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
«15» 12 2017 г.

**Методические указания для самостоятельной работы
по изучению дисциплины
«Преступность в сфере высоких технологий»
для студентов всех форм обучения
специальности 40.05.02 Правоохранительная деятельность**

Курск 2017

УДК 343.2

Составители: М. И. Синяева, А. А. Байбарин, А. А. Гребеньков

Рецензент
Доктор юридических наук, доцент В.В. Богдан

Методические указания для самостоятельной работы по изучению дисциплины «Преступность в сфере высоких технологий» для студентов всех форм обучения специальности 40.05.02 Правоохранительная деятельность / сост. М. И. Синяева, А. А. Байбарин, А. А. Гребеньков: Юго-Зап. гос. ун-т. Курск, 2017. 39 с.

Методические указания составлены на основании учебного плана специальности 40.05.02 Правоохранительная деятельность и рабочей программы дисциплины «Преступность в сфере высоких технологий».

Включают общие положения, широкий набор различных видов работы обучающихся при освоении дисциплины «Преступность в сфере высоких технологий»: 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 бакалавров.

Методические указания помогают сформировать студентам знания и навыки в предметной области дисциплины, развить у студентов перспективное мышление и творческие способности к исследовательской деятельности, усвоить необходимые компетенции.

Предназначены для студентов всех форм обучения специальности 40.05.02 Правоохранительная деятельность.

Текст печатается в авторской редакции

Подписано в печать 15.12.17. Формат 60х84 1/16.
Усл. печ. л.2,3. Уч.-изд. л. 2,1. Тираж 50 экз. Заказ 3676. 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.

Задачи дисциплины:

- научить студента формулировать и решать задачи, возникающие в ходе научно-исследовательской и педагогической деятельности по дисциплинам уголовно-правового цикла (в том числе криминологии),
- дать ему углубленные профессиональные знания, касающиеся преступлений в сфере новых информационных технологий,
- сформировать умение выбирать необходимые методы исследования, модифицировать существующие и разрабатывать новые методы, исходя из задач исследования,
- научить студента обрабатывать полученные результаты, анализировать и осмысливать их с учетом имеющихся литературных данных, вести библиографическую работу с привлечением современных информационных технологий, представлять итоги проделанной работы в виде отчетов, рефератов, статей, оформленных в соответствии с имеющимися требованиями, с привлечением современных средств редактирования и печати,
- сформировать понимание методологических основ и специфики методов, используемых в уголовно-правовой и криминологической теории, а также информационном праве в связи с проблематикой преступности в сфере новых информационных технологий.

Обучающиеся должны **знать:**

— общие принципы раскрытия и расследования преступлений в сфере высоких технологий, основные элементы их уголовно-правовой, криминологической и криминалистической характеристики;

— специфичные для отдельных преступлений в сфере высоких технологий особенности признаков их составов, приёмы квалификации, криминологическую специфику, технико-тактические особенности их выявления, раскрытия и расследования;

— положения теории уголовного права, криминологии и криминалистики, связанные с обеспечением эффективного противодействия преступности в сфере высоких технологий, борьбы с ней;

— общие принципы предупреждения преступлений в сфере высоких технологий, основные элементы комплекса их причин и условий;

— характерные для отдельных преступлений в сфере высоких технологий компоненты комплекса причин и условий, особенности личности преступника, механизма преступления, влияющие на выбор мер их предупреждения;

— разрабатываемые уголовно-правовой и криминологической доктриной передовые методы решения проблемных задач в сфере предупреждения преступлений в сфере высоких технологий, установления их причин и условий и воздействия на них;

уметь:

— на основе теоретических знаний о раскрытии и расследовании преступлений в сфере высоких технологий и с использованием технических средств и тактических приемов выделять из окружающей действительности уголовно-правовые, криминологические и криминалистические факты, явления, события; наблюдать, сравнивать, анализировать и систематизировать признаки преступлений в сфере высоких технологий, понимать их механизм;

— объяснять, описывать на языке современной уголовно-правовой, криминологической и криминалистической науки характеристику преступности в сфере высоких технологий, прогнозировать её развитие, находить пути более эффективного

раскрытия и расследования преступлений в сфере высоких технологий;

— моделировать опытно-экспериментальную и исследовательскую работу в сфере уголовно-правового, криминалистического и криминологического противодействия преступности в сфере высоких технологий, применения технико-криминалистических средств и методов, совершенствования тактических приёмов и форм организации раскрытия и расследования преступлений в сфере высоких технологий;

— выявлять причины и условиях конкретных преступных деяний в сфере высоких технологий, предлагать меры частного криминологического воздействия;

— оценивать общую криминологическую ситуацию в сфере противодействия преступлениям в сфере высоких технологий с выявлением системных причин и условий их совершения, разрабатывать правовые, организационные и технические меры предупреждения преступности в данной сфере;

— на теоретическом уровне осуществлять прогнозирование состояния преступности в сфере высоких технологий с учётом тенденций развития её детерминационного комплекса, а также предпринимаемых мер по её предупреждению;

владеть:

— спецификой методологии практического применения теоретических основ раскрытия и расследования преступлений в сфере высоких технологий с учётом специфики их уголовно-правовой, криминологической и криминалистической характеристики;

— способами правильного установления, фиксации и оценки фактов, событий, обстоятельств, позволяющими установить объективную истину по делам о преступлениях в сфере высоких технологий;

— приемами и методами, позволяющими осуществить правильную уголовно-правовую оценку конкретных преступлений в сфере высоких технологий, определить наиболее эффективные пути и средства их расследования, криминологические меры предупреждения аналогичных преступлений в будущем;

— навыками индивидуального криминологического воздействия на ситуацию, в которой совершаются преступные деяния в сфере высоких технологий, с целью устранения их причин и условий, предупреждения совершения будущих преступлений;

— умением комплексно анализировать сложившуюся на уровне региона и страны в целом криминологическую обстановку по преступлениям в сфере высоких технологий, разрабатывать комплексные социально-экономические меры противодействия данной категории преступлений;

— методами и приёмами научного криминологического исследования причин и условий преступности в сфере высоких технологий, поиска новых инновационных способов противодействия ей, теоретического и эмпирического анализа их эффективности.

У обучающихся формируются следующие компетенции:

— способность применять в профессиональной деятельности теоретические основы раскрытия и расследования преступлений, использовать в целях установления объективной истины по конкретным делам технико-криминалистические методы и средства, тактические приемы производства следственных действий, формы организации и методику раскрытия и расследования отдельных видов и групп преступлений (ПК-14).

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 «29» декабря 2016 г., протокол №4.

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 (кол-во часов)			СРС (объем в часах)
		Лк	Лр	Пр	
1	Понятие и общая характеристика преступлений в сфере высоких технологий.	2	0	4	6
2	Компьютерная информация как объект уголовно-правовой охраны.	2	0	4	6
3	Неправомерный доступ к компьютерной информации.	2	0	4	6
4	Создание, использование и распространение вредоносных компьютерных программ.	2	0	4	6
5	Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телеком-муникационных сетей.	2	0	4	6
6	Посягательства на авторские и смежные права в компьютерных сетях.	2	0	4	6
7	Хищения с использованием новых информационных технологий.	4	0	8	12
8	Распространение порнографии в компьютерных сетях.	2	0	4	6
	Итого за 7 семестр	18		36	54
	Форма контроля	зачет			
	Общая трудоемкость (час) / ЗЕ	54 часов / 1,5 ЗЕ			54часа /1,5 ЗЕ
ВСЕГО по дисциплине		108 часа / 3 ЗЕ			

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

№ п/п	Наименование темы	Вид проводимого занятия (кол-во часов)			СРС (объем в часах)
		Лк	Лр	Пр	
1	Понятие и общая характеристика преступлений в сфере высоких технологий.	1	0	1	47
2	Компьютерная информация как объект уголовно-правовой охраны.		0	1	0
3	Неправомерный доступ к компьютерной информации.		0	1	0
4	Создание, использование и распространение вредоносных компьютерных программ.		0	1	0
5	Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телеком-муникационных сетей.	1	0	1	0
6	Посягательства на авторские и смежные права в компьютерных сетях.		0	1	0
7	Хищения с использованием новых информационных технологий.		0	1	47
8	Распространение порнографии в компьютерных сетях.		0	1	0
	Итого за семестр	2		8	94
	Контроль /экз (подготовка к экзамену)				4
	Форма контроля	зачет			
	Общая трудоемкость (час) / ЗЕ	10 часов / 0,2 ЗЕ			98 часов /2,8 ЗЕ
ВСЕГО по дисциплине		108 часа / 3 ЗЕ			

1.3. Методические рекомендации по организации изучения дисциплины

В рамках изучения дисциплины «Преступность в сфере высоких технологий» работа студентов организуется в следующих формах:

— работа с конспектом лекций и дополнительной литературой по темам курса;

— изучение вопросов, выносимых за рамки лекционных занятий (дискуссионные вопросы для дополнительного изучения);

— подготовка к семинарскому занятию;

— выполнение групповых и индивидуальных домашних заданий, в том числе:

— проведение собеседования по теме лекции;

— подготовка краткого доклада (резюме, эссе) по теме семинарского занятия и разработка мультимедийной презентации к нему;

— выполнение практических заданий (решение задач);

— 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 конечном итоге успешно сдать зачёт по дисциплине «Преступность в сфере высоких технологий».

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

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 ученых по изучаемой теме. Необходимым является глубокое усвоение содержания лекции и свободное владение им, в том числе использованной в ней терминологии (понятий), категорий и законов (глоссарий к каждой теме содержится в разделе 2 настоящих методических указаний). 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. 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 бакалавров. *Изучение вопросов, выносимых за рамки лекционных занятий,* предполагает самостоятельное изучение студентами дополнительной литературы и её конспектирование по этим вопросам.

3. В ходе *практических занятий* проводится разъяснение теоретических положений курса, уточнение междисциплинарных связей.

Подготовка к практическому (семинарскому) занятию предполагает большой объём самостоятельной работы и включает в себя:

— знакомство с планом семинарского 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;

— ответы на вопросы, приведенные к каждой теме;

— обдумывание вопросов для обсуждения, выдвижение собственных вариантов ответа;

— выполнение заданий преподавателя.

— 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. По дисциплине «Уголовное право» она предполагает подготовку индивидуальных или групповых (на усмотрение преподавателя) *докладов (сообщений, рефератов, эссе, творческих заданий)* на семинарских занятиях и разработку мультимедийной презентации к ним, а также решение задач в письменной (электронной) форме.

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.

По усмотрению преподавателя, он сам формирует задание, либо даёт возможность студентам возможность самостоятельно выбрать одну из предлагаемых тем. 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 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.

Также по дисциплине «Преступность в сфере высоких технологий» формой самостоятельной работы студентов является *выполнение практических заданий (решение задач)*. Часть практических заданий может быть выполнена студентами на аудиторных практических (лабораторных) 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.

Обязательными к выполнению являются практические задания, выдаваемые студентам индивидуально для домашней подготовки (как правило, 2 задания на 1 тему). Они должны быть выполнены студентами в письменной (электронной) форме и представлены на проверку преподавателем.

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

7. *Самоконтроль* является обязательным элементом самостоятельной работы студента по дисциплине «Преступность в сфере высоких технологий». 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:

— ответ на вопросы для самоконтроля для самоанализа глубины и прочности знаний и умений по дисциплине;

— 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 предлагают вопросы для самоконтроля по каждой изучаемой теме);

— самостоятельное решение практических заданий;

— самостоятельное тестирование по предложенным в настоящих методических указаниях тестовым заданиям.

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.

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 зачета. Контрольно-измерительные материалы к зачету и экзамену утверждаются заведующим 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 (max 100)	менее 50	50-69	70-84	85-100
Оценка по дисциплине без экзамена	Не зачтено	Зачтено		

Промежуточная аттестация по дисциплине проводится в форме зачета. Зачет проводится в форме бланкового тестирования.

Для тестирования используются контрольно-измерительные материалы (КИМ) – задания в тестовой форме, составляющие банк тестовых заданий (БТЗ) по дисциплине, утвержденный в установленном в университете порядке.

Проверяемыми на промежуточной аттестации элементами содержания являются темы дисциплины, указанные в разделе 3 настоящей программы. Все темы дисциплины отражены в КИМ в равных долях (%). БТЗ включает в себя не менее 100 заданий и постоянно пополняется.

Для проверки *знаний* используются вопросы и задания в различных формах:

–закрытой (с выбором одного или нескольких правильных ответов),

–открытой (необходимо вписать правильный ответ),

– на установление правильной последовательности,

– на установление соответствия.

Умения, навыки и компетенции проверяются с помощью задач (ситуационных, производственных или кейсового характера) и различного вида конструкторов. Все задачи являются многоходовыми. Некоторые задачи, проверяющие уровень сформированности компетенций, являются многовариантными. Часть умений, навыков и компетенций прямо не отражена в формулировках задач, но они могут быть проявлены обучающимися при их решении.

В каждый вариант КИМ включаются задания по каждому проверяемому элементу содержания во всех перечисленных выше формах и разного уровня сложности. Такой формат КИМ позволяет объективно определить качество освоения обучающимися

основных элементов содержания дисциплины и уровень сформированности компетенций.

Примеры заданий типового бланкового тестирования

1. Компьютерная информация может быть представлена в форме:

1) электрических сигналов
2) магнитной записи
3) распечатки машинного кода
4) QR-кода

2. Установите соответствие:

А) Информационная безопасность	1) Неправомерный доступ к КИ
Б) Общественная нравственность	2) Распространение порнографии
В) Конституционные права и свободы	3) Нарушение авторских прав
Г) Собственность	4) Компьютерное мошенничество

3. Сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи — это _____.

4. Установите последовательность этапов совершения преступления в сфере компьютерной информации:

1) формирование умысла
2) приготовление
3) покушение
4) оконченное преступление

Кейс-задача

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.

Для промежуточной аттестации студентов очной 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 последовательности – 2 балла,
- задание на установление соответствия – 2 балла,
- решение задачи – 6 баллов.

Максимальное количество баллов за тестирование - 36 баллов.

Для промежуточной аттестации студентов очно-заочной и 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 последовательности – 3 балла,
- задание на установление соответствия – 3 балла,
- решение задачи – 15 баллов.

Максимальное количество баллов за тестирование –60 баллов.

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

1. Понятие и общая характеристика преступлений в сфере высоких технологий

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.

План

1. Понятие киберпреступности
2. Виды преступлений в сфере высоких технологий
3. Особенности личности «киберпреступников»
4. Источники правового регулирования

Рекомендуемая литература и электронные ресурсы

Киберпреступность. URL: http://soft.compulenta.ru/security/crime/
Раймонд Э.С. Новый словарь хакера. М.: Центрком, 1996.
Тропина Т.Л. Борьба с киберпреступностью: возможна ли разработка универсального механизма? // Международное правосудие. 2012. № 3. С. 86 - 95.

Чекунов И.Г. Киберпреступность: понятие и классификация // Российский следователь. 2012. № 2. С. 37 - 44.
Гребеньков А. А. Преступность в сфере высоких технологий: исторический аспект // Известия Юго-Западного государственного университета. Серия История и право. 2012. № 1. Часть 1. С. 184-188.

Темы рефератов и докладов

Социально-культурологический портрет «хакера»

Международно-правовое регулирование борьбы с киберпреступностью

История российского законодательства о борьбе с киберпреступностью

2. Компьютерная информация как объект уголовно-правовой охраны

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.

План

1. Понятия «информация» и «компьютерная информация»

2. Общие принципы информационной безопасности и защиты компьютерной информации в Российской Федерации
3. Объект преступлений в сфере компьютерной информации

Рекомендуемая литература и электронные ресурсы

Овчинский А. С. Информация и оперативно-розыскная деятельность : Монография. - М. : ИНФРА-М, 2002. - 95 с. - ISBN 5-16-00106-X

Волькенштейн М. В. Энтропия и информация. - М. : Наука, 1986. - 190 с.

Мельников В. П. Информационная безопасность и защита информации: учебное пособие. М.: Академия, 2006. 336 с.

Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации. М. : Горячая линия-Телеком, 2004. 280 с.

Информация // Википедия. Дата обновления: 04.03.2014. URL: http://ru.wikipedia.org/?oldid=42336021

Голубев В. Компьютерная информация, как объект правоотношений. URL: http://www.crime-research.ru/library/Golubev09_03.html

Карчевский Н. В. Компьютерные преступления: определение, объект и предмет. URL: http://www.ifap.ru/pi/05/karchev.htm

Соколова С.Н., Сенив Ю.М. Информационное право и государственное регулирование информационной безопасности // Информационное право. 2013. № 2. С. 3 - 7.

Гребеньков А. А. История формирования норм об ответственности за компьютерные преступления в России // Известия Юго-Западного государственного университета. Серия История и право. 2012. № 1. Часть 2. С. 53-56.

Гребеньков А. А. Общие подходы к определению понятия «компьютерная информация» в уголовно-правовой теории // Известия Юго-Западного государственного университета. Серия История и право. 2012. № 1. Часть 2. С. 135-138.

Гребеньков А. А. Родовой объект преступлений в сфере компьютерной информации // Известия Юго-Западного государственного университета. Серия История и право. 2012. № 2. Часть 2. С. 30-34.

Темы рефератов и докладов

История российского законодательства об информационном обороте и информационной безопасности

Доктрина информационной безопасности РФ

Основные стандарты обеспечения информационной безопасности

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

План

1. Уголовно-правовая характеристика неправомерного доступа к компьютерной информации
2. Способы совершения неправомерного доступа к компьютерной информации
3. Криминологическая характеристика неправомерного доступа к компьютерной информации
4. Особенности расследования преступлений, связанных с неправомерным доступом к компьютерной информации

Рекомендуемая литература и электронные ресурсы

Гайдамакин Н. А. Разграничение доступа к информации в компьютерных системах: монография. - Екатеринбург : Изд-во Урал. ун-та, 2003. - 328 с. - ISBN 5-86037-024-5

Веретенников А. А. Защита информации от несанкционированного доступа: учебно-методическое пособие. Курск : РОСИ, 2006. 40 с.

Богомолов Н. В. Уголовная ответственность за неправомерный доступ к компьютерной информации. URL: http://ndki.narod.ru/liblary/manuals/manuals_docs/Bogomolov_MB-Manual1.doc (дата обращения: 03.03.2014).

Гребеньков А. А. Проблемы разграничения неправомерного доступа к компьютерной информации с другими составами преступлений // Известия Юго-Западного государственного университета. Серия История и право. 2012. № 2. Часть 1. С. 159-163.

Гребеньков А. А. Субъективные и квалифицирующие признаки неправомерного доступа к компьютерной информации // Известия Юго-Западного государственного университета. Серия История и право. 2012. № 2. Часть 1. С. 214-217.

Гребеньков А. А. Отдельные последствия и причинная связь в составе неправомерного доступа к компьютерной информации // Известия Юго-Западного государственного университета. Серия История и право. 2013. № 1. С. 21-26.

Гребеньков А. А. Факультативные признаки неправомерного доступа к компьютерной информации // Известия Юго-Западного государственного университета. Серия История и право. 2013. № 1. С. 63-67.

Кейс-задачи

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?

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.

Темы рефератов и докладов

Основные методы защиты от неправомерного доступа

Личность преступника, совершающего неправомерный доступ к компьютерной информации.

Понятие «компьютерная информация»

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.

План

1. Уголовно-правовая характеристика создания, использования и распространения вредоносных компьютерных программ
2. Способы совершения создания, использования и распространения вредоносных компьютерных программ
3. Криминологическая характеристика создания, использования и распространения вредоносных компьютерных программ
4. Особенности расследования преступлений, связанных с созданием, использованием и распространением вредоносных компьютерных программ

Рекомендуемая литература и электронные ресурсы

Компьютерный вирус // Википедия. Дата обновления: 03.03.2014. URL: http://ru.wikipedia.org/?oldid=42320442 (дата обращения: 03.03.2014).

История вредоносных программ. URL: http://www.securelist.com/ru/threats/detect?chapter=34 (дата обращения: 03.03.2014).

Евдокимов К.Н. К вопросу о совершенствовании объективной стороны состава преступления при создании, использовании и распространении вредоносных компьютерных программ (ст. 273 УК РФ) // Российский следователь. 2013. № 7. С. 18 - 24.

Евдокимов К.Н. К вопросу о субъективной стороне состава преступления при создании, использовании и распространении вредоносных компьютерных программ (ст. 273 УК РФ) // Российский следователь. 2013. № 8. С. 22 - 26.

Евдокимов К.Н. К вопросу об объекте состава преступления при создании, использовании и распространении вредоносных программ для ЭВМ (ст. 273 УК РФ) // Российский следователь. 2012. № 12. С. 24 - 27.

Быков В.М., Черкасов В.Н. Новое об уголовной ответственности за создание, использование и распространение вредоносных компьютерных программ // Российский судья. 2012. № 7. С. 16 - 21.

Кейс-задачи

К., обнаружив в интернете сайт, на котором представители кавказских национальностей обсуждали способы знакомства с русскими девушками, движимый мотивом неприязни к лицам указанных национальностей, разместил на одном из популярных интернет-форумов своё описание ситуации, в котором в грубой форме с использованием матерной брани высказал мнение о неполноценности лиц указанных национальностей. К сообщению К. приложил ссылку на программу «Low Orbit Ion Cannon», предназначенную для организации интернет-атак типа «распределённый отказ в обслуживании» (DDoS) и инструкцию по её использованию для приведения в неработоспособное состояние указанного им сайта. Согласно записям в техническом журнале

форума, программу скачали 2530 человек. В ходе следственных мероприятий была установлена личность 120 из них, доказать факт использования программы удалось в отношении 10. В результате атаки сайт не работал две недели, в результате перегрузки оборудования владельцу оборудования ООО «Самшит», на котором размещался сайт, был причинён ущерб 30 тысяч рублей, на восстановление сайта и перенос его на другой сервер его владельцем Г. было потрачено 50 тысяч рублей. Кроме того, Ч., один из пользователей форума, на котором К. разместил сообщение, подобрав пароль администратора сайта, скопировал личные данные 1300 пользователей сайта (электронные адреса, пароли, анкеты для знакомств) и разместил их на том же форуме. Дайте полную юридическую оценку деяния.

Боровиков, являясь оператором ЭВМ в одной из организаций, на своем компьютере изготовил электронное почтовое сообщение с рекламой товаров, приложив к нему в качестве подробного каталога с ценами составленную им программу ЭВМ, и распространил ее в сети Интернет 350 адресатам. В результате массового распространения этой программы после ее запуска пользователями сети Интернет, Боровиков несанкционированно получил по своему электронному адресу 87 учетных имен и паролей для доступа в Интернет, которые скопировал на жесткий диск своего компьютера и в дальнейшем использовал для доступа в сеть Интернет.

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.

5. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

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.

План

1. Уголовно-правовая характеристика нарушения правил эксплуатации средств хранения, обработки или передачи

компьютерной информации и информационно-телекоммуникационных сетей
2. Криминологическая характеристика нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей
3. Перспективы совершенствования нормы об ответственности за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

Рекомендуемая литература и электронные ресурсы

Быков В.М., Черкасов В.Н. Новая редакция ст. 274 УК // Законность. 2012. № 11. С. 25 - 29.

Ягудин А. Н. Уголовная ответственность за нарушение правил эксплуатации средств хранения, обработки и передачи компьютерной информации и информационно-телекоммуникационных сетей. Автореферат дисс… канд. юрид. наук. М., 2013. 28 с.

Суслопаров А.В., Тарбагаев А.Н. Ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей: уголовно-правовой и административный аспекты // Правовая политика и правовая жизнь. 2012. № 2. С. 53-58.

Кейс-задачи

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.

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 основания для привлечения к ответственности владельцев компьютерного клуба? Должны ли нести уголовную ответственность родители мальчика?

Темы рефератов и докладов

DDoS-атаки и уголовно-правовое противодействие им
Основные правила эксплуатации компьютерной техники
Основные правила эксплуатации средств хранения данных
Основные правила эксплуатации компьютерных сетей

6. Посягательства на авторские и смежные права в компьютерных сетях

Глоссарий

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.

Соавтор — лицо или организация, создавшие произведение совместно с другим лицом или организацией.

Автор — творец чего-нибудь, составитель, создатель какого-нибудь научного, литературного, художественного произведения, проекта, изобретения.

Программа для ЭВМ — объективная форма представления совокупности данных и команд, предназначенных для

функционирования ЭВМ и других компьютерных устройств с целью получения определенного результата.

План

1. Уголовно-правовая характеристика посягательств на авторские и смежные права в компьютерных сетях
2. Способы совершения посягательств на авторские и смежные права в компьютерных сетях
3. Криминологическая характеристика посягательств на авторские и смежные права в компьютерных сетях
4. Особенности расследования посягательств на авторские и смежные права в компьютерных сетях

Рекомендуемая литература и электронные ресурсы

Близнец И. А. Авторское право и смежные права: учебник / под ред. И. А. Близнеца. М. : Проспект, 2010. 416 с.

Интеллектуальная собственность: охрана авторских и смежных прав [Текст] . Ч. II : Защита авторских и смежных прав. Государственная аккредитация коллективных управлений. Охрана авторского права программного обеспечения. М. : Фабрика АРТ, 2008. 96 с.

Авторское право // Википедия. Дата обновления: 23.02.2014. URL: http://ru.wikipedia.org/?oldid=42022902

Технические средства защиты авторских прав // Википедия. [2012—2014]. Дата обновления: 19.02.2012. URL:http://ru.wikipedia.org/?oldid=41927103

Нарушение авторского права // Википедия. Дата обновления: 16.02.2014. URL: http://ru.wikipedia.org/?oldid=41805542

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.

7. 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.

План

1. Уголовно-правовая характеристика хищений с использованием новых информационных технологий
2. Способы совершения хищений с использованием новых информационных технологий
3. Криминологическая характеристика хищений с использованием новых информационных технологий
4. Особенности расследования хищений с использованием новых информационных технологий

Рекомендуемая литература и электронные ресурсы

Лямин Л.В. Управление противодействием компьютерным мошенничествам // Управление в кредитной организации. 2011. № 1. С. 87 - 97.

Хилюта В.В. Уголовная ответственность за хищения с использованием компьютерной техники // Журнал российского права. 2014. № 3. С. 111 - 118.

Комаров А.А. Об уточнении понятия «компьютерное мошенничество» в свете законодательных инициатив Верховного Суда РФ // Юрист. 2013. № 17. С. 33 - 36.

Кейс-задачи

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

8. Распространение порнографии в компьютерных сетях

Глоссарий

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.

План

1. Уголовно-правовая характеристика распространения порнографии в компьютерных сетях
2. Криминологическая характеристика распространения порнографии в компьютерных сетях
3. Особенности расследования распространения порнографии в компьютерных сетях

Рекомендуемая литература и электронные ресурсы

Миллерова Е. Особенности уголовно-правовой оценки распространения и торговли порнографическими материалами // Уголовное право. 2011. № 5. С. 20 - 22.

Иванова А.А. Содержание криминалистической характеристики незаконного изготовления, распространения и оборота порнографических материалов или предметов // Российский следователь. 2011. № 11. С. 8 - 10.

Иванова А.А. Личность преступника как элемент криминалистической характеристики незаконного изготовления, распространения и оборота порнографических материалов или предметов // Российский следователь. 2011. № 5. С. 2 - 3.

Панфилов И.А. Порнография в сети Интернет и ее криминогенное значение // Российский следователь. 2013. № 23. С. 34 - 37.

Скобликов П.А. Криминализация оборота детской порнографии: системный анализ существующих законопроектов // Закон. 2013. № 3. С. 91 - 100.

Темы рефератов и докладов

Определение понятия «порнография»

Методы борьбы с распространением порнографии в Интернете

Законодательство стран мира о порнографии

3. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

3.1. Основная и дополнительная литература

Основная литература

1. Байбарин А. А. Уголовное право России. Общая часть [Электронный ресурс]: учебное пособие / А. А. Байбарин, А. А. Гребеньков, С. В. Шевелева; Юго-Зап. гос. ун-т. - Курск: [б. и.], 2013. - 428 с.
2. Загинайлов Ю. Н. Теория информационной безопасности и методология защиты информации [Текст]: учебное пособие / Ю. Н. Загинайлов. – М., Берлин: Директ-Медиа, 2015. – 253 с. // Режим доступа – http://biblioclub.ru/

Дополнительная литература

3. Байбарин А. А., Гребеньков А. А., Урда М. Н. Практикум по курсу «Уголовное право» [Текст]: учебное пособие / ЮЗГУ; под ред. А. А. Гребенькова. – Курск: ЮЗГУ, 2013. - 209 с.
4. Байбарин А. А., Гребеньков А. А., Урда М. Н. Практикум по курсу «Уголовное право» [Электронный ресурс]: учебное пособие / ЮЗГУ; под ред. А. А. Гребенькова. – Курск: ЮЗГУ, 2013. - 209 с.
5. Уголовный кодекс Российской Федерации: федер. закон Рос. Федерации от 13.06.1996 № 63-ФЗ. URL: http://www.consultant.ru/document/cons_doc_LAW_10699/
6. Уголовное право [Текст] : науч.-практ. журн. - Москва : Юрид. программы, 1996 - . - Выходит раз в два месяца. - ISSN 2071-5870.
7. Право интеллектуальной собственности: актуальные проблемы [Текст]: монография / С. М. Михайлов, Е. А. Моргунова, А. А. Рябов [и др.]; под общ. ред. Е. А. Моргуновой. М.: НОРМА, ИНФРА-М, 2014. 176 с.
8. Уголовное право Российской Федерации. Общая и Особенная части [Текст]: учебник / Т.Б. Басова, Е.В. Благов, П.В. Головненков [и др.]; под ред. А.И. Чучаева. - М.: КОНТРАКТ, ИНФРА-М, 2013. - 704 с.
9. Информационное право [Текст]: учебник для бакалавров / Министерство образования и науки Российской Федерации, Московский государственный юридический университет им. О. Е. Кутафина; отв. ред. д-р юрид. наук И. М. Рассолов. - М.: Проспект, 2013. - 352 с.

3.2. Перечень методических указаний

1. Методические указания для самостоятельной работы по изучению дисциплины «Преступность в сфере высоких технологий» для студентов всех форм обучения специальности 40.05.02 «Правоохранительная деятельность» / сост. М. И. Синяева, А. А. Байбарин, А. А. Гребеньков: Юго-Зап. гос. ун-т. Курск, 2016. 26 с.
2. Методические указания по подготовке к практическим занятиям по дисциплине «Преступность в сфере высоких технологий» для студентов всех форм обучения специальности 40.05.02 «Правоохранительная деятельность» / сост. М. И. Синяева, А. А. Байбарин, А. А. Гребеньков: Юго-Зап. гос. ун-т. Курск, 2016.

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

1. http://www.cyberpol.ru/ – компьютерная преступность и борьба с ней.
2. http://www.crime-research.ru/ –Центр исследования компьютерной преступности.
3. Электронная библиотека elibrary.ru.
4. Электронная библиотека cyberleninka.ru.
5. Сайт кафедры уголовного права: http://www.swsu.ru/structura/up/uf/kup/index.php.
6. СПС «Консультант+: Высшая школа».
7. СПС «ГАРАНТ-Студент».
8. Программа для ЭВМ «Программа для формирования бланков тестовых заданий», авторы: Калашникова А. А., Гребеньков А. А.
9. Программа для ЭВМ «Программа для осуществления тестового контроля знаний студентов» , авторы: Калашникова А. А., Гребеньков А. А.