Учреждение образования
«Гомельский государственный университет
имени Франциска Скорины»

С. Л. ЕМЕЛЬЯНОВ, О. Г. ШЛЯХТОВА

УГОЛОВНОЕ ПРАВО (ОСОБЕННАЯ ЧАСТЬ)

ПРЕСТУПЛЕНИЯ ПРОТИВ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Практическое пособие

для студентов специальности
1-24 01 02 «Правоведение»

Гомель
ГГУ им. Ф. Скорины
2024

УДК 343.45:004.9(076)
ББК 67.408.135я73
Е601

Рецензенты:

кандидат юридических наук Т. П. Афонченко,
кандидат юридических наук И. Н. Цыкунова

Рекомендовано к изданию научно-методическим советом учреждения образования «Гомельский государственный университет имени Франциска Скорины»

Емельянов, С. Л.

Е601 Уголовное право (Особенная часть). Преступления против компьютерной безопасности : практическое пособие / С. Л. Емельянов, О. Г. Шляхтова ; Гомельский гос. ун-т им. Ф. Скорины. – Гомель : ГГУ им. Ф. Скорины, 2024. – 27 с.
ISBN 978-985-32-0025-6

Практическое пособие включает перечни вопросов для самоконтроля, задач, а также тем для рефератов и литературу. Издание предназначено для закрепления основных правовых понятий и категорий в сфере компьютерной безопасности, а также для контроля и самоконтроля знаний студентов.

Адресовано студентам специальностей 1-24 01 02 «Правоведение».

УДК 343.45:004.9(076)
ББК 67.408.135я73

ISBN 978-985-32-0025-6

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

В нашей стране и за рубежом ежегодно наблюдается рост преступлений против компьютерной безопасности. Сегодня мы можем говорить о переходе «традиционных» преступлений в виртуальное пространство. Актуальность данного вопроса обусловлена двумя взаимосвязанными явлениями.

Во-первых, повсеместное внедрение высоких технологий в нашу профессиональную и повседневную жизнь закономерно привело к тому, что информационная безопасность стала не просто важным направлением деятельности заинтересованных субъектов, а необходимым условием обеспечения всех сфер национальной безопасности, политических, экономических, социальных и иных интересов общества и государства. В то время когда у нас принят курс на выстраивание «IT-страны», создание безопасных условий в области информатизации положительно сказывается и на инвестиционной привлекательности государства.

Во-вторых, возможности данных технологий – анонимность, трансграничность, широкий охват аудитории – используются злоумышленниками для совершения весьма обширного круга противоправных деяний: от несанкционированного доступа до незаконного оборота наркотиков и мошенничества.

Цель подготовки и издания практического пособия – сформировать у студентов системные знания, умения и навыки по уголовно-правовому, криминологическому и криминалистическому анализу преступлений, совершенных с использованием компьютеров, информационно-коммуникационных технологий или сетей (киберпреступлений), их квалификации с учетом требований действующего законодательства, криминалистических методов их выявления и расследования.

Достижение указанной цели предполагает решение следующих задач:

– расширить знания обучающихся в области основных понятий и категорий уголовно-правовой политики в области информационной и компьютерной безопасности;

– развить навыки криминологического анализа киберпреступности, ее показателей, состояния и динамики, причинного комплекса, особенностей личности преступников в сфере информационной безопасности, системы мер предупреждения данного вида преступлений;

– расширить знания современных криминалистических приемов исследования, фиксации и защиты электронной информации при расследовании компьютерных преступлений.

Представленное практическое пособие является частью учебно-методического обеспечения по дисциплине «Уголовное право (Особенная часть)», содержит в себе алгоритмы подготовки и ведения практических занятий по разделу «Преступления против компьютерной безопасности».

Издание предназначено для самостоятельной работы студентов и проведения практических занятий на юридическом и других факультетах высших учебных заведений, учебными планами которых предусмотрено изучение дисциплины «Уголовное право (Особенная часть)».

1. ПОНЯТИЕ ПРЕСТУПЛЕНИЙ ПРОТИВ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

1. Понятие, содержание и значение компьютерной безопасности.
2. Роль и значение информации как признака состава преступления в зависимости от ее формы и содержания.
3. Понятие преступлений против компьютерной безопасности.
4. Виды и источники угроз компьютерной безопасности.
5. Субъекты обеспечения компьютерной безопасности.

Вопросы для самоконтроля

1. Дайте определение компьютерной безопасности.
2. Дайте правовую характеристику преступлению против компьютерной безопасности.
3. Назовите основные источники права Республики Беларусь в области обеспечения компьютерной безопасности.
4. Охарактеризуйте субъектов информационной безопасности.
5. Дайте определение понятию источников угроз компьютерной безопасности.
6. Назовите основные виды угроз компьютерной безопасности.

Практические задания

Задача 1. Серегин взломал компьютерную базу данных потерпевшей Ахтямовой, проникнув на ее страничку в сайте «В контакте», обидевшись на то, что девушка не желала продолжить с ним виртуальную переписку. Решив отомстить, он украл и поменял пароли от ее электронного почтового ящика и анкеты на сайте. В результате девушка не могла попасть на свою страницу. Серегин вступал от ее имени в эротическую переписку с мужчинами, а также разместил фотографии порнографического содержания.

Есть ли в действиях Серегина признаки какого-либо состава преступления?

Задача 2. Студент заочного отделения Шатурин решил использовать компьютер из компьютерного класса университета для оформления контрольных и курсовых работ. Без разрешения деканата факультета он проник в класс и стал работать на компьютере. Из-за крайне по-

верхностных знаний и навыков работы на компьютере произошли сбои в работе машины, что привело в дальнейшем к отключению модема – одного из элементов компьютерной системы.

Подлежит ли уголовной ответственности Шатурин?

Задача 3. Аспирант университета Хохлов занимался исследовательской работой по компьютерной «вирусологии». Целью работы было выяснение масштаба глобальной сетевой инфраструктуры. В результате ошибки в механизме размножения вирусы («сетевые черви») проникли в университетскую компьютерную сеть и уничтожили информацию, содержащуюся в компьютерах факультетов и подразделений. В результате этого были полностью уничтожены списки сотрудников университета, расчеты бухгалтерии по зарплате, повреждены материалы научно-исследовательской работы, в том числе «пропали» две кандидатские и одна докторская диссертации.

Решите вопрос о правомерности действий Хохлова. В чем заключается субъективная сторона преступлений в сфере компьютерной информации?

Задача 4. Примерно в мае–июне 2015 г. Н., будучи осведомленным о возможности проведения оператором сотовой связи «Х» процедуры замены клиентам сим-карт при их утере или неисправности, имея корыстную заинтересованность, принял решение осуществлять хищения денежных средств с лицевых счетов абонентов указанного оператора связи путем неправомерного доступа к данным счетам с использованием сим-карт, полученных при их несанкционированной замене.

Для реализации своего преступного умысла Н. подыскал сотрудника «Х» К., занимающего в указанной компании должность специалиста обслуживания и продаж и осуществляющего в силу своих должностных обязанностей обработку персональных данных абонентов, и вступил с ним в преступный сговор, направленный на осуществление совместного неправомерного доступа к персональным данным абонентов указанного оператора связи с последующей несанкционированной их модификацией с целью хищения денежных средств, находящихся на лицевых счетах.

Полученные в ходе осуществления описанной «схемы» денежные средства, похищенные с лицевых счетов абонентов «Х», Н. и К. делили между собой поровну.

Дайте уголовно-правовую характеристику данному деянию.

Задача 5. Студент одного из ВУЗов Левин, хорошо владея компьютерной техникой, взломал защитную компьютерную систему одного из банков Великобритании и перевел с его счета на счет своих друзей в США свыше 200 тыс. долларов. Через некоторое время Левин был задержан.

Квалифицируйте содеянное Левиным.

Задача 6. Корбин, желая получить компрометирующую информацию о своем начальнике из его персонального компьютера, в начале рабочего дня испортил замок входной двери в кабинете Юшина – начальника лаборатории одного из научно-исследовательского института (НИИ). Затем Корбин позвонил Юшину по телефону с целью получения доступа к компьютеру в его отсутствие. После того как Юшин вышел из кабинета, Корбин проник в кабинет, включил компьютер и стал искать нужные файлы. При перезаписи файлов на флешку в кабинет вошли Юшин и инженер Иванов.

Квалифицируйте деяние Корбина.

Задача 7. Васильченко и Овчаров – студенты радиотехнического ВУЗа – создали резидентную программу с целью блокирования тестирующей программы проверки знаний по физике, находящейся на сервере одной из кафедр института.

В результате запуска созданной программы по компьютерной сети ВУЗа распространился компьютерный вирус, блокировавший системные программы всех компьютеров.

Дайте правовую квалификацию деянию студентов.

Задача 8. Неизвестные лица, перепилив с помощью ножовки по металлу прутья оконных металлических решеток, проникли в необорудованный охранной сигнализацией операционный зал государственного банка, откуда похитили два системных блока персональных компьютеров стандартной модификации, содержащих в своей постоянной памяти банк данных на всех вкладчиков банка, физических и юридических лиц, кредиторов с полными установочными данными, зафиксированными электромагнитным способом на жестком диске.

Дайте правовую квалификацию деянию.

Задача 9. Будучи экономистом по учету заработной платы и отвечая за достоверность документов и сдачу их в бухгалтерию, К. на протяжении ряда лет вносила в документы на начисление заработной платы подложные документы. В результате чего заработная плата начисля-

лась на счета вымышленных лиц и переводилась в банки г. Бреста на специально открытые ею счета: на имя матери К. (7 115 руб. 63 коп.), сестры (4 954 руб. 30 коп.), знакомого (5 379 руб.). Всего таким образом К. похитила 22 960 руб.

Квалифицируйте содеянное К.

Задача 10. Была задержана организованная преступная группа из числа руководителей «Аверс Т. банка» (включая председателя правления банка), которая осуществляла хищения денежных средств путем заключения фиктивных кредитных договоров с «Банком Х.», его отделениями и другими коммерческими банками. При этом использовались нелегальные корреспондентские счета, открытые «Аверс Т. банком» в ряде банков г. Минска. Таким образом, было похищено 18 млрд руб., которые были проконвертированы и зачислены на счета иностранных фирм в зарубежных банках. Из указанной суммы 22 млн руб. руководство «Аверс Т. банка» по расходным ордерам обналичило и присвоило.

Дайте правовую квалификацию данному деянию.

Примерная тематика рефератов

1. Понятие, содержание и значение информационной безопасности современного цифрового (информационного) общества.
2. Современное состояние и проблемы информационной безопасности.
3. Понятие и правовая характеристика преступлений против компьютерной безопасности.
4. Криминогенные факторы современного цифрового мира.
5. Виды и источники угроз информационной безопасности Республики Беларусь.
6. Международно-правовая классификация киберпреступлений.
7. Хакеры: криминологическая характеристика.
8. Организованная преступность цифрового мира.
9. Использование искусственного интеллекта криминальными сообществами.
10. Современные биотехнологии и преступность.

2. ЗАКОНОДАТЕЛЬСТВО РЕСПУБЛИКИ БЕЛАРУСЬ В СФЕРЕ ОБЕСПЕЧЕНИЯ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

1. Концепция национальной безопасности Республики Беларусь.
2. Концепция информационной безопасности Республики Беларусь.
3. Уголовный кодекс Республики Беларусь.
4. Законы и подзаконные нормативные правовые акты Республики Беларусь в сфере защиты компьютерной информации.
5. Акты технического реагирования.
6. Международные нормативные правовые акты в сфере борьбы с преступлениями против компьютерной (информационной) безопасности.

Вопросы для самоконтроля

1. Назовите статьи уголовного закона о преступлениях, предметом или средством совершения которых является информация, их уголовно-правовая характеристика.
2. Назовите примеры применения статей о незаконном собирании либо распространении информации о частной жизни, нарушении тайны переписки, телефонных переговоров, телеграфных или иных сообщений в условиях цифровизации общества.
3. Охарактеризуйте несколько основных международных правовых актов в сфере обеспечения компьютерной безопасности.
4. Дайте правовой анализ Концепции информационной безопасности Республики Беларусь.
5. Проведите сравнительный анализ Концепции информационной безопасности Республики Беларусь и Конвенции Совета Европы «О преступности в сфере компьютерной информации» (EST № 185).
6. Проведите правовой анализ положений о защите информации Концепции национальной безопасности Республики Беларусь.
7. Перечислите субъекты реализации Концепции информационной безопасности Республики Беларусь.

Практические задания

Задача 1. Директора АО Бульдогова заинтересовали банковские счета конкурента. Он нанял специалиста, который, преодолев защиту, проник в компьютерную сеть банка, отыскал информацию об операци-

ях по нужному счету и вывел ее на экран монитора. Бульдогов просмотрел информацию и сделал выписки в блокнот о заинтересовавших его операциях по счету.

Квалифицируйте содеянное.

Задача 2. Логунов написал и распространил с помощью электронной почты программу, которая активизировалась при попытке открыть почтовое сообщение и производила несанкционированные изменения в операционной системе. 31 декабря на мониторах всех компьютеров с измененным программным обеспечением отобразилось: «С новым годом!».

Квалифицируйте содеянное Логуновым.

Задача 3. Боков сконструировал прибор-сканер, с помощью которого перехватывал идентификационные коды мобильных телефонов пользователей и, вводя их в память своего устройства, осуществлял звонки, счета на оплату которых приходили законным абонентам. Общая сумма в счетах пользователям сотовых телефонов превысила базовую величину более чем в 250 раз. В ходе предварительного расследования было установлено, что идентификационный код, перехватываемый Боковым, является компьютерной информацией.

Решите вопрос об ответственности Бокова.

Задача 4. Уволенный за несоответствие занимаемой должности программист компании «Регион» Поповский, желая отомстить директору, перед уходом ввел в компьютерную сеть фирмы вредоносную программу, которая уничтожила большую часть информации о расчетах с клиентами и смежниками.

Для восстановления уничтоженной информации предприятию пришлось провести большую работу, расходы составили около 180 тыс. руб.

Квалифицируйте содеянное Поповским.

Задача 5. Студент института Воскобойников разработал компьютерный вирус и ввел его в компьютерную сеть института с целью срыва проверки остаточных знаний студентов по высшей математике. Однако вирус распространился по компьютерным сетям города. По заключению экспертов, разработанный Воскобойниковым вирус не поддается уничтожению.

Дайте уголовно-правовую характеристику данному деянию.

Задача 6. Группа хакеров в составе Малина, Нелюбова и Рукина «добиралась» до информационных ресурсов интернет-магазинов, копи-

ровала документы о финансовых операциях, идентификационных данных расчетных и платежных карт. После чего пускала эти конфиденциальные сведения в свободную продажу. Нередко секретную информацию предлагалось выкупить, прежде всего, ее же законным владельцам.

Дайте юридическую оценку действиям вышеуказанных лиц.

Задача 7. Студенты автомобильно-дорожного института Скопенко и Жилинский знали о том, что в деканате находится институтский компьютер. Решив его использовать для оформления дипломных работ, Скопенко и Жилинский проникли в деканат и начали работать на компьютере. Из-за их крайне поверхностных знаний и навыков в работе машины произошли сбои, что в дальнейшем привело к отключению модема – одного из элементов компьютерной системы.

Квалифицируйте содеянное. Подлежат ли уголовной ответственности Скопенко и Жилинский?

Задача 8. Смыслов, разработав очередную программу, предусмотрел в ней такого рода защиту, при которой любая попытка несанкционированного её копирования приведет к автоматическому блокированию важнейших файлов программ-оболочек компьютера. Предупреждение о последствиях несанкционированного копирования было указано в установочных файлах программы.

Квалифицируйте содеянное. Содержат ли действия Смыслова состав преступления в сфере компьютерной информации?

Задача 9. Наладчик компьютерной техники научно-производственного объединения «Юг» Блинкович, прибывший на работу в нетрезвом виде, по небрежности вывел из строя сканер стоимостью 3 500 руб. В дополнение к этому, он стер из памяти компьютера, переданного ему для ремонта, информацию о результатах научного эксперемента, под которым значительное время работал не только коллектив института, но и привлекались сотрудники других научных заведений.

Подлежит ли уголовной ответственности Блинкович за преступление в сфере компьютерной безопасности?

Задача 10. Выполняя работу по наладке компьютера в соответствии с указанием начальника отдела, Марчук скопировал для себя несколько отсутствующих у него программ и, таким образом, модифицировал команды загрузочного файла. В результате отдельные программы перестали запускаться. О том, что он снял копии с некоторых про-

грамм, Маркин по окончании работы поставил в известность своего начальника. Спустя некоторое время, ввиду жалоб пользователей сетей, тот сам был вынужден устранить сбой в её работе.

Квалифицируйте содеянное. Образуют ли действия Марчука неправомерный доступ к компьютерной информации?

Примерная тематика рефератов

1. Историко-правовой анализ развития законодательства Республики Беларусь в области обеспечения информационной безопасности.
2. Концепция информационной безопасности Республики Беларусь и субъекты ее реализации.
3. Акты ООН и Совета Европы о борьбе с киберпреступлениями как инструмент международного сотрудничества.
4. Сетевые «тролли» и иные группы травли в Интернете.
5. Особенности преступности в сфере современных информационно-коммуникационных технологий в Республике Беларусь.
6. Проблемы правоприменительной практики статей гл. 31 УК в деятельности органов, ведущих уголовный процесс.
7. Зарубежный опыт и международные стандарты уголовно-правовой борьбы с преступлениями в сфере современных информационно-коммуникационных технологий.
8. Уголовно-правовая характеристика и проблемы применения норм УК о преступлениях, предметом или средством совершения которых является информация.
9. Судебная практика по уголовным делам о преступлениях против информационной безопасности.
10. Использование новейших технологий цифрового мира в предупреждении преступлений.

3. УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА ОТДЕЛЬНЫХ СОСТАВОВ ПРЕСТУПЛЕНИЙ ПРОТИВ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

1. Терминологический аппарат уголовно-правовых норм о преступлениях против компьютерной безопасности.

2. Несанкционированный доступ к компьютерной безопасности (ст. 349 УК).

3. Уничтожение, блокирование или модификация компьютерной информации (ст. 350 УК).

4. Неправомерное завладение компьютерной информацией (ст. 352 УК).

5. Разработка, использование, распространение либо сбыт вредоносных компьютерных программ или специальных программных или аппаратных средств (ст. 354 УК).

6. Нарушение правил эксплуатации компьютерной системы или сети (ст. 355 УК).

7. Незаконные действия в отношении информации о частной жизни и персональных данных (ст. 203^1 УК).

Вопросы для самоконтроля

1. Дайте уголовно-правовую характеристику ст. 354 УК (Разработка, использование, распространение либо сбыт вредоносных компьютерных программ или специальных программных или аппаратных средств).

2. Дайте уголовно-правовую характеристику ст. 355 УК (Нарушение правил эксплуатации компьютерной системы или сети).

3. Дайте уголовно-правовую характеристику ст. 352 УК (Неправомерное завладение компьютерной информацией).

4. Дайте уголовно-правовую характеристику ст. 349 УК (Несанкционированный доступ к компьютерной информации).

5. Дайте уголовно-правовую характеристику ст. 350 УК (Уничтожение, блокирование или модификация компьютерной информации).

6. Дайте уголовно-правовую характеристику объективных и субъективных признаков преступлений против компьютерной безопасности.

7. Дайте уголовно-правовую характеристику ст. 203^1 УК (Незаконные действия в отношении информации о частной жизни и персональных данных).

Практические задания

Задача 1. Шевцов и Трусов, продолжительное время работая на одном предприятии – ООО «Виктория», вступили в сговор, направленный на хищение ликероводочной продукции. Они обговорили условия, по которым Шевцов создает на фирме условия для получения продукции без предоплаты, а Трусов обеспечивает вывоз и сбыт.

Будучи главным специалистом службы сбыта и маркетинга и зная порядок ввода информации в локальную компьютерную сеть для последующего получения продукции предприятия с отсрочкой платежа, Шевцов с помощью компьютера проник в локально-вычислительную сеть ООО «Виктория», где, уничтожив в списке клиентов фирмы запись «300» – номер договора с ЗАО «Лотос», ввел в указанный реестр заведомо ложную информацию о фирме «Победа», что послужило основанием для отгрузки последней ликероводочной продукции.

Трусов подыскал для исполнения роли экспедитора своего знакомого Котова, о чем уведомил Шевцова, который на имеющемся у него типовом бланке оформил доверенность от фирмы «Победа» на получение 200 ящиков ликероводочной продукции на имя экспедитора Котова, и поставил на нее оттиск печати фирмы «Победа».

На следующий день Котов, используя доверенность фирмы «Победа», вывез со склада ООО «Виктория» 4 тыс. бутылок водки «Столичная». Трусов реализовал водку за наличный расчет, полученные деньги поделил со Шевцовым и Котовым.

Дайте юридическую оценку действиям указанных лиц.

Задача 2. С целью получения информации о валютных резервах одного из коммерческих банков директор конкурирующего банка Новиков дал задание своему заместителю за крупное вознаграждение поручить главному программисту Коновалову скопировать компьютерную информацию о балансе банка, что тот и сделал.

Квалифицируйте данное деяние.

Задача 3. Савченко осуществлял рассылку подложных электронных писем с целью завладения персональной информацией клиентов «Ситибанка». Рассылка представляла собой электронное письмо с со-

общением о переводе 100 долларов США на личный счет клиента и содержала просьбу зайти в систему Интернет-бакинга “CitibankOnline” для подтверждения перевода. В случае следования по указанной ссылке происходило попадание на сайт, созданный Савченко, и очень похожий на стартовый экран “CitibankOnline”. Десять человек ввели номер кредитной карты и пин-код для того, чтобы войти в систему. Воспользовавшись полученной таким образом информацией, Савченко совершил завладение денежными средствами Павлова и Костенко, находящимися в «Ситибанке», в сумме 15 и 20 тыс. долларов США соответственно.

Квалифицируйте содеянное Савченко.

Задача 4. Гуляшов, студент факультета вычислительной математики, организовывал сетевые атаки, заключающиеся в получении обманным путем доступа в сеть посредством имитации соединения. Таким образом он получил доступ к информации о счетах пользователей интернета и номерах некоторых кредитных карт и пин-кодов. Полученную информацию Гуляшов передавал Сорокиной за вознаграждение, которая использовала ее для хищения денежных средств.

Квалифицируйте содеянное Гуляшовым и Сорокиной.

Задача 5. Петров использовал доработанный сотовый телефон-«сканер», который позволял производить звонки за чужой счет. Всего в течение шести месяцев Петров таким образом «израсходовал» 15 тыс. руб.

Можно ли считать информацию, содержащуюся в сотовым телефоне, компьютерной информацией? Как соотносятся компьютерная информация и коммерческая тайна? Квалифицируйте содеянное Петровым.

Задача 6. Корреспондент газеты «Сорока» Говорухин решил приобрести информацию о готовящейся комплексной операции по пресечению административного правонарушения в г. Минске. Данная информация составляла служебную тайну. Узнав из своих источников о том, что проект плана операции хранится на флешке в кабинете начальника УВД, Говорухин предложил своему знакомому Кошеленко, работавшему в УВД, за вознаграждение достать ему эту флешку. Кошеленко выполнил просьбу Говорухина и передал ему флешку.

Квалифицируйте содеянное Говорухиным и Кошеленко.

Задача 7. Крыленко купил на радиорынке комплект дисков с игровой программой и, проверив её на наличие «вирусов», которые обнаружены не были, установил на свой ПК. Спустя некоторое время работа

компьютера была полностью заблокирована. Придя к выводу, что причиной тому новейший «вирус», которым поражена купленная им программа, Крыленко продал ее вместе с комплектом дисков своему приятелю, скрыв от него имеющийся дефект.

Квалифицируйте содеянное. Есть ли в деянии Крыленко состав преступления в сфере компьютерной информации?

Задача 8. Используя свой компьютер, Малиновский «на спор» сумел подключиться к сети Гомельгидромета и для доказательства того, что это ему удалось, скопировал информацию о параметрах метеоусловий в Крыму и изменил пароль для доступа к этой информации работников Гомельгидромета.

Квалифицируйте содеянное. Совершено ли Малиновским преступление?

Задача 9. Главный специалист НИИ Кубицкая по роду выполняемой работы использовала компьютер. В нерабочее время она разрешала воспользоваться им своему 16-летнему сыну Андрею. Когда Кубицкая на некоторое время отлучилась, Андрей по ошибке ввел команду на уничтожение важной информации. Кубицкая не сумела восстановить утраченное, используя необходимые программы. На следующий день она была вынуждена доложить руководству учреждения о случившемся.

Квалифицируйте содеянное. Подлежат ли Кубицкая и ее сын уголовной ответственности за содеянное? Обоснуйте свой ответ.

Задача 10. Совместная белорусско-американская фирма разработала и продавала компьютерную программу. При установке программа автоматически заменяла некоторые стандартные драйверы адаптированными, разработанными специалистами фирмы, что в ряде случаев приводило к нарушению работы компьютеров. В документации по программе об этих особенностях программы не сообщалось. Кроме того, программа установки тестировала аппаратное обеспечение пользователя, считывая информацию из памяти компьютера, которую передавала маркетинговой службе фирмы. Об этой особенности программы также не сообщалось.

Дайте юридический анализ содеянному.

Примерная тематика рефератов

1. Киберпреступность: понятие, основные концепции.
2. Преимущества и недостатки уголовно-правовой охраны информационной безопасности в Республике Беларусь.

3. Программные и программно-аппаратные методы защиты компьютерной информации.

4. Система мер предупреждения преступлений против компьютерной безопасности в Республике Беларусь.

5. Уголовная ответственность за коммерческий шпионаж.

6. Существенный вред как общественно опасное последствие преступлений против компьютерной безопасности.

7. Виды преступлений против компьютерной безопасности и их уголовно-правовая характеристика.

8. Составляющие элементы понятия компьютерной безопасности как объекта уголовно-правовой охраны.

9. Экономические киберпреступления.

10. Развитие и мотивы киберпреступности.

4. АКТУАЛЬНЫЕ ВОПРОСЫ ПРИВЛЕЧЕНИЯ К ГРАЖДАНСКОЙ И АДМИНИСТРАТИВНОЙ ОТВЕТСТВЕННОСТИ ЗА ПРАВОНАРУШЕНИЯ В СФЕРЕ ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

1. Понятие несанкционированного доступа к компьютерной информации.

2. Административные правонарушения в области связи и информации.

3. Гражданско-правовая ответственность за преступления в сфере защиты компьютерной информации.

4. Имущественные права правообладателей объектов авторского права.

5. Возмещение убытков, компенсация морального вреда и другие споры в области авторского права и смежных прав.

Вопросы для самоконтроля

1. Дайте понятие термину «несанкционированный доступ к компьютерной информации».

2. Что является предметом правонарушения по ст. 23.4 Кодекса Республики Беларусь об административных правонарушениях?

3. Что образует состав неправомерного доступа к компьютерной информации по ст. 23.4 Кодекса Республики Беларусь об административных правонарушениях?

4. Что является предметом правонарушения по ст. 23.7 Кодекса Республики Беларусь об административных правонарушениях?

5. Что является предметом правонарушения по ст. 19.7 Кодекса Республики Беларусь об административных правонарушениях?

6. Что является объектами авторского права согласно Гражданскому кодексу Республики Беларусь?

7. Что является субъектами авторского права согласно гражданскому законодательству Республики Беларусь?

Практические задания

Задача 1. Программист одного из филиалов коммерческого банка, используя свое служебное положение, при обслуживании программы

«Вклады населения» совершил хищение чужого имущества на общую сумму 62 млн руб. Суть его преступных действий заключалась в том, что он вносил разного рода неправомерные изменения в данные о суммах на лицевых счетах вкладчиков, начисляя по ним проценты и переносил денежные суммы с одного вида вклада на другой, где были предусмотрены более высокие проценты. Все незаконно начисленные суммы он переводил на заранее открытые счета, а затем изымал их по фиктивным (подделывал подписи вкладчиков) расходным кассовым ордерам, используя свои доверительные отношения с другими работниками банка.

Квалифицируйте данное деяние.

Задача 2. Сотрудница мобильного оператора скопировала из базы данных информацию о телефонных соединениях абонента без его ведома и соответствующего заявления. При этом доступ к этой информации у нее имелся с помощью рабочих логина и пароля, то есть она имела право на доступ в силу выполнения трудовой функции.

Дайте квалификацию содеянному.

Задача 3. Мошенник, осуществив несанкционированный доступ в мессенджере “Viber” гражданки В. и воспользовавшись ее аккаунтом, от имени женщины переслал сообщения, содержащие фишинговые ссылки – ее друзьям, зарегистрированным в сети. Перейдя по ним, пользователи мессенджера проходили опрос, тем самым принимая участие в вымышленной «акции». В результате, друзья гражданки В. ввели реквизиты своих банковских платежных карт (БПК) с целью получения вознаграждения за участие в ней, однако после данных действий они лишились денежных средств. Стоит обратить внимание, что злоумышленник, при отправлении сообщений, содержащих фишинговые ссылки, пользовался данными, хранящимися в чатах, а именно: использовал способ переписки, словесные обороты, жизненные события, отраженные в предыдущих сообщениях гражданки В. и ее друзей.

Квалифицируйте данное деяние.

Задача 4. Разработчики Закона Республики Беларусь «О предпринимательстве в Республике Беларусь» обратились в суд с требованием об уплате им авторского вознаграждения.

Укажите, правомерны ли требования разработчиков закона. Определите, какое решение должен принять суд.

Задача 5. Студент Мишин, случайно подсмотрев записанный пароль от электронного ящика студентки своей группы Савченко, со сво-

его ноутбука ознакомился с ее перепиской, содержащейся в этом электронном ящике. Убедившись, что круг ее абонентов не вызывает для него неприязни, аккуратно вышел из ее электронной почты, не внеся никаких изменений.

Дайте правовую характеристику сложившейся ситуации.

Задача 6. Специалист одного из государственных учреждений Слуцкий, используя многочисленные флешки и диски с информацией, полученной от сотрудников других организаций, не всегда проверял их на наличие «вирусов», доверяясь заверениям поставщиков о том, что данные носители чистые. Из-за этого в компьютер сотрудника Плаксина был внесен вирус, получивший наименование «с любовью», что провело к утрате важнейшей информации и поставило на грань срыва важного государственного мероприятия.

Квалифицируйте содеянное.

Задача 7. Марченко регулярно «взламывал» программы защиты информации, проникая в компьютерные системы отечественных и зарубежных банков, в оборонные системы. Считав интересующую его информацию, он делился ею со своим знакомым. С ним он также обсуждал добытую информацию о новых и интересных защитных программах, с которыми ему довелось столкнуться, обсуждал методы преодоления защиты. Свою деятельность Марченко объяснял желанием постоянно профессионально совершенствоваться, практиковаться в решении сложных технических задач способом поддержания навыков квалифицированной работы с информацией.

Квалифицируйте содеянное. Подлежит ли Марченко уголовной ответственности? Обоснуйте свой ответ.

Задача 8. Ранее судимый Максудов по заказу неизвестного лица обязался предоставить информацию о домашних адресах и телефонах сотрудников фонда ветеранов афганской войны «Братство». С этой целью он подкупил охранника фонда и проник в офис. Подобрав ключ к кабинету начальника отдела кадров, он проник в него, включил компьютер и получил возможность снимать информацию о сотрудниках из базы данных. Руководитель фонда и ряд его сотрудников после представительской встречи решили вернуться в офис, где и задержали Максудова в тот момент, когда он переписывал адреса сотрудников, интересующих заказчика в блокнот.

Квалифицируйте содеянное Максудовым.

Задача 9. Весной прошлого года ведущий бухгалтер отдела валютных операций филиала Х-банка, используя свое служебное положение ввела в компьютер ложные команды и в несколько приемов перевела со счета 76 (расчеты по прочим иностранным операциям) на личные счета своих знакомых 123 тыс. долларов США.

Квалифицируйте содеянное.

Задача 10. Терешкин, увольняясь с предприятия, стер с диска сервера информационно-правовые базы, приобретенные предприятием, и программу, содержащую все данные бухгалтерского учета предприятия.

Квалифицируйте данное деяние.

Примерная тематика рефератов

1. Ответственность за нарушение авторских прав на компьютерную программу.
2. Ответственность за регистрацию на интернет ресурсах, призванных экстремистскими, распространение экстремистских материалов в глобальной сети Интернет.
3. Уголовно-административные механизмы ответственности за правонарушения в информационной сфере.
4. Определение оценки категории «существенный вред» в процессе квалификации административных правонарушений в информационной сфере.
5. Взаимосвязь режима коммерческой тайны и контроля за использованием лицензионного программного обеспечения в организации.
6. Сфера действия авторского права.
7. Объекты смежных прав.
8. Охрана частной жизни гражданина.
9. Обеспечение прав субъектов информационных отношений при создании, использовании и эксплуатации информационных систем и информационных сетей, использовании информационных технологий.
10. Свободный интернет: политические принципы и правовые нормы.

ЛИТЕРАТУРА

Нормативные правовые акты

1. Об информации, информатизации и защите информации : Закон Республики Беларусь, 10 нояб. 2008 г., № 455-З : в ред. Закона Республики Беларусь от 10.10.2022 г., № 209-З // Нац. реестр правовых актов Респ. Беларусь. – 2008. – № 279. – 2/1552.

2. О Концепции информационной безопасности Республики Беларусь [Электронный ресурс] : постановление Совета Безопасности Республики Беларусь, 18 марта 2019 г., № 1. – Режим доступа: https://etalonline.by/document/?regnum=p219s0001. – Дата доступа: 06.05.2023.

3. О защите персональных данных [Электронный ресурс] : Закон Республики Беларусь, 7 мая 2021 г., № 99-З : в ред. Закона Республики Беларусь от 01.06.2022 г., № 175-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

4. Об утверждении положений об организационных мерах по защите персональных данных переписи населения Республики Беларусь и порядке предоставления итоговых данных переписи населения Республики Беларусь [Электронный ресурс] : постановление Совета Министров Республики Беларусь, 10 сент. 2009 г., № 1178 : в ред. постановления Совета Министров Республики Беларусь от 17.11.2016 г., № 930 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

5. Уголовный кодекс Республики Беларусь [Электронный ресурс] : 9 июля 1999 г., № 275-З : принят Палатой представителей 4 июня 1999 г. : одобрен Советом Республики 24 июня 1999 г. : в ред. Закона Республики Беларусь от 09.03.2023 г., № 256-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

6. Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в области обеспечения информационной безопасности [Электронный ресурс] : ратифицировано Законом Республики Беларусь от 14 июля 2014 г. «О ратификации Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в области обеспечения информационной безопасности» // Национальный правовой Интернет-портал Республики Беларусь. – Режим доступа: https://pravo.by/document/?guid=12551&p0=N01300115&p1=1. – Дата доступа: 05.05.2023.

7. О модельном законе «Об электронном правительстве» : постановление Межпарламентской Ассамблеи государств-участников Содружества Независимых Государств, 25 нояб. 2016 г., № 45-14 // Информационный бюллетень Межпарламентской Ассамблеи СНГ. – 2017. – № 66.

8. Кодекс Республики Беларусь об административных правонарушениях [Электронный ресурс] : 6 янв. 2021 г., № 91-З : принят Палатой представителей 18 дек. 2020 г. : одобрен Советом Республики 18 дек. 2020 г. : в ред. Закона Республики Беларусь от 17.07.2023 г., № 284-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

9. Гражданский кодекс Республики Беларусь [Электронный ресурс] : 7 дек. 1998 г., № 218-З : принят Палатой представителей 28 окт. 1998 г. : одобрен Советом Республики 19 нояб. 1998 г. : в ред. Закона Республики Беларусь от 13.11.2023 г., № 312-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

10. Решение о Концепции информационной безопасности государств-участников Содружества Независимых Государств в военной сфере [Электронный ресурс] : вступило в силу в 4 июня 1999 г. – Режим доступа: https://etalonline.by/document/?regnum=n99900107. – Дата доступа: 06.05.2023.

11. Концепция согласованной социальной политики государств-членов ЕврАзЭС, представленная постановлением Бюро Межпарламентской Ассамблеи Евразийского экономического сообщества от 17 нояб. 2005 г., № 13 [Электронный ресурс] // Документы заседания Бюро Межпарламентской Ассамблеи Евразийского экономического сообщества. – Режим доступа: https://etalonline.by/document/?regnum=f20500064. – Дата доступа: 06.05.2023.

12. Об электронном документе и электронной цифровой подписи : Закон Республики Беларусь, 28 дек. 2009 г., № 113-З [Электронный ресурс] : в ред. Закона Республики Беларусь от 14.10.2022 г., № 213-З // Национальный правовой Интернет-портал Республики Беларусь. – Режим доступа: https://pravo.by/document/?guid=3961&p0=H10900113. – Дата доступа: 28.10.2022.

13. О кибербезопасности [Электронный ресурс] : Указ Президента Республики Беларусь от 14 февр. 2023 г., № 40 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

14. О защите персональных данных [Электронный ресурс] : Закон Республики Беларусь, 7 мая 2021 г., № 99-З : в ред. Закона Республики

Беларусь от 01.06.2022 г., № 175-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

15. Соглашение между Правительством Республики Беларусь и Правительством Российской Федерации о сотрудничестве в области обеспечения международной информационной безопасности [Электронный ресурс] : ратифицировано Законом Республики Беларусь от 4 янв. 2015 г. «О ратификации Соглашения между Правительством Республики Беларусь и Правительством Российской Федерации о сотрудничестве в области обеспечения международной информационной безопасности» // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

16. Информационные технологии. Средства защиты информации. Информационная безопасность [Электронный ресурс] : ТР 2013/027/BY : принят 15 мая 2013 г. : вступ. в силу 01 янв. 2014 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

Основная литература

17. Волеводз, А. Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества / А. Г. Волеводз. – М. : Юрлитинформ, 2001. – 496 с.

18. Леонтьев, Б. К. Хакеры, взломщики и другие информационные убийцы / Б. К. Леонтьев. – М. : Майор (Осипенко), 2001. – 190 с.

19. Вехов, В. Б. Компьютерные преступления. Способы совершения. Методики расследования / В. Б. Вехов. – М. : Право и Закон, 1996. – 182 с.

20. Ахраменка, Н. Ф. Проблемы криминализации общественно опасного поведения с использованием информационно-вычислительных систем : автореф. дис. … канд. юрид. наук : 12.00.08 / Н. Ф. Ахраменка ; БГУ. – Минск, 1996. – 26 с.

21. Хусяинов, Т. М. Интернет-преступления (киберпреступления) в российском уголовном законодательстве / Т. М. Хусяинов // Уголовный закон Российской Федерации : проблемы правоприменения и перспективы совершенствования : материалы всероссийского круглого стола, Иркутск, 20 марта 2015 г. / Восточно-Сибирский институт Министерства внутренних дел Российской Федерации. – Иркутск, 2015. – Вып. 6. – С. 120–125.

22. Буз, С. И. Киберпреступления: понятие, сущность и общая характеристика / С. И. Буз // Юристъ–Правоведъ. – 2019. – № 4 (91). – С. 78–82.

23. Беспалова, И. В. Специфика сети Интернет как информационно-коммуникативной среды / И. В. Беспалова // Международный научно-исследовательский журнал. – 2017. – № 06 (60), ч. 1. – С. 80–84.

24. Уголовный кодекс Республики Беларусь: научно-практический комментарий / Т. П. Афонченко [и др.] ; под ред. : В. М. Хомича, А. В. Баркова, В. В. Марчука. – Минск : Национальный центр правовой информации Республики Беларусь, 2019. – 1000 с.

25. Киберпреступления в Беларуси: невыдуманные истории и советы от УВД, как не стать жертвой мошенников [Электронный ресурс]. – Режим доступа: https://mlyn.by/20052022/kiberprestupleniya-v-belarusi-nevydumannye-istorii-i-sovety-ot-uvd-kak-ne-stat-zhertvoj-moshennikov/. – Дата доступа: 28.10.2022.

26. Козлов, В. «Computer crime»? Что стоит за названием? [Электронный ресурс] / В. Козлов. – Режим доступа: https://www.crime-research.ru/library/CCrime.html. – Дата доступа: 04.10.2022.

Дополнительная литература

27. Предотвращение компьютерных преступлений // Проблемы преступности в капиталистических странах (по материалам зарубежной печати) : Ежемесячный информационный бюллетень. – М., 1986. – № 4. – С. 4–10.

28. Шляхтова, О. Г. Компьютерные преступления: историко-правовой аспект / О. Г. Шляхтова // Известия Гомельского государственного университета им. Ф. Скорины. – 2023. – № 2 (137). – С. 89–93.

29. Основные направления государственной политики в области информационной безопасности : материалы для членов информационно-пропагандистских групп (декабрь 2022 г.) / Академия управления при Президенте Республики Беларусь. – Минск, 2022. – 10 с.

30. Председатель Президиума НАН Беларуси – об информационной безопасности страны [Электронный ресурс]. – Режим доступа: https://pravo.by/novosti/obshchestvenno-politicheskie-i-v-oblasti-prava/2019/mart/33256/. – Дата доступа: 02.07.2023.

31. Шляхтова, О. Г. Состояние и динамика преступности против компьютерной безопасности в Республике Беларусь: аналитический обзор / О. Г. Шляхтова // Экономико-правовые перспективы развития общества, государства и потребительской кооперации : сборник научных

статей IV Международной научно-практической интернет-конференции, Гомель, 31 марта 2023 г. / редкол. : С. Н. Лебедева [и др.] ; под науч. ред. канд. юрид. наук, доцента Ж. Ч. Коноваловой. – Гомель : учреждение образования «Белорусский торгово-экономический университет потребительской кооперации», 2023. – С. 108–111.

32. Булва, В. Феномен социальных сетей в контексте информационной безопасности [Электронный ресурс] / В. Булва // Международная жизнь. – Режим доступа: https://interaffairs.ru/jauthor/material/2799. – Дата доступа: 05.11.2023.

33. Кибершпионаж [Электронный ресурс] / Управление ООН по наркотикам и преступности. – Режим доступа: https://www.unodc.org/e4j/ru/cybercrime/module-14/key-issues/cyberespionage.html. – Дата доступа: 07.07.2023.

34. Дубко, М. А. Особенности квалификации неправомерного завладения компьютерной информацией и отграничения от иных преступлений против информационной безопасности / М. А. Дубко // Вестник Полоцкого государственного университета. – 2015. – № 13. – С. 180–185.

35. Полещук, Д. Г. Уголовно-правовая охрана информационной безопасности (на примере отдельных аспектов охраны кибербезопасности и защиты информации органиченного распространения) : автореф. дис. … канд. юрид. наук : 12.00.08 / Д. Г. Полещук. – Минск, 2020. – 35 с.

36. Бегишев, И. Р. Преступления в сфере обращения цифровой информации / И. Р. Бегишев, И. И. Бикеев. – Казань : Изд-во «Познание» Казанского инновационного университета, 2020. – 300 с.

37. Киберпреступность: риски и угрозы : материалы Всероссийского студенческого круглого научно-практического стола с международным участием (Северо-Западный филиал ФГБОУВО Российский государственный университет правосудия), Санкт-Петербург, 11 февраля 2021 г. / под ред. д-ра юрид. наук, доцента Е. Н. Рахмановой. – СПб : Астерион, 2021. – 236 с.

38. Галушкин, А. А. К вопросу о кибершпионаже и киберконтрразведке на соврменном этапе / А. А. Галушкин // Вестник РУДН. – 2014. – № 3. – С. 42–45.

39. Амирова, Д. К. К вопросу об установлении уголовной ответственности за кибербуллинг / Д. К. Амирова, Ю. В. Куницына // Ученые записки Казанского юридического института МВД России. – 2022. – Т. 1, № 7 (13). – С. 12–16.

40. Безруков, А. В. Преступления в сфере компьютерной информации: юридический анализ, проблемы квалификации / А. В. Безруков, О. В. Безрукова // Научный журнал «Эпомен». – 2020. – № 42. – С. 28–39.

Производственно-практическое издание

Емельянов Сергей Леонидович,
Шляхтова Оксана Геннадьевна

УГОЛОВНОЕ ПРАВО (ОСОБЕННАЯ ЧАСТЬ)

ПРЕСТУПЛЕНИЯ ПРОТИВ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Практическое пособие

Редактор Е. С. Балашова
Корректор В. В. Калугина

Подписано в печать 26.03.2024. Формат 60x84 1/16.
Бумага офсетная. Ризография.
Усл. печ. л. 1,63. Уч.-изд. л. 1,78.
Тираж 10 экз. Заказ 195.

Издатель и полиграфическое исполнение:
учреждение образования
«Гомельский государственный университет имени Франциска Скорины».
Специальное разрешение (лицензия) № 02330 / 450 от 18.12.2013 г.
Свидетельство о государственной регистрации издателя, изготовителя,
распространителя печатных изданий в качестве:
издателя печатных изданий № 1/87 от 18.11.2013 г.;
распространителя печатных изданий № 3/1452 от 17.04.2017 г.
Ул. Советская, 104, 246028, Гомель.