отличие распространённых представлений о личности киберпреступников от реальной действительности?
Чем обусловлено вовлечение в киберпреступность всё большего числа граждан?
Какие основные акты в сфере борьбы с преступностью технологий были приняты мировым сообществом?
Применяются ли эти акты в России?
Какие акты национального законодательства содержат нормы, направленные на борьбу с киберпреступностью?
Каковы основные признаки информации?
В чём отличие информации от материи и энергии?

Кейс-задачи для обсуждения

Житель Челябинска Андрисов создал компьютерную программу, которая производила автоматическую отсылку СМС-сообщений на сотовые телефоны. Чтобы скомпрометировать одну сотовую

компанию, он запустил программу с одного из серверов Санкт-Петербурга. В результате более 16 тыс. человек получили на сотовые телефоны послания нецензурного содержания. Проведите юридический анализ изложенной выше ситуации. Есть ли здесь признаки какого-либо посягательства, совершаемого при помощи информационно-телекоммуникационных сетей?

Незадолго до выборов в Государственную Думу Федерального Собрания РФ в Интернете помимо официального веб-сайта руководителя одной из политических партий Дюгалова появился «паразитический» сайт с аналогичным названием, на котором образ этого политического лидера выглядел совсем не престижно. Например, на главной странице сайта Дюгалов был изображен в бюстгальтере. Сайт содержал ненормативную лексику и пошлые карикатуры на Дюгалова. После выборов сайт перестал функционировать. Впоследствии выяснилось, что сайт был создан Бломбергом, Волкаевым и Жадовым, которые были наняты Кроминым и Серегиным, членами избирательного штаба политического оппонента Дюгалова. Проведите юридический анализ изложенной выше ситуации. Есть ли здесь признаки какого-либо посягательства, совершаемого при помощи информационно-телекоммуникационных сетей?

Темы рефератов и докладов

Социально-культурологический портрет «хакера»
Международно-правовое регулирование борьбы с киберпреступностью
История российского законодательства о борьбе с киберпреступностью

ТЕМА 2. ОБЩАЯ ХАРАКТЕРИСТИКА КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

Глоссарий

Компьютерная информация — сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи

Информация — любые сведения, данные, сообщения,

передаваемые посредством сигналов

Информационная безопасность — состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

Защита информации — совокупность методов и средств, обеспечивающих целостность, конфиденциальность, достоверность, аутентичность и доступность информации в условиях воздействия на нее угроз естественного или искусственного характера.

Объект преступления — уголовно-правовая категория, которая используется для обозначения общественных институтов, которым причиняется ущерб вследствие совершения преступления.

Структура (план)

1.1. Понятия «информация» и «компьютерная информация».
1.2. Общие принципы информационной безопасности и защиты компьютерной информации в Российской Федерации.
1.3. Объект преступлений в сфере компьютерной информации

Практическое занятие

В ходе практического занятия рассматриваются следующие вопросы: понятия «информация» и «компьютерная информация». Общие принципы информационной безопасности и защиты компьютерной информации в Российской Федерации. Объект преступлений в сфере компьютерной информации

Вопросы для самоконтроля

Каковы основные признаки компьютерной информации?
Что такое архитектура фон Неймана?
Какие права, связанные с информацией, закрепляются в Конституции РФ?
Какие права имеет обладатель информации?
Какие обязанности имеет обладатель информации?
Что такое «конфиденциальность информации»?
Какими видами мер обеспечивается информационная безопасность?

Каков родовой и видовой объект компьютерных преступлений?

Кейс-задачи для обсуждения

В период с июня по декабрь 2012 г. руководитель малого предприятия Паршин совместно с кассиром Кондратьевой, действуя с единым умыслом, направленным на сокрытие доходов от налогообложения, ежедневно с 17 до 19 ч в торговых палатках предприятия подключали в гнезда двух контрольно-кассовых аппаратов специально изготовленный самодельный прибор, уничтожали информацию о проведенных в течение текущей смены финансовых операциях и вносили измененные данные о сумме выручки. Есть ли здесь признаки какого-либо компьютерного преступления?

14-летний Сонин провел в компьютерном клубе 12 часов. Когда он пришел домой, ему стало плохо. Вызвали скорую помощь, отвезли его в больницу, где он провел в реанимации семь дней. Усилия врачей оказались тщетны — ребенок умер. Установленная причина смерти — острое нарушение мозгового кровообращения — инсульт. По мнению врачей, у Сонина произошла декомпенсаторная реакция на фоне переутомления, а мерцание компьютерного экрана в темной комнате спровоцировало именно такую реакцию головного мозга. Есть ли здесь признаки какого-либо компьютерного преступления? Есть ли основания для привлечения к ответственности владельцев компьютерного клуба? Должны ли нести уголовную ответственность родители мальчика?

Темы рефератов и докладов

История российского законодательства об информационном обороте и информационной безопасности

Доктрина информационной безопасности РФ

Основные стандарты обеспечения информационной безопасности

ТЕМА 3. НЕПРАВОМЕРНЫЙ ДОСТУП К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Глоссарий

Неправомерный доступ к компьютерной информации — незаконное либо не разрешенное собственником или иным ее законным владельцем использование возможности получения информации.

Уничтожение информации — любое условие, делающее информацию непригодной для использования независимо от причины

Модификация информации — обнаруженное или необнаруженное несанкционированное или случайное изменение информации

Блокирование информации — действия, в результате которых информация становится недоступна для субъекта, имеющего право доступа к ней

Копирование информации — воспроизведение информации (данных) с сохранением исходного состояния, при этом физическая форма копии может отличаться от исходной

Структура (план)

1.1. Уголовно-правовая характеристика неправомерного доступа к компьютерной информации.
1.2. Способы совершения неправомерного доступа к компьютерной информации.
1.3. Криминологическая характеристика неправомерного доступа к компьютерной информации.

Практическое занятие

В ходе практического занятия рассматриваются следующие вопросы: уголовно-правовая характеристика неправомерного доступа к компьютерной информации. Способы совершения неправомерного доступа к компьютерной информации. Криминологическая характеристика неправомерного доступа к компьютерной информации.

Вопросы для самоконтроля

Каковы основные признаки компьютерной информации?

В каком случае доступ к информации будет считаться неправомерным?
Является ли удаление файла в компьютере удалением информации?
В чём отличие модификации и уничтожения информации?
Происходит ли копирование информации при ознакомлении с ней?
Что такое крупный ущерб и тяжкие последствия в контексте ст. 272 УК РФ?
Что подразумевается под использованием служебного положения?
Каковы основные способы неправомерного доступа к информации?

Кейс-задачи для обсуждения

Сотрудники отдела «К» УВД г. Энска А. и З. для повышения показателей раскрываемости компьютерных преступлений решили провести «оперативный эксперимент». Найдя в газете бесплатных объявлений объявление об оказании услуг «компьютерной помощи», они позвонили давшему его Р. и попросили его оказать помощь в установке на компьютер программного продукта Autodesk Alias Surface 2016 (стоимость лицензии на который составляла 1 млн. 145 тыс. рублей). Поначалу Р. отказался, однако после повторных звонков и обещания дополнительного вознаграждения всё же согласился. Требуемую программу он скачал из Интернета, там же он нашёл средства, позволяющие обойти технические ограничения, связанные с защитой авторских прав. Для установки программы был подготовлен компьютер, содержащий «чистую» ОС Windows. После того, как Р. закончил установку и «взломал» программу, оперативники задержали его. Р. было предъявлено обвинение в покушении на совершение нарушения авторских и смежных прав в особо крупном размере, неправомерный доступ к компьютерной информации, совершённый из корыстной заинтересованности и причинивший крупный ущерб, а также в использовании вредоносных компьютерных программ, предназначенных для нейтрализации средств защиты компьютерной информации, совершённое из корыстной заинтересованности и причинивший крупный ущерб. Правильна ли такая квалификация? Правомерны ли действия оперативников?
Заключив пари, Савин, используя свой компьютер, сумел подключиться к сети Минобороны России, скопировал информацию о связях этого ведомства с комитетами солдатских матерей и

изменил пароль для получения доступа к данной информации сотрудников министерства. Совершено ли Савиным преступление? Обоснуйте свой ответ. Следует ли рассматривать содеянное им в качестве деяния, предусмотренного ст. 272 УК?

Темы рефератов и докладов

Основные методы защиты от неправомерного доступа
Личность преступника, совершающего неправомерный доступ к компьютерной информации.
Понятие «компьютерная информация»

ТЕМА 4. СОЗДАНИЕ, ИСПОЛЬЗОВАНИЕ И РАСПРОСТРАНЕНИЕ ВРЕДОНОСНЫХ КОМПЬЮТЕРНЫХ ПРОГРАММ

Глоссарий

Вредоносная программа — программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных

Компьютерный вирус — фрагмент исполняемого кода, который копирует себя в другую программу (главную программу), модифицируя ее при этом

Иная вредоносная компьютерная информация — иная информация, которая при вводе в информационную систему способна осуществить несанкционированные уничтожение, блокирование, модификацию, копирование компьютерной информации или нейтрализацию средств защиты компьютерной информации.

Использование вредоносной программы — это работа с программой, применение ее по назначению и иные действия по введению ее в хозяйственный оборот в изначальной или модифицированной форме, при котором активизируются их вредные свойства.

Нейтрализация средств защиты информации — приведение их в нерабочее состояние, например отключение антивирусного программного обеспечения, системы обнаружения вторжения или

системы шифрования, межсетевого фильтра.

Структура (план)

1.1. Уголовно-правовая характеристика создания, использования и распространения вредоносных компьютерных программ.
1.2. Способы совершения создания, использования и распространения вредоносных компьютерных программ.
1.3. Криминологическая характеристика создания, использования и распространения вредоносных компьютерных программ.

Практическое занятие

В ходе практического занятия рассматриваются следующие вопросы: уголовно-правовая характеристика создания, использования и распространения вредоносных компьютерных программ. Способы совершения создания, использования и распространения вредоносных компьютерных программ. Криминологическая характеристика создания, использования и распространения вредоносных компьютерных программ.

Вопросы для самоконтроля

Чем вредоносная программа отличается от обычной?
Как следует оценивать создание программ, которые могут использоваться как в полезных, так и во вредоносных целях?
Какие основные типы вредоносных программ распространены в настоящее время?
Может ли быть привлечён к ответственности программист, ошибочно включивший в программу функции, которые могут привести к потере данных пользователя?
Какие обстоятельства влияют на размер ответственности по данной статье?
Как следует расценивать разработку и распространение программ, позволяющих осуществлять незаконное копирование объектов авторского права?

Кейс-задачи для обсуждения

Специалисту по ЭВМ Коновалову была поручена разработка программы поиска необходимой информации. После ее установки была блокирована локальная сеть ЭВМ организации и частично уничтожена информация, вследствие того, что новая программа содержала «троянского коня». Коновалов заявил, что он сделал это специально, потому что хотел отомстить директору организации за то, что тот встречался с его женой. Организация потерпела огромные убытки, так как пришлось восстанавливать информацию, которую накапливали годами.

АО «Окно» разработало и продавало компьютерную игру. При установке игры на компьютер некоторые стандартные драйверы устройств заменялись на драйверы, разработанные АО «Окно», в результате была нарушена нормальная работа нескольких тысяч компьютеров. При установке программа тестировала компьютерное оборудование и программное обеспечение пользователя, сведения о которых при регистрации с помощью модема сообщались в АО «Окно». В документации к игре не сообщалось об этом. Квалифицируйте содеянное.

Темы рефератов и докладов

История вредоносных программ.
Ботнеты.
Вредоносные программы как средство информационной войны.
DDoS-атаки и уголовно-правовое противодействие им

ТЕМА 5. НАРУШЕНИЕ ПРАВИЛ ЭКСПЛУАТАЦИИ СРЕДСТВ ХРАНЕНИЯ, ОБРАБОТКИ ИЛИ ПЕРЕДАЧИ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ И ИТС И ПОСЯГАТЕЛЬСТВА НА КРИТИЧЕСКУЮ ИНФОРМАЦИОННУЮ ИНФРАСТРУКТУРУ

Глоссарий

Информационно-телекоммуникационная сеть — технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с

использованием средств вычислительной техники

Хранение информации — процесс передачи информации во времени, связанный с обеспечением неизменности состояний материального носителя информации

Обработка информации — любое преобразование информации из одного вида в другой, производимое по строгим формальным правилам.

Передача информации — процесс переноса информации (данных) от ее источника к потребителю

Правила эксплуатации — содержатся в различных положениях, инструкциях, уставах, приказах, ГОСТах, проектной документации на соответствующую автоматизированную информационную систему, договорах, соглашениях и иных официальных документах.

Структура (план)

1.1. Уголовно-правовая характеристика нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.
1.2. Криминологическая характеристика нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.
1.3. Перспективы совершенствования нормы об ответственности за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и ИТС.
1.4. Уголовно-правовая и криминологическая характеристика посягательств на критическую информационную инфраструктуру.

Практическое занятие

В ходе практического занятия рассматриваются следующие вопросы: уголовно-правовая характеристика нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-

телекоммуникационных сетей. Криминологическая характеристика нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей. Перспективы совершенствования нормы об ответственности за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и ИТС. Уголовно-правовая и криминологическая характеристика посягательств на критическую информационную инфраструктуру.

Вопросы для самоконтроля

Какие нормативные акты предусматривают специальные правила безопасной эксплуатации компьютерной техники и информационных сетей?
Охватываются ли составом данного преступления атаки типа «отказ в обслуживании» (DoS)?
Охватывается ли составом данного преступления неустановка системным администратором антивируса на компьютеры предприятия?
Кто является субъектом данного преступления?
Какова форма вины в данном преступлении?
Может ли наступать уголовная ответственность по данной статье за нарушение условий лицензионного договора?

Кейс-задачи для обсуждения

На сборочном конвейере Волжского автомобильного завода программист из мести руководству организации внес изменения в программу ЭВМ, управляющей подачей деталей на конвейер. В результате сбоя работы конвейера, который останавливался при подаче на него определенного числа деталей, заводу был причинен ущерб в виде 200 невыпущенных автомобилей в смену.
Индивидуальный предприниматель Гончаров из корыстных побуждений отключил в рабочее время в офисе своего конкурента Борисова электричество, что привело к уничтожению деловой информации, обрабатываемой в это время в сети ЭВМ фирмы, и причинило Борисову значительный материальный ущерб.

Темы рефератов и докладов

Основные правила эксплуатации компьютерной техники
Основные правила эксплуатации средств хранения данных
Основные правила эксплуатации компьютерных сетей

ТЕМА 6. ХИЩЕНИЯ С ИСПОЛЬЗОВАНИЕМ НОВЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Глоссарий

Хищение — совершенные с корыстной целью противоправные безвозмездное изъятие и/или обращение чужого имущества в пользу виновного или других лиц, причинившее ущерб собственнику или иному владельцу этого имущества

Мошенничество — преступление в сфере экономики, направленное против собственности, представляющее собой хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием

Компьютерное мошенничество — хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации или иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

Вымогательство — требование передачи имущества или прав на имущество под угрозой насилия над личностью потерпевшего или других лиц, оглашение сведений, которые будут иметь нежелательные последствия для потерпевшего.

Кража — тайное хищение чужого имущества.

Структура (план)

1.1. Уголовно-правовая характеристика хищений с использованием новых информационных технологий.
1.2. Способы совершения хищений с использованием новых информационных технологий.

1.3. Криминологическая характеристика хищений с использованием новых информационных технологий

Практическое занятие

В ходе практического занятия рассматриваются следующие вопросы: уголовно-правовая характеристика хищений с использованием новых информационных технологий. Способы совершения хищений с использованием новых информационных технологий. Криминологическая характеристика хищений с использованием новых информационных технологий

Вопросы для самоконтроля

Как квалифицируется получение в банкомате денег по чужой платёжной карте?
Совершение каких видов хищений возможно с использованием компьютерной техники?
Как квалифицируются многоэпизодные хищения?
Как квалифицируется использование вредоносных программ для совершения хищения?
Возможна ли квалификация хищений по совокупности с преступлениями в сфере компьютерной информации?

Кейс-задачи для обсуждения

Сотрудники вычислительного центра банка «Уникум» Каталов, Арбузов и Григорьев, имея доступ к компьютерной программе учета, ведения и оформления банковских операций отдела текущих счетов, изменили ее таким образом, что она позволяла округлять размеры платежей, а разницу перечислять на счет, открытый женой Каталова. Затем жена Каталова сняла со счета деньги в размере 120 тыс. руб., которые Каталов, Арбузов и Григорьев поделили поровну.
Группа из восьми лиц в возрасте от 20 до 36 лет, возглавляемая Лупиносом, осуществляла несанкционированный доступ к сайтам ряда коммерческих банков, получая таким образом информацию о клиентах этих финансовых учреждений. По электронной почте пострадавшим направлялись письма якобы от известных компаний. В письмах прятался вирус-троян. Он преодолевал защиту

компьютера и открывал доступ к информации. В итоге таких электронных атак указанные лица переводили на свои счета крупные суммы денег, уничтожая при этом всю базу данных на компьютерах владельцев. Как квалифицировать действия группы лиц, возглавляемой Лупиносом?

22-летний Виртальский специализировался на создании хакерских программ. Он не только создавал бот-системы и массово распространял вредоносные программы, но и лично принимал участие в хищении денег с различных счетов. Мишенью хакера были компьютеры с установленным на них программным обеспечением «Банк-Клиент». Технология была такова. Для заражения этих компьютеров и последующего хищения денег Виртальский использовал троянские программы типа Carber различных модификаций и, получив с их помощью логины, пароли и цифровые подписи, осуществлял платежи якобы от имени организаций или граждан на счета подставных фирм. Впоследствии он переводил деньги на пластиковые карты и обналичивал в банкоматах. Почти все зараженные компьютеры находились на территории России. Ежедневно вредоносные программы рассылались более чем миллиону «заинтересованных» лиц, в результате чего в отдельные дни заражалось свыше 100 тыс. компьютеров. За один раз Виртальскому удавалось завладеть сразу несколькими десятками миллионов рублей. На момент задержания хакера количество зараженных компьютеров составило около 6 млн, из них в основной бот-сети — 4,5 млн. Со счетов граждан и организаций похищено свыше 150 млн руб. Как квалифицировать действия Виртальского? Нет ли оснований для применения в этой ситуации ст. 159.6 УК?

Двадцатичетырехлетний математик, гражданин РФ Левин, изменив физический адрес технического устройства и использовав чужое имя, проник в компьютерную систему Сити-банка (Англия) с целью хищения 2,8 млн. долларов. Своими действиями Левин блокировал на длительное время законного пользователя информации о движении финансовых средств банка и осуществил разрыв сети ЭВМ. Дайте уголовно-правовую оценку действий Левина. Когда считается оконченным состав данного преступления? Что характерно для субъективной стороны этого посягательства?

Темы рефератов и докладов

Хищения с использованием банковских платёжных карт
История использования компьютеров для совершения хищений
Компьютерное вымогательство

ТЕМА 7. ПРЕСТУПЛЕНИЯ ПРОТИВ ЛИЧНОСТИ, СОВЕРШАЕМЫЕ С ПРИМЕНЕНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Глоссарий

Кибербуллинг — намеренное запугивание или травля человека с помощью цифровых технологий.

Доведение до самоубийства — преступление, в котором объектом преступления является жизнь другого человека. Объективная сторона преступления заключается в доведении до самоубийства или до покушения на самоубийство путём угроз, жестокого обращения или систематического унижения человеческого достоинства потерпевшего.

Развратные действия — действия, направленные на удовлетворение половой страсти самого виновного либо на возбуждение полового влечения или удовлетворение половой страсти потерпевшего лица. Развратные действия могут носить как физический, так и интеллектуальный характер. К развратным действиям, имеющим физический характер, относятся, например, обнажение половых органов потерпевших и стимуляция их руками или половым членом, межбёдренный коитус, мастурбация в присутствии потерпевших, совершение действий сексуального характера (половой акт, мужеложство, лесбиянство и т. д.) с третьим лицом в присутствии потерпевших, демонстрация половых органов и т. д. Развратные действия, имеющие интеллектуальный характер, предполагают информационное воздействие на психику потерпевшего лица: ведение бесед откровенного содержания, демонстрация эротических и порнографических фотографий или видеозаписей, подстрекательство потерпевших к вступлению в сексуальные контакты с третьими лицами и т. п. Развратными могут

признаваться и такие действия, которые совершаются с использованием сети Интернет, иных информационно-телекоммуникационных сетей.

Авторское право — часть гражданского права, регулирующая отношения, которые складываются в связи с использованием произведений науки, литературы и искусства.

Объект авторских прав — произведения науки, литературы и искусства независимо от достоинств и назначения произведения, а также от способа его выражения.

Программа для ЭВМ — объективная форма представления совокупности данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств с целью получения определенного результата.

Структура (план)

1.1. Уголовно-правовая характеристика преступлений против личности с использованием новых информационных технологий.
1.2. Кибербуллинг.
1.3. Развратные действия через Интернет.
1.4. Нарушение авторских и смежных прав.
1.5. Способы совершения преступлений против личности с использованием новых информационных технологий.
1.6. Криминологическая характеристика преступлений против личности с использованием новых информационных технологий

Практическое занятие

В ходе практического занятия рассматриваются следующие вопросы: уголовно-правовая характеристика преступлений против личности с использованием новых информационных технологий. Кибербуллинг. Развратные действия через Интернет. Нарушение авторских и смежных прав. Способы совершения преступлений против личности с использованием новых информационных технологий. Криминологическая характеристика преступлений против личности с использованием новых информационных технологий

Вопросы для самоконтроля

Что такое кибербуллинг?
В каких случаях кибербуллинг можно рассматривать как составляющую объективной стороны доведения до самоубийства?
Каковы особенности развратных действий, совершаемых через Интернет?
Все ли программы могут рассматриваться как объект авторских прав?
Какие действия с программой пользователь может осуществлять без согласия автора?
Какие технические средства можно использовать для защиты авторских прав?
Что такое пиринговые сети?
Каков размер нарушенных прав, необходимый для привлечения лица к уголовной ответственности?

Кейс-задачи для обсуждения

Ане 12 лет. Как и многие подростки, она мечтает стать блогером, но еще не определилась с темой блога. Пробует снимать ролики о том, как она делает себе простые прически или девчачий макияж. Делает таймлапсы о том, как рисует. Снимает процесс приготовления бутербродов или «фирменной» яичницы. Однажды родители заметили, что Аня начала сидеть на диетах. Дочь говорила, что решила вести здоровый образ жизни: отказаться от сладкого и мучного, больше гулять и все такое. Потом начались реальные проблемы с едой. Аня отказывалась есть какие-то продукты, есть в определенное время, иногда вообще ничего не ела. Дважды в день она вставала на весы и страшно психовала, если хоть чуть-чуть поправилась. Доходило до истерик, во время которых она кричала: «Я поправилась! Я не хочу быть толстой!». Наконец, Аня показала маме, что ей пишут в личных сообщениях. Там было огромное количество оскорблений: «Ты корова, ты жирная, сначала щеки втяни, потом макияж делай», «Сначала похудей, потом будешь бутерброды готовить». Писали все это как подростки, так и более взрослые люди. В основном, незнакомые. С котиками и мультяшками на аватарках. Дайте юридическую оценку ситуации.

Что бы вы ответили матери, которая пришла к вам на консультацию? Управление «К» МВД возбудило уголовное дело против 26-летнего москвича, который разместил на своей странице в «В контакте» 18 записей «известной российской музыкальной группы», сообщила пресс-служба управления. Дело возбуждено по ст. 146 УК «Нарушение авторских и смежных прав» (до шести лет лишения свободы) по обращению фирмы грамзаписи «Никитин», которой принадлежат исключительные права на эти записи. В ходе проверки специалисты управления «К» установили, что размещенные пользователем аудиозаписи скачивались более 200 000 раз, оценив ущерб «Никитина» в 108 000 руб. Дайте юридическую оценку ситуации.

Темы рефератов и докладов

Технические средства защиты авторского права и ответственность за их обход

Уголовная ответственность за нарушения авторского права с использованием пиринговых сетей

Методики оценки ущерба от нарушений авторских прав в компьютерных сетях.

ТЕМА 8. ПРЕСТУПЛЕНИЯ ПРОТИВ ЗДОРОВЬЯ НАСЕЛЕНИЯ И ОБЩЕСТВЕННОЙ НРАВСТВЕННОСТИ, СОВЕРШАЕМЫЕ С ПРИМЕНЕНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Глоссарий

Наркотические средства — вещества синтетического или естественного происхождения, препараты, включенные в Перечень наркотических средств, психотропных веществ и их прекурсоров, подлежащих контролю в Российской Федерации, в соответствии с законодательством Российской Федерации, международными договорами Российской Федерации, в том числе Единой конвенцией о наркотических средствах 1961 года.

Даркнет — скрытая сеть, соединения которой устанавливаются только между доверенными пирами, иногда

именующимися как «друзья», с использованием нестандартных протоколов и портов.

Проституция — систематическое (три и более раз) вступление в половую связь в любой форме с другим лицом за деньги или иное вознаграждение.

Порнографические материалы — живописные, графические, литературные, музыкальные и иные произведения, основным содержанием которых является грубо натуралистичное детальное изображение анатомических и/или физиологических подробностей сексуальных отношений.

Порнография — грубо натуралистическое детальное изображение анатомических и (или) физиологических подробностей интимных частей тела и сексуальных отношений (в том числе, в завуалированном виде) в форме, противоречащей принятым в обществе моральным нормам, которые не имеют художественной или научной ценности и направлены на разжигание чувственной страсти.

Распространение порнографии — возмездная или безвозмездная передача другим лицам предметов порнографического характера (изображений, видеофильмов и т.п.).

Изготовление порнографии — участие в создании любым способом (печатание, фотографирование, кино- и видеосъемка, рисование и т.п.) материала или предмета порнографического характера.

Детская порнография — материалы или предметы, содержащие любые изображения или описания ребенка или совершеннолетнего лица, имитирующего ребенка, совершающего или имитирующего действия сексуального характера или принимающего участие в совершении таких действий или в их имитации, либо реалистичные изображения (в том числе созданные с использованием анимации и электронной техники) образа ребенка, совершающего или участвующего в совершении действий сексуального характера, а равно любое изображение или описание половых органов ребенка в сексуальных целях.

Структура (план)

1.1. Уголовно-правовая характеристика преступлений против здоровья населения и общественной нравственности с использованием новых информационных технологий.
1.2. Сбыт наркотиков через Интернет и даркнет.
1.3. Проституция в Интернете.
1.4. Порнография в интернете.
1.5. Способы совершения преступлений против здоровья населения и общественной нравственности с использованием новых информационных технологий.
1.6. Криминологическая характеристика преступлений против здоровья населения и общественной нравственности с использованием новых информационных технологий

Практическое занятие

В ходе практического занятия рассматриваются следующие вопросы: уголовно-правовая характеристика преступлений против здоровья населения и общественной нравственности с использованием новых информационных технологий. Сбыт наркотиков через Интернет и даркнет. Проституция в Интернете. Порнография в интернете. Способы совершения преступлений против здоровья населения и общественной нравственности с использованием новых информационных технологий. Криминологическая характеристика преступлений против здоровья населения и общественной нравственности с использованием новых информационных технологий

Вопросы для самоконтроля

Как распространяются наркотики через сеть Интернет?
Можно ли привлечь создателей сайтов с рекламой проституток к уголовной ответственности?
Что такое порнография? Есть ли законодательное определение данного понятия?
Какие виды порнографии различаются законодателем?
Существуют ли законные способы распространения порнографии?

Возможна ли борьба с порнографией в условиях существования глобальных компьютерных сетей?

Кейс-задачи для обсуждения

Пронин расклеил на подъездах нескольких домов объявление о том, что его жена Ангелина оказывает сексуальные услуги. Фото супруги в эротических позах сопровождались пояснениями, что «ночная бабочка» удовлетворит любые фантазии и сделает для жителей этого района большие скидки. Для связи был указан телефон и адрес «путаны». Обнаружив объявления, Ангелина сразу обратилась в милицию. Расклейщика задержали. Мотивом его действий стала ревность. Молодые люди поженились в прошлом году, но прожили вместе недолго. Пронин постоянно ревновал Ангелину, придирался, изводил мелочными упреками. В итоге женщина выгнала супруга из дома. Пронин пытался помириться, но жена не захотела простить ревнивца. И он решил «пойти на крайние меры». Снимки он специально смонтировал на компьютере: лицо на них принадлежало жене, а тело — известной порнозвезде. Дайте юридический анализ изложенной выше ситуации.

Житель Краснодарского края Михаил Колесников создал интернет-сайт, своего рода витрину «продукции», через которую рекламировал курительные смеси и предлагал их купить всем желающим. Клиент, который желал приобрести смесь, связывался с ним посредством программы для общения — Skype. Обсудив детали покупки, Колесников направлял клиенту номер электронного кошелька (счета) в системе Qiwi. После получения предоплаты за товар Колесников направлял смс-сообщение на номер мобильного телефона покупателя, в котором четко указывал место, где оставлена смесь. Для закладки «спайсов» он привлек свою знакомую — 27-летнюю Марину Каширину, роль которой заключалась в распространении уже расфасованного и приготовленного к сбыту наркотика. В дальнейшем Каширина также вовлекла в торговлю спайсами Павла Пылева, который из полученного от Кашириной реагента с помощью аптечной ромашки изготавливал наркотическое средство, расфасовывал его в удобные для сбыта упаковки разных объемов. Затем указанные лица привлекли в дело Алексея и Михаила Антоновых. Последние взяли на себя основную работу по хранению, фасовке и подготовке для реализации наркотического

вещества. Дайте юридический анализ изложенной выше ситуации.

Темы рефератов и докладов

Сети TOR и I2P
«Маркетплейсы» по распространению наркотических средств
Определение понятия «порнография»
Методы борьбы с распространением порнографии в Интернете
Законодательство стран мира о порнографии

ТЕМА 9. ПРЕСТУПЛЕНИЯ ПРОТИВ КОНСТИТУЦИОННОГО СТРОЯ И БЕЗОПАСНОСТИ ГОСУДАРСТВА, СОВЕРШАЕМЫЕ С ПРИМЕНЕНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Глоссарий

Государственная тайна — сведения военного, экономического и политического характера, имеющие важное государственное значение и специально охраняемые государством.

Государственная измена — шпионаж, выдача государственной тайны, оказание помощи иностранному государству, иностранной организации или их представителям в проведении враждебной деятельности в ущерб внешней безопасности Российской Федерации, совершенное гражданином Российской Федерации.

Шпионаж — выражается в передаче, а равно собирании, похищении или хранении в целях передачи иностранному государству, иностранной организации или их представителям сведений, составляющих государственную тайну, а также передаче или собирании по заданию иностранной разведки иных сведений для использования их в ущерб внешней безопасности РФ, если эти деяния совершены иностранным гражданином или лицом без гражданства.

Доступ к сведениям, составляющим государственную тайну — санкционированное полномочным должностным лицом ознакомление конкретного работника со сведениями, составляющими государственную тайну.

Режим секретности — совокупность определяемых органами

власти и управления правил, которыми ограничивается допуск лиц к секретным материалам и работам, регламентируется порядок пользования секретных материалов, соответствующим образом регулируется поведение людей.

Экстремизм — насильственное изменение основ конституционного строя и (или) нарушение территориальной целостности Российской Федерации (в том числе отчуждение части территории Российской Федерации), за исключением делимитации, демаркации, редемаркации Государственной границы Российской Федерации с сопредельными государствами; публичное оправдание терроризма и иная террористическая деятельность; возбуждение социальной, расовой, национальной или религиозной розни; пропаганда исключительности, превосходства либо неполноценности человека по признаку его социальной, расовой, национальной, религиозной или языковой принадлежности или отношения к религии; нарушение прав, свобод и законных интересов человека и гражданина в зависимости от его социальной, расовой, национальной, религиозной или языковой принадлежности или отношения к религии; воспрепятствование осуществлению гражданами их избирательных прав и права на участие в референдуме или нарушение тайны голосования, соединенные с насилием либо угрозой его применения; воспрепятствование законной деятельности государственных органов, органов местного самоуправления, избирательных комиссий, общественных и религиозных объединений или иных организаций, соединенное с насилием либо угрозой его применения; совершение преступлений по мотивам, указанным в пункте "е" части первой статьи 63 Уголовного кодекса Российской Федерации; использование нацистской атрибутики или символики, либо атрибутики или символики, сходных с нацистской атрибутикой или символикой до степени смешения, либо атрибутики или символики экстремистских организаций, за исключением случаев использования нацистской атрибутики или символики, либо атрибутики или символики, сходных с нацистской атрибутикой или символикой до степени смешения, либо атрибутики или символики экстремистских организаций, при которых формируется негативное отношение к идеологии нацизма и экстремизма и отсутствуют признаки пропаганды или оправдания нацистской и экстремистской идеологии; публичные призывы к осуществлению указанных деяний

либо массовое распространение заведомо экстремистских материалов, а равно их изготовление или хранение в целях массового распространения; публичное заведомо ложное обвинение лица, замещающего государственную должность Российской Федерации или государственную должность субъекта Российской Федерации, в совершении им в период исполнения своих должностных обязанностей деяний, указанных в настоящей статье и являющихся преступлением; организация и подготовка указанных деяний, а также подстрекательство к их осуществлению;

Кибердиверсия — хакерские атаки на значимые для общества и государства информационные ресурсы для запрета доступа к ним или изменения их содержимого.

Структура (план)

1.1. Уголовно-правовая характеристика преступлений против конституционного строя и безопасности государства с использованием новых информационных технологий.
1.2. Экстремизм в интернете.
1.3. Кибердиверсия.
1.4. Государственная измена, шпионаж и разглашение государственной тайны.
1.5. Способы совершения преступлений против конституционного строя и безопасности государства с использованием новых информационных технологий.
1.6. Криминологическая характеристика преступлений против конституционного строя и безопасности государства с использованием новых информационных технологий

Практическое занятие

В ходе практического занятия рассматриваются следующие вопросы: уголовно-правовая характеристика преступлений против конституционного строя и безопасности государства с использованием новых информационных технологий. Экстремизм в интернете. Кибердиверсия. Государственная измена, шпионаж и разглашение государственной тайны. Способы совершения преступлений против конституционного строя и безопасности государства с использованием новых информационных технологий.

Криминологическая характеристика преступлений против конституционного строя и безопасности государства с использованием новых информационных технологий

Вопросы для самоконтроля

Какие преступления против конституционного строя и безопасности государства могут совершаться с использованием новых информационных технологий?
В чём опасность экстремизма в Интернете?
Как может быть осуществлена кибердиверсия?
Какие возможности предоставляет Интернет для деятельности разведки иностранных государств?
Как можно предотвратить распространение сведений, составляющих государственную тайну, в Интернете.

Кейс-задачи для обсуждения

Спецслужбами государства X была разработана вредоносная программа. Это был «червь», перехватывающий и модифицирующий информационный поток между программируемыми логическими контроллерами марки Simatic S7 и рабочими станциями SCADA-системы Simatic WinCC фирмы Siemens. Таким образом, червь может быть использован в качестве средства несанкционированного сбора данных (шпионажа) и диверсий в АСУ ТП промышленных предприятий, электростанций, аэропортов и т. п. Основной целью данного «червя» была ядерная программа государства Y. После успешного заражения компьютерных систем государства Y, «червь» нарушил работу почти 1000 центрифуг для обогащения уранового топлива.
В соцсети известного блогера была опубликована статья, посвященная вопросам борьбы с проявлениями национализма, расовой и религиозной розни. К этой статье была приложена иллюстрация в виде рисунка, на котором были изображены Христос, Моисей, Будда и Мохаммед, которые смотрят телевизор. На экране телевизора видны две группы людей, явно готовящихся к драке. Подпись под рисунком гласила: «А ведь мы их этому не учили». После данной публикации несколько отделений партий и общественных организаций обратились в прокуратуру, чтобы

выяснить, не возбуждает ли рисунок ненависть либо вражду к человеку в зависимости от его отношения к религии и национальности. 1. Проанализируйте данную ситуацию. 2. Есть ли основания для применения в этом случае ст. 282 УК?

Темы рефератов и докладов

Кибервойна
Примеры кибердиверсий
Борьба с киберэкстремизмом

ТЕМА 10. ПРЕСТУПЛЕНИЯ ПРОТИВ ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ, СОВЕРШАЕМЫЕ С ПРИМЕНЕНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Глоссарий

Оружие — устройства и предметы, конструктивно предназначенные для поражения живой или иной цели, подачи сигналов.

Кибертерроризм — использование Интернета для совершения насильственных действий, которые приводят к гибели людей или причинению значительного вреда здоровью или угрожают им, с целью достижения политических или идеологических выгод путем угроз или запугивания.

Пропаганда терроризма — деятельность по распространению материалов и (или) информации, направленных на формирование у лица идеологии терроризма, убежденности в ее привлекательности либо представления о допустимости осуществления террористической деятельности.

Оправдание терроризма — публичное заявление о признании идеологии и практики терроризма правильными, нуждающимися в поддержке и подражании.

Массовые беспорядки — преступление против общественной безопасности, заключающееся в организации и участии в массовых беспорядках, сопровождающихся насилием, погромами, поджогами, уничтожением имущества, применением огнестрельного оружия, взрывчатых веществ или взрывных устройств, а также оказанием вооружённого сопротивления представителям власти.

Структура (план)

1.1. Уголовно-правовая характеристика преступлений против общественной безопасности с использованием новых информационных технологий.
1.2. Сбыт оружия через Интернет и даркнет.
1.3. Кибертерроризм.
1.4. Пропаганда и оправдание терроризма.
1.5. Организация массовых беспорядков.
1.6. Способы совершения преступлений против общественной безопасности с использованием новых информационных технологий.
1.7. Криминологическая характеристика преступлений против общественной безопасности с использованием новых информационных технологий

Практическое занятие

В ходе практического занятия рассматриваются следующие вопросы: Уголовно-правовая характеристика преступлений против общественной безопасности с использованием новых информационных технологий. Сбыт оружия через Интернет и даркнет. Кибертерроризм. Пропаганда и оправдание терроризма. Организация массовых беспорядков. Способы совершения преступлений против общественной безопасности с использованием новых информационных технологий. Криминологическая характеристика преступлений против общественной безопасности с использованием новых информационных технологий

Вопросы для самоконтроля

Как распространяется оружие через сеть Интернет?
Может ли акт кибертерроризма причинить физический вред?
Опасно ли оправдание терроризма?
Как могут использоваться информационно-телекоммуникационные сети для организации массовых беспорядков?
Кем ведётся пропаганда терроризма?

Кейс-задачи для обсуждения

Выступая в своей авторской передаче «Минутка просветления», журналистка Светлана Прокопьева прочитала свой текст с размышлениями о причинах взрыва в УФСБ Архангельска, закончившегося смертью 17-летнего левого террориста и анархо-коммуниста Михаила Жлобицкого. Прокопьева связала самоподрыв Жлобицкого с общественно-политической ситуацией в стране. На следующий день, 8 ноября, текст выступления был опубликован на сайте информагентства «Псковская лента новостей» под заголовком «Репрессии для государства». Прокопьевой было предъявлено обвинение в оправдании терроризма. Дайте юридическую оценку ситуации.

Telegram-канал «Что делать!» был создан 3 февраля 2021 года, но первая запись в группе появилась 6 мая. Были ли до этого какие-то записи, которые могли быть удалены, неизвестно. Первая публикация начиналась с громких слов о том, что «Россия все глубже впадает в жесткую диктатуру», но это «можно и необходимо исправить». «Давайте объединяться, неважно, за кого вы, главное: за все хорошее против всего плохого!» — заканчивается текст. Все последующие записи в группе были также с явным «оппозиционным» уклоном. Авторы регулярно повторяли, что «Россия будет свободной и счастливой», жаловались на «захлестнувшие страну политические репрессии», репостили публикации известных правозащитных НКО и ролики из СМИ. Канал, очевидно, не пользовался популярностью: в записи от 7 июня авторы признавались, что на тот момент в их группе состояло всего 32 человека, а «вчера было четыре». 20 июня участники канала перешли к активным действиям и открыли отдельный чат для «координации и консолидации на местах» для сторонников из Санкт-Петербурга. В тот же день появилось сообщение, где авторы канала готовят «показательную акцию во всех крупных и средних городах», предлагалось распределить роли между собой и составить план действий. Из постов в группе сложно однозначно понять, что конкретно планировали организаторы. Цель протеста описана расплывчато, а сам текст изложен казенным языком: «Определяем по назначениям подразделения и группы, которые будут заниматься своими специализированными действиями. Для этого мы определим профессиональные и физические способности участников нашего

движения. Специфика работы у каждой группы будет своя, в соответствии с их навыками и назначением». Дайте юридическую оценку ситуации.

Темы рефератов и докладов

Известные акты кибертерроризма
Использование mesh-сетей для организации массовых беспорядков
Маркетплейсы по сбыту оружия в Интернете

ТЕМА 11. ЧАСТНЫЕ ВОПРОСЫ ОРГАНИЗАЦИИ ДЕЯТЕЛЬНОСТИ СОТРУДНИКОВ УИС ПО ПРЕСЕЧЕНИЮ УГРОЗ И ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С ИСПОЛЬЗОВАНИЕМ ИТС

Глоссарий

Информационные технологии — процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информационная система — совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Обладатель информации — лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

Конфиденциальность информации — обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Распространение информации — действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

Структура (план)

1.1. Особенности деятельности сотрудников УИС по пресечению угроз и преступлений, связанных с использованием ИТС.
1.2. Сбор информации о посягательствах, совершаемых с использованием ИТС.
1.3. Тактика пресечения преступных деяний по отдельным видам преступлений в сфере высоких технологий.

Практическое занятие

В ходе практического занятия рассматриваются следующие вопросы: особенности деятельности сотрудников УИС по пресечению угроз и преступлений, связанных с использованием ИТС. Сбор информации о посягательствах, совершаемых с использованием ИТС. Тактика пресечения преступных деяний по отдельным видам преступлений в сфере высоких технологий.

Вопросы для самоконтроля

Назовите характерные для данной сферы деятельности угрозы, связанные с использованием ИТС.
Назовите основные направления деятельности сотрудников правоохранительных органов по пресечению угроз, связанных с использованием ИТС
Назовите основные направления деятельности сотрудников правоохранительных органов по пресечению преступлений, связанных с использованием ИТС
Назовите основные методы сбора информации о посягательствах, совершаемых с использованием ИТС.
Назовите основные тактические приёмы пресечения преступных действий в сфере высоких технологий.

Кейс-задачи для обсуждения

Проходивший в правоохранительном органе практику студент Воскобойников разработал компьютерный вирус и ввел его в

компьютерную сеть правоохранительного органа с целью подрыва его деятельности. Укажите меры по пресечению данного преступления, основные методы сбора необходимой информации и действия сотрудников правоохранительного органа.

С целью получения информации о деятельности правоохранительного органа вор в законе Новиков поручил своему «помощнику» передать крупное вознаграждение программисту Коновалову, имевшему доступ к этой информации. Коновалов скопировал требуемую информацию, которая была передана Новикову. Укажите меры по пресечению данного преступления, основные методы сбора необходимой информации и действия сотрудников правоохранительного органа.

Темы рефератов и докладов

Пресечение преступных деяний, связанных с неправомерным доступом к информации

Пресечение преступных деяний, связанных с саботажем информационных систем

Пресечение преступных деяний, связанных с распространением информации

ТЕМА 12. ЧАСТНЫЕ ВОПРОСЫ ОРГАНИЗАЦИИ ДЕЯТЕЛЬНОСТИ СОТРУДНИКОВ УИС ПО ПРЕСЕЧЕНИЮ УГРОЗ И ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С ИСПОЛЬЗОВАНИЕМ ИТС

Глоссарий

Коммуникационная инфраструктура — сетевая инфраструктура, обеспечивающая передачу информации между территориально распределенными источниками и получателями, состоящая из линий связи, использующих различные среды распространения электромагнитных сигналов, и оборудования, обеспечивающего прием, передачу этих сигналов, и их обработку в процессе этой передачи.

Информационная безопасность — состояние защищенности, обеспечивающее конфиденциальность доступа к информации,

авторизованный доступ к ней, ее целостность, достоверность, полноту и непротиворечивость.

Оперативно-розыскная деятельность — мероприятия, выполняемые гласно и негласно уполномоченными на это государственными органами с целью выявить, пресечь или раскрыть преступление, отыскать скрывающихся и пропавших без вести людей, установить имущество, подлежащее конфискации, добыть информацию о событиях и деяниях, опасных для государства.

Негласное наблюдение — комплекс мероприятий, которые проводят оперативные службы в рамках оперативно-разыскной деятельности по скрытому, негласному, либо зашифрованному визуальному наблюдению за лицом, представляющим оперативный интерес, с целью получения о нём и его образе жизни максимально полной информации.

Криминологическая профилактика — деятельность, нацеленная именно на недопущение преступлений. Такая профилактика реализовывается путем влияния на условия и причины совершения преступлений и конкретных лиц (или некоторые их категории), в отношении которых существует надобность удержания их от совершения преступлений.

Структура (план)

1.1. Особенности деятельности сотрудников УИС по профилактике преступлений, связанных с использованием ИТС.
1.2. Сбор информации о планируемых посягательствах, совершаемых с использованием ИТС.
1.3. Тактика профилактики преступных деяний по отдельным видам преступлений в сфере высоких технологий.

Практическое занятие

В ходе практического занятия рассматриваются следующие вопросы: особенности деятельности сотрудников УИС по профилактике преступлений, связанных с использованием ИТС. Сбор информации о планируемых посягательствах, совершаемых с использованием ИТС. Тактика профилактики преступных деяний по отдельным видам преступлений в сфере высоких технологий

Вопросы для самоконтроля

Назовите характерные для данной сферы деятельности направления профилактики преступлений, связанных с использованием ИТС.
Назовите основные приёмы деятельности сотрудников правоохранительных органов по профилактике угроз, связанных с использованием ИТС
Назовите какие подразделения правоохранительных органов в соответствующей сфере занимаются профилактикой преступлений, связанных с использованием ИТС
Назовите основные методы сбора информации о планируемых посягательствах, совершаемых с использованием ИТС.
Назовите основные тактические приёмы профилактики преступных действий в сфере высоких технологий.

Кейс-задачи для обсуждения

Инженер-программист Рунов работал в информационно-вычислительном центре правоохранительного органа. В нерабочее время на вверенном ему компьютере Рунов писал научные работы с целью их продажи студентам юридических вузов. При этом он использовал флэшки, зараженные компьютерными вирусами, в результате действия которых была уничтожена хранящаяся в компьютере информация. Укажите, какие профилактические мероприятия могли бы предотвратить подобные преступления.
Уволенный за несоответствие занимаемой должности программист правоохранительного органа Поповский, желая отомстить начальнику, перед уходом ввел в компьютерную сеть органа вредоносную программу, которая уничтожила большую часть информации о сотрудниках данного органа и материалы по текущим делам. Для восстановления уничтоженной информации органа пришлось провести большую работу, причинён крупный имущественный ущерб, планы правоохранительной деятельности были сорваны. Укажите, какие профилактические мероприятия могли бы предотвратить подобные преступления.

Темы рефератов и докладов

Профилактика преступных деяний, связанных с неправомерным доступом к информации
Профилактика преступных деяний, связанных с саботажем информационных систем
Профилактика преступных деяний, связанных с распространением информации

3. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

3.1. Основная и дополнительная литература

Основная:

1. Спеваков, Александр Геннадьевич. Информационная безопасность : учебное пособие : [для студентов, обучающихся по специальностям 100301 "Информационная безопасность", 400301 "Правоохранительная деятельность", 380301 "Экономика"] / А. Г. Спеваков, М. О. Таныгин, В. С. Панищев ; Юго-Зап. гос. ун-т. - Курск : ЮЗГУ, 2017. - 196 с. Текст: электронный.
2. Спеваков, Александр Геннадьевич. Информационная безопасность : учебное пособие : [для студентов, обучающихся по специальностям 100301 "Информационная безопасность", 400301 "Правоохранительная деятельность", 380301 "Экономика"] / А. Г. Спеваков, М. О. Таныгин, В. С. Панищев ; Юго-Зап. гос. ун-т. - Курск : ЮЗГУ, 2017. - 196 с. Текст: непосредственный.
3. Криминология. Особенная часть [Текст] : учебник для академического бакалавриата : в 2 т. / Академия Генеральной прокуратуры РФ ; под общ. ред. ректора Академии Генеральной прокуратуры РФ, д-ра юрид. наук, проф. О. С. Капинус. - Москва : Юрайт, 2017. - ISBN 978-5-534-03382-3. - Текст : непосредственный. Т. 1. - 312 с.
4. Байбарин, Андрей Андреевич. Уголовное право России. Общая часть : учебное пособие : [для студентов и слушателей, обучающихся по программам специалистов, бакалавров и магистров, профессорско-преподавательского состава высших учебных заведений, научных работников] / А. А. Байбарин, А. А. Гребеньков, С. В. Шевелева ; Юго-Зап. гос. ун-т. - Курск : ЮЗГУ, 2017. - 428 с. - Текст : электронный.

5. Байбарин, Андрей Андреевич. Уголовное право России. Общая часть : учебное пособие : [для студентов и слушателей, обучающихся по программам специалистов, бакалавров и магистров, профессорско-преподавательского состава высших учебных заведений, научных работников] / А. А. Байбарин, А. А. Гребеньков, С. В. Шевелева ; Юго-Зап. гос. ун-т. - Курск : ЮЗГУ, 2017. - 428 с. - Текст : непосредственный.

Дополнительная литература

6. Байбарин, Андрей Андреевич. Практикум по курсу "Уголовное право" : учебное пособие / А. А. Байбарин, А. А Гребеньков, М. Н. Урда ; Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования "Юго-Западный государственный университет". - Курск : ЮЗГУ, 2013. - 209 с. - Текст : электронный.
7. Уголовный кодекс Российской Федерации: федер. закон Рос. Федерации от 13.06.1996 № 63-ФЗ. URL: http://www.consultant.ru/document/cons_doc_LAW_10699/
8. Криминология. Особенная часть [Текст] : учебник для академического бакалавриата : в 2 т. / Академия Генеральной прокуратуры РФ ; под общ. ред. ректора Академии Генеральной прокуратуры РФ, д-ра юрид. наук, проф. О. С. Капинус. - Москва : Юрайт, 2017. - Текст : непосредственный. Т. 2. - 311 с.

3.2. Перечень методических указаний

Противодействие посягательствам в уголовно-исполнительной системе, совершаемых при помощи информационно-телекоммуникационных сетей: методические рекомендации по подготовке к практическим занятиям для студентов всех форм обучения специальности 40.05.02 Правоохранительная деятельность / Юго-Зап. гос. ун-т; сост.: А.А. Гребеньков, М. И. Синяева, А.Б. Баумштейн. - Курск, 2022. - 30 с.

3.3. Используемые информационные технологии и перечень ресурсов информационно-телекоммуникационной сети Интернет

1. www.elibrary.ru - Электронная библиотека

2. http://www.garant.ru - Он-лайн версия справочно-правовой системы «Гарант» - нормативные акты, судебная практика, комментарии к законодательству, научные статьи

3. http:// www.gov.ru - Сервер органов государственной власти Российской Федерации

4. http://biblioclub.ru - Электронно-библиотечная система «Университетская библиотека онлайн».

5. http://www.consultant.ru - Официальный сайт компании «Консультант Плюс».

https://e.lanbook.com / - ЭБС «Лань»