

УДК 343.2/.7

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

Рецензент

Доктор юридических наук, доцент И.Б. Лагутин

Преступность в сфере высоких технологий: методические рекомендации по подготовке к практическим занятиям для студентов всех форм обучения специальности 40.05.02 Правоохранительная деятельность / Юго-Западный гос. ун-т; сост.: А. А. Байбарин, А. А. Гребеньков, М. И. Синяева. Курск, 2017. 34 с.

Излагаются методические рекомендации по подготовке к практическим занятиям по дисциплине «Преступность в сфере высоких технологий».

Даются рекомендации относительно общих принципов подготовки к практическим занятиям, правила оформления рефератов, приводятся планы занятий, литература, темы рефератов и контрольные вопросы. Методические рекомендации соответствуют требованиям программы дисциплины «Преступность в сфере высоких технологий».

Предназначены для студентов всех форм обучения специальности 40.05.02 Правоохранительная деятельность

Текст печатается в авторской редакции

Подписано в печать 15.12.17. Формат 60x84 1/16.

Усл. печ. л.2,3. Уч.-изд. л. 2,1. Тираж 50 экз. Заказ 3677. Бесплатно.

Юго-Западный государственный университет.

305040, г. Курск, ул. 50 лет Октября, 94

Оглавление

Введение	4
Методические указания по выполнению рефератов	5
Основная учебная литература для подготовки ко всем занятиям	12
Планы семинарских занятий	13
Приложение 1	24
Приложение 2	25

Введение

Семинарские занятия по дисциплине «Преступность в сфере высоких технологий» ориентируют студентов на всестороннее и системное изучение основных институтов уголовного права, его принципов и категорий, с помощью которых осмысливаются и решаются проблемы формирования и вывода специфических понятий, суждений, умозаключений, реализуется аргументационный процесс. Кроме того, рассматриваются специфические вопросы, связанные с противодействием преступности в данной сфере.

Изучение дисциплины «Преступность в сфере высоких технологий» студентами университета осуществляется в течение одного семестра. Структурно курс состоит из 9 тем. Важнейшим условием успешного изучения курса является систематическая самостоятельная работа с рекомендованной литературой. Студент должен овладеть понятийным аппаратом дисциплины, знать и понимать основные категории уголовного права, основные особенности противодействия преступлениям в сфере высоких технологий.

Большое место в успешном овладении дисциплиной отводится семинарским занятиям. Семинар — это средство коллективного творческого раздумья, школа творческого мышления, столь необходимых будущему специалисту в его практической деятельности. Семинарское занятие требует от студента глубокого самостоятельного изучения рекомендованных источников и литературы по теме занятия.

Рекомендуется следующий алгоритм подготовки к семинару.

1. Внимательное изучение плана семинарского занятия, списка рекомендованных источников и литературы, методических рекомендаций преподавателя.

2. Изучение программы дисциплины с целью уяснения требований к объему и содержанию знаний по изучаемой теме.

3. Изучение и доработка конспекта лекций, прочитанных преподавателем по темам, выносимым на семинарское занятие.

4. Изучение вопросов темы по учебникам и основным рекомендованным пособиям.

5. Изучение дополнительной литературы.

При этом перед собой нужно иметь соответствующие статьи УК РФ, которые неоднократно перечитывать. Рекомендуется вести кон-

спект прочитанного, записывать научные определения, краткие формулировки, сопоставлять различные точки зрения. Следует продумать свой ответ по вопросам, составить краткий план ответа по каждому вопросу.

От студента не требуется изучения всей рекомендуемой литературы. Количество и объем изучаемых работ зависит от конкретной задачи: подготовки доклада, реферата, фиксированного выступления и т.д.

При ответе не следует повторять сказанное предыдущими выступающими, повторять самому, злоупотреблять временем другим способом. Пользоваться при ответе учебниками, лекциями, УК можно лишь с разрешения преподавателя.

Обязательно наличие Уголовного кодекса РФ в последней редакции на практических занятиях, методических пособий кафедры по дисциплине. Рекомендуется выполнять творческие задания и решать задачи письменно в отдельной тетради. Рекомендуется самостоятельно решать задачи и тесты по дисциплине.

Методические указания по выполнению рефератов

Планы семинарских занятий предусматривают самостоятельное выполнение студентом рефератов. Тема реферата назначается преподавателем. Студент может сам выбрать тему, согласовав её с преподавателем.

Перед выполнением реферата студент должен внимательно ознакомиться с рекомендуемой учебной и научной литературой, а также проанализировать действующее российское законодательство в части проблематики работы.

Подбор источников для написания реферата производится студентом самостоятельно с учётом рекомендаций преподавателя и данных методических указаний. Первым этапом подбора источника является составление списка источников, с которыми необходимо будет ознакомиться, с использованием систем каталогизации и поиска библиографической информации.

При составлении списка источников рекомендуется выписывать библиографическую информацию в полном объёме, чтобы впоследствии этот список можно было использовать при оформлении списка использованной литературы.

Кроме того, студенту перед началом непосредственного ознакомления с источниками рекомендуется изучить конспект лекций по выбранной теме (при его наличии) или соответствующие разделы учебной литературы. Это необходимо для того, чтобы составить представление об основных теоретических и практических проблемах изучаемой темы, а также её границах.

Получение текстов источников по составленному списку может производиться на абонементных и в читальных залах библиотек, из баз данных справочных правовых систем. Отдельные источники могут быть доступны в сети Интернет. Получать тексты нормативных документов предпочтительно из справочных правовых систем, поскольку в них представлена актуальная редакция документа. Целесообразным является копирование источников небольшого объёма для облегчения повторного доступа к их тексту.

При изучении источников рекомендуется делать выписки, содержащие отдельные цитаты или выдержки, изложенные собственными словами, по вопросам, относящимся к рассматриваемой теме. Кроме того, выписки могут содержать возникающие в ходе чтения суждения, вопросы, которые необходимо дополнительно рассмотреть или по которым необходима консультация преподавателя. В случае расхождения мнения студента и мнения автора рассматриваемой работы также рекомендуется отметить это расхождение, возникающие доводы и аргументы в обоснование своего мнения.

Выписки рекомендуется систематизировать (по разделам работы или определённым проблемам), используя для этого пометки или отдельные папки.

Подготовительный этап написания реферата включает в себя чтение статей в периодической печати.

После проделанной работы студенту рекомендуется составить план реферата. План должен охватывать все вопросы выбранной темы.

Ответы на поставленные вопросы должны полностью раскрывать их содержание. Положительно влияет на оценку реферата рассмотрение студентом научных проблем по тематике работы, анализ направлений совершенствования действующего уголовного законодательства.

Реферат должен быть написан с соблюдением правил орфографии и пунктуации, с правильным употреблением юридической терминологии, соответствующим значению терминов и контексту, в котором они употребляются. При этом следует избегать усложнения языка работы, не использовать без необходимости громоздкие языковые конструкции. Автор работы должен быть способен дать пояснения относительно значения любого из использованных в реферате специальных терминов, поэтому следует избегать использования слов, значение которых является неясным.

В рефератах недопустимо употребление жаргонных слов и выражений. Автор работы должен с уважением относиться к мнениям других учёных и специалистов. Своё несогласие с их мнением следует излагать максимально корректно, обращая особое внимание на полноту и точность аргументации.

Следует избегать изложения очевидных истин (например, «необходимо стремиться к сокращению преступности», «уголовное право является одной из важнейших отраслей права» и т.п.), бездоказательных утверждений, штампов, излишне «громких», эмоциональных, наполненных пафосом предложений. Изложение рекомендуется вести безлично («считается»), в третьем лице («автор работы считает») или с использованием личного местоимения «мы» («мы считаем»). Использование местоимения «я» не отвечает требованиям к языку реферата. В реферате допустимо использование лишь общепринятых сокращений («УК РФ», «и т.д.», «и т.п.»).

Материал реферата излагается своими словами. При этом все важные положения должны быть подтверждены ссылками на источники, в том числе нормативные акты. Содержание источников может цитироваться или пересказываться. Цитирование всегда осуществляется дословно. Цитата берётся в кавычки, если в ней делаются пропуски, на их месте ставится многоточие. Недопустимо делать пропуски, искажающие смысл исходного текста. При цитировании должны передаваться также шрифтовые выделения: курсив, жирный шрифт.

Реферат должен содержать: титульный лист по установленной форме (приводится в приложении), оглавление, изложение содержания темы, список литературы.

Объём реферата не должен превышать 10-15 страниц машинописного текста. При компьютерном выполнении реферата он оформляется по следующим параметрам страниц: сверху 2 см., внизу 2 см., слева 3 см., справа 1 см. Шрифт – Times New Roman, 14 пт, межстрочный интервал – 1,5, сноски – внизу каждой страниц (начинаются всегда с «1»).

При использовании в работе текста и заимствовании фактических сведений из научных работ других авторов, законодательных актов и иных источников необходимо указание на этот источник в подстрочной библиографической ссылке.

Ссылки на статьи Конституции РФ, Основ законодательства и кодексов даются только в тексте работы с указанием части (пункта) и статьи нормативного акта (источник публикации не указывается).

Для прочих нормативных актов в тексте указывается часть (пункт), статья и полное название нормативного акта (например, ФЗ «Об оружии»). Остальные данные (дата принятия, редакция, источник официального опубликования) приводятся в подстрочной библиографической ссылке (сноске).

Ссылки на иные источники оформляются так же, как и в списке использованной литературы, однако указывается не общее число страниц (при наличии), а конкретная страница, на которой находится утверждение, подтверждаемое ссылкой.

Список использованной литературы располагается после заключения работы, но перед приложениями, имеет нумерованный заголовок «Список использованной литературы». В список литературы должны быть включены все использовавшиеся при написании работы нормативные акты и прочие источники. Не допускается включение в список литературы источников, ссылки на которые отсутствуют в тексте работы, а также работ, непосредственное ознакомление с которыми не производилось. В списке литературы используется сплошная нумерация источников, без выделения каких-либо рубрик.

Должен соблюдаться следующий порядок расположения источников в списке:

1. Нормативно-правовые акты, материалы судебной практики в порядке убывания юридической силы:
 - а) международные правовые акты;

- б) Конституция РФ;
- с) федеральные конституционные законы;
- д) кодексы;
- е) федеральные законы;
- ф) постановления Конституционного суда РФ;
- г) указы и распоряжения Президента РФ;
- h) постановления и распоряжения Правительства РФ;
- и) приказы и инструкции федеральных органов исполнительной власти;
- j) конституции и уставы субъектов РФ, акты органов законодательной власти субъектов РФ;
- к) акты органов исполнительной власти субъектов РФ;
- l) акты муниципальных органов власти;
- м) нормативные акты Верховного Суда РФ;
- п) материалы судебной и следственной практики;
- о) нормативно-правовые акты, утратившие юридическую силу, нормативно-правовые акты иностранных государств;
- р) проекты нормативно-правовых актов.

Внутри каждой из этих групп нормативные акты располагаются в порядке убывания даты их принятия.

2. Все литературные источники, включая учебную литературу, комментарии законодательства, монографии, диссертации, журнальные статьи и т.д.

Литературные источники располагаются по фамилиям авторов (заглавию в случае коллективных работ) в алфавитном порядке. Не допускается группировка по типу издания.

При оформлении списка литературы следует руководствоваться следующими правилами, составленными на основе ГОСТ Р 7.0.5-2008 «Библиографическая ссылка. Общие требования и правила составления»¹.

Оформление описания нормативных актов:

а) при использовании специальных изданий нормативных актов (Конституции, кодексов):

Уголовный кодекс Российской Федерации: текст с изменениями и дополнениями на 1 января 2011 года. М.: Эксмо, 2011. 208 с.

б) при использовании акта официального опубликования:

¹ https://secure.wikimedia.org/wikisource/ru/wiki/ГОСТ_Р_7.0.5—2008

Об оружии: федеральный закон РФ от 13.12.1996 г. № 150-ФЗ (ред. от 31.05.2010) // Российская газета. 1996. № 241.

в) при использовании сборников законов РФ:

Об оружии: федеральный закон РФ от 13.12.1996 г. № 150-ФЗ (ред. от 31.05.2010) // Сборник законов РФ. М.: «Кодекс», 2010. С. 12-32.

г) при использовании электронных справочных правовых систем:

Об утверждении положения о награждении именованным оружием: Приказ ГТК РФ от 30.06.2008 № 446 (ред. от 23.09.2002) // КонсультантПлюс [Электронный ресурс]. М., 2011.

д) при использовании интернет-ресурсов:

Статут Международного Суда от 26.06.1945 г. URL: <http://www.un.org/russian/document/basicdoc/statut.htm> (дата обращения 10.01.2011).

ВАЖНО: описание нормативных документов имеет следующую структуру:

Название документа: вид документа от дата принятия номер: редакция // источник.

Использование интернет-ресурсов допускается лишь в тех случаях, когда их можно идентифицировать с использованием универсального интернет-адреса. Также рекомендуется использовать только официальные интернет-ресурсы с открытым доступом.

Описание материалов юридической практики оформляется следующим образом:

О судебной практике по делам об убийстве (ст. 105 УК РФ): постановление Пленума Верховного Суда РФ от 27.01.1999 № 1 (ред. от 03.12.2009) // КонсультантПлюс [Электронный ресурс]. М., 2011.

ВАЖНО: в список литературы не записываются материалы конкретных уголовных дел, как опубликованные в Бюллетене Верховного суда и иных изданиях, так и не публиковавшиеся (архивные). На них даются лишь подстрочные ссылки:

¹ Постановление Президиума Ярославского областного суда от 08.12.2010 № 44-у-207-2010 // КонсультантПлюс [Электронный ресурс]. М., 2011.

² Приговор Курского областного суда от 25.08.2010 в отношении подсудимых Русина В.С., Лисовского Г.А. URL:

http://oblsud.krs.sudrf.ru/modules.php?name=bsr&op=show_text&srv_num=1&id=46400001012310916324981000096568 (дата обращения 10.01.2011)

³. Приговор Курского областного суда от 25.08.2010 по делу № 46-у-109-2010 // Архив Курского областного суда.

Описания монографий оформляются следующим образом:

а) один, два или три автора:

Бородин С. В. Ответственность за убийство: квалификация и наказание по российскому праву. М.: Юрист, 1994. 216 с.

Ломброзо Ч., Ферреро Г. Женщина преступница и проститутка. Ставрополь: Издательство А. А. Торбы, 1991. 224 с.

б) четыре и более авторов

Российское уголовное право. Общая часть / Ю. В. Баулин и др.; отв. ред. В. С. Комиссаров. СПб.: Питер, 2005. 560 с.

Комментарий к Уголовному кодексу РФ (постатейный). Изд. 3-е, доп. и испр. / Г. Н. Борзенков и др.; под ред. В. М. Лебедева // КонсультантПлюс. М., 2011.

в) в многотомных изданиях номер тома и подзаголовков тома, если он имеется, указываются после года издания, но до общего числа страниц:

Курс советского уголовного права (Часть Особенная) / Н. А. Беляев и др.; отв. ред. Н. А. Беляев. Л.: Изд-во Ленинградского Университета, 1978. Т. 4. 558 с.

Описания статей из сборников научных трудов и материалов конференций даются следующим образом:

Шабунина А. Н. Изменения в Уголовный кодекс Российской Федерации: проблемы квалификации // Сборник материалов межвузовской научно-практической конференции «Совершенствование законодательства: вчера, сегодня, завтра», посвящённой 40-летию Курского государственного технического университета / Курский государственный технический университет; отв. ред. М. В. Мозгов. Курск, 2004. С. 239-243.

Описания статей из журналов даются в следующем оформлении:

Звечаровский И. О концепции развития уголовного законодательства России // Уголовное право. 2005. № 3. С. 32-34.

Гонтарь Д., Гребёнкин Ф. Уголовная ответственность за неисполнение приговора суда, решения суда или иного судебного акта // Уголовное право. 2005. № 3. С. 24-27.

Допускается не указывать страницы, если статья используется в электронной версии (СПС Консультант+, ГАРАНТ).

Реферат должен быть сдан для проверки преподавателем. Основные его положения студент должен рассказать на занятии. При этом не рекомендуется зачитывать реферат.

Основная учебная литература для подготовки ко всем занятиям

1. Конституция РФ.
2. Уголовный кодекс РФ.
3. Бачило И. Л. Информационное право [Текст] : учебник / И. Л. Бачило. - М. : Юрайт, 2009. - 454 с. - (Магистр права). - ISBN 978-5-9692-0462-1 : 52р.
4. Городов О. А. Информационное право [Текст] : учебник / Олег Александрович Городов. - М. : Проспект, 2009. - 256 с. - ISBN 978-5-392-00411-9 : 189р.
5. Уголовное право России. Части общая и особенная [Текст] : учебник / под ред. А. В. Бриллиантова. - М. : Проспект, 2010. - 1232 с. - ISBN 978-5-392-00763-9 : 496р.
6. Уголовное право России. Части общая и особенная [Текст] : курс лекций / под ред. д-ра юр. наук, проф. А. И. Рарога. - 2-е изд., перераб. и доп. - М. : Проспект, 2009. - 496 с. - ISBN 978-5-482-01952-8 : 296р.

Планы семинарских занятий

1. Понятие и общая характеристика преступлений в сфере высоких технологий

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/> (дата обращения: 04.03.14).

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

Контрольные вопросы

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?

2. Компьютерная информация как объект уголовно-правовой охраны

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., Сенев 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

Контрольные вопросы

Каковы основные признаки информации?

В чём отличие информации от материи и энергии?

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?

3. Неправомерный доступ к компьютерной информации

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. унта, 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

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.

Темы рефератов и докладов

Основные методы защиты от неправомерного доступа

Личность преступника, совершающего неправомерный доступ к компьютерной информации.

Понятие «компьютерная информация»

Контрольные вопросы

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?

4. Создание, использование и распространение вредоносных компьютерных программ

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>

История вредоносных программ. URL: <http://www.securelist.com/ru/threats/detect?chapter=34>

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.

Темы рефератов и докладов

История вредоносных программ.

Ботнеты.

Вредоносные программы как средство информационной войны.

Контрольные вопросы

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?

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

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.

Сулопаров 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.

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
 Контрольные вопросы

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?

6. Посягательства на авторские и смежные права в компьютерных сетях

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..
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.

Контрольные вопросы

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?

7. Хищения с использованием новых информационных технологий

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.

Темы рефератов и докладов

Хищения с использованием банковских платёжных карт

История использования компьютеров для совершения хищений

Компьютерное вымогательство

Контрольные вопросы

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?

8. *Распространение порнографии в компьютерных сетях*

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

Контрольные вопросы

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?

9. Высокотехнологичный терроризм и экстремизм

План

1. Уголовно-правовая характеристика преступлений террористического и экстремистского характера, совершаемых с использованием новых информационных технологий
2. Криминологическая характеристика преступлений террористического и экстремистского характера, совершаемых с использованием новых информационных технологий

3. Особенности расследования преступлений террористического и экстремистского характера, совершаемых с использованием новых информационных технологий

Рекомендуемая литература и электронные ресурсы

Незнамов А.В. Территориальная подсудность дел о признании экстремистскими информационных материалов, размещенных в сети Интернет // Арбитражный и гражданский процесс. 2010. № 5. С. 12 - 16.

Денисов Ю.Д. Противодействие экстремизму в сети Интернет // Законность. 2009. № 6.

Информационное общество: Информационные войны. Информационное управление. Информационная безопасность / Под ред. М. А. Вуса. СПб.: СПб. ун-т, 1999. 212 с.

Касьяненко М.А. Правовые проблемы при использовании Интернета в транснациональном терроризме // Информационное право. 2012. № 1. С. 21 - 25.

Паненков А.А. Предложения по оптимизации борьбы с использованием сети Интернет в террористических целях // Правовые вопросы связи. 2011. № 2. С. 15 - 21.

Темы рефератов и докладов

Информационная война

Блокирование интернет-ресурсов экстремистской направленности

Понятие «социальная группа»

Контрольные вопросы

Как высокие технологии могут использоваться для совершения диверсий и террористических актов?

Как высокие технологии содействуют экстремистской деятельности?

Каковы основные меры государственной политики РФ в области противодействия терроризму и экстремизму?

Приложение 1. Образец оформления титульного листа реферата

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

Кафедра уголовного права

РЕФЕРАТ

по дисциплине «Преступность в сфере высоких технологий »
на тему «Название темы»

Специальность 40.05.02 Правоохранительная деятельность

Автор работы: _____

подпись, дата

Группа: ПД

Проверил: _____

подпись, дата

Оценка: _____

Курск, 20__ г.

Приложение 2. Примерный перечень вопросов для подготовки к зачёту

1. Понятие преступлений в сфере высоких технологий
 - а) понятие киберпреступности
 - б) виды преступлений в сфере высоких технологий
2. Общая характеристика преступлений в сфере высоких технологий
 - а) особенности личности «киберпреступников»
 - б) источники правового регулирования
3. Компьютерная информация как объект уголовно-правовой охраны
 - а) понятие «информация»
 - б) понятие «компьютерная информация»
4. Общие принципы информационной безопасности и защиты компьютерной информации в Российской Федерации
 - а) понятие информационной безопасности и защиты информации
 - б) принципы информационной безопасности и защиты информации
5. Объект преступлений в сфере компьютерной информации
 - а) общие принципы обеспечения безопасности в уголовном праве
 - б) безопасность компьютерной информации как видовой объект преступления
6. Объективные признаки неправомерного доступа к компьютерной информации
 - а) объект неправомерного доступа к компьютерной информации
 - б) объективная сторона неправомерного доступа к компьютерной информации
7. Субъективные признаки неправомерного доступа к компьютерной информации
 - а) субъект неправомерного доступа к компьютерной информации
 - б) субъективная сторона неправомерного доступа к компьютерной информации
8. Квалифицирующие признаки неправомерного доступа к компьютерной информации
 - а) неправомерный доступ к компьютерной информации, причинивший крупный ущерб или совершенный из корыстной заинтересованности
 - б) неправомерный доступ к компьютерной информации, совершённый группой лиц по предварительному сговору или организованной

группой либо лицом с использованием своего служебного положения, а также повлекший тяжкие последствия или создавший угрозу их наступления

9. Способы совершения неправомерного доступа к компьютерной информации

а) технические способы неправомерного доступа к компьютерной информации

б) социальные способы неправомерного доступа к компьютерной информации

10. Криминологическая характеристика неправомерного доступа к компьютерной информации

а) состояние данного вида преступности

б) личность лиц, совершающих неправомерный доступ

11. Профилактика неправомерного доступа к компьютерной информации

а) причины и условия неправомерного доступа к компьютерной информации

б) предупреждение неправомерного доступа к компьютерной информации

12. Особенности расследования преступлений, связанных с неправомерным доступом к компьютерной информации

а) технические средства фиксации следов неправомерного доступа к компьютерной информации

б) основные следственные действия при расследовании неправомерного доступа к компьютерной информации

13. Объективные признаки создания, использования и распространения вредоносных компьютерных программ

а) объект создания, использования и распространения вредоносных компьютерных программ

б) объективная сторона создания, использования и распространения вредоносных компьютерных программ

14. Субъективные признаки создания, использования и распространения вредоносных компьютерных программ

а) субъект создания, использования и распространения вредоносных компьютерных программ

б) субъективная сторона создания, использования и распространения вредоносных компьютерных программ

15. Квалифицирующие признаки создания, использования и распространения вредоносных компьютерных программ

а) совершение деяния группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, либо причинившее крупный ущерб или совершенное из корыстной заинтересованности

б) совершение деяние, повлекшее тяжкие последствия или создавший угрозу их наступления

16. Способы совершения создания, использования и распространения вредоносных компьютерных программ

а) современные разновидности вредоносных программ

б) способы распространения компьютерных программ

17. Криминологическая характеристика создания, использования и распространения вредоносных компьютерных программ

а) состояние данного вида преступности

б) личность лиц, совершающих создание, использование и распространение вредоносных компьютерных программ

18. Профилактика создания, использования и распространения вредоносных компьютерных программ

а) причины и условия создания, использования и распространения вредоносных компьютерных программ

б) предупреждение создания, использования и распространения вредоносных компьютерных программ

19. Особенности расследования преступлений, связанных с созданием, использованием и распространением вредоносных компьютерных программ

а) технические средства фиксации следов создания, использования и распространения вредоносных компьютерных программ

б) основные следственные действия при расследовании создания, использования и распространения вредоносных компьютерных программ

20. Объективные признаки нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

а) объект нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

б) объективная сторона нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

21. Субъективные признаки нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

а) субъект нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

б) субъективная сторона нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

22. Криминологическая характеристика нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

а) состояние данного вида преступности

б) личность лиц, совершающих нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

23. Профилактика нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

а) причины и условия нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

б) предупреждение нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

24. Особенности расследования нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

а) технические средства фиксации следов нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

б) основные следственные действия при расследовании нарушения правил эксплуатации средств хранения, обработки или передачи

компьютерной информации и информационно-телекоммуникационных сетей

25. Объективные признаки нарушения авторских прав в компьютерных сетях

- а) объект нарушения авторских прав в компьютерных сетях
- б) объективная сторона нарушения авторских прав в компьютерных сетях

26. Субъективные признаки нарушения авторских прав в компьютерных сетях

- а) субъект нарушения авторских прав в компьютерных сетях
- б) субъективная сторона нарушения авторских прав в компьютерных сетях

27. Способы совершения нарушения авторских прав в компьютерных сетях

- а) способы индивидуального нарушения авторских прав
- б) способы нарушения авторских прав в состав пиринговых сетей

28. Криминологическая характеристика нарушения авторских прав в компьютерных сетях

- а) состояние данного вида преступности
- б) личность лиц, совершающих нарушения авторских прав в компьютерных сетях

29. Профилактика нарушения авторских прав в компьютерных сетях

- а) причины и условия нарушения авторских прав в компьютерных сетях
- б) предупреждение нарушения авторских прав в компьютерных сетях

30. Особенности расследования нарушения авторских прав в компьютерных сетях

- а) технические средства фиксации следов нарушения авторских прав в компьютерных сетях
- б) основные следственные действия при расследовании нарушения авторских прав в компьютерных сетях

31. Объективные признаки хищений с использованием новых информационных технологий

- а) объект хищений с использованием новых информационных технологий
- б) объективная сторона хищений с использованием новых информационных технологий

32. Субъективные признаки хищений с использованием новых информационных технологий

а) субъект хищений с использованием новых информационных технологий

б) субъективная сторона хищений с использованием новых информационных технологий

33. Способы совершения хищений с использованием новых информационных технологий

а) способы совершения мошенничеств с использованием новых информационных технологий

б) способы совершения иных хищений с использованием новых информационных технологий

34. Криминологическая характеристика хищений с использованием новых информационных технологий

а) состояние данного вида преступности

б) личность лиц, совершающих хищения с использованием новых информационных технологий

35. Профилактика хищений с использованием новых информационных технологий

а) причины и условия хищений с использованием новых информационных технологий

б) предупреждение хищений с использованием новых информационных технологий

36. Особенности расследования хищений с использованием новых информационных технологий

а) технические средства фиксации следов хищений с использованием новых информационных технологий

б) основные следственные действия при расследовании хищений с использованием новых информационных технологий

37. Объективные признаки распространения порнографии в компьютерных сетях

а) объект распространения порнографии в компьютерных сетях

б) объективная сторона распространения порнографии в компьютерных сетях

38. Субъективные признаки распространения порнографии в компьютерных сетях

а) субъект распространения порнографии в компьютерных сетях

б) субъективная сторона распространения порнографии в компьютерных сетях

40. Криминологическая характеристика распространения порнографии в компьютерных сетях

а) состояние распространения порнографии в компьютерных сетях

б) личность лиц, совершающих распространение порнографии в компьютерных сетях

41. Профилактика распространения порнографии в компьютерных сетях

а) причины и условия распространения порнографии в компьютерных сетях

б) предупреждение распространения порнографии в компьютерных сетях

42. Особенности расследования распространения порнографии в компьютерных сетях

а) технические средства фиксации следов распространения порнографии в компьютерных сетях

б) основные следственные действия при расследовании распространения порнографии в компьютерных сетях

43. Общая характеристика высокотехнологичного терроризма и экстремизма

а) общая характеристика высокотехнологичного терроризма

б) общая характеристика высокотехнологичного экстремизма

44. Уголовно-правовая характеристика преступлений террористического и экстремистского характера, совершаемых с использованием новых информационных технологий

а) уголовно-правовая характеристика преступлений террористического характера, совершаемых с использованием новых информационных технологий

б) уголовно-правовая характеристика преступлений экстремистского характера, совершаемых с использованием новых информационных технологий

45. Криминологическая характеристика преступлений террористического и экстремистского характера, совершаемых с использованием новых информационных технологий

а) криминологическая характеристика преступлений террористического характера, совершаемых с использованием новых информационных технологий

б) криминологическая характеристика преступлений экстремистского характера, совершаемых с использованием новых информационных технологий

46. Особенности расследования преступлений террористического и экстремистского характера, совершаемых с использованием новых информационных технологий

а) особенности расследования преступлений террористического характера, совершаемых с использованием новых информационных технологий

б) особенности расследования преступлений экстремистского характера, совершаемых с использованием новых информационных технологий