Министерство науки и высшего образования
Российской Федерации
ФГБОУ ВО «Удмуртский государственный университет»
Институт права, социального управления и безопасности
Кафедра уголовного права и криминологии

С.А. Стяжкина

ОХРАНА ИНФОРМАЦИИ УГОЛОВНО-ПРАВОВЫМИ СРЕДСТВАМИ

Учебное пособие

Ижевск
2021

УДК 343.3
ББК 67.408
С 889

Рекомендовано к изданию Учебно-методическим советом УдГУ

С889	**Стяжкина С.А.** Охрана информации уголовно-правовыми средствами: учебное пособие. Ижевск, 2021. 70 с.

В пособии раскрываются проблемы уголовно-правовой охраны информации. Подробно раскрываются объективные и субъективные признаки составов преступлений, посягающих на различные виды информации.

Учебное пособие адресовано студентам, изучающим уголовное право, а также дисциплину «Охрана информации уголовно-правовыми средствами»

УДК 343.3
ББК 67.408

Введение

Одной из важнейших характеристик современного этапа развития цивилизации является массовая информатизация всех сторон общественной жизни.

Информация является неотъемлемой частью любого современного общества, которое получило название информационного. Большинство аналитиков связывают процессы глобализации современного мирового сообщества с развитием информационной революции.

Последнее десятилетие характеризуется все возрастающими темпами усиления информационной зависимости людей и увеличением объема потребляемой и используемой информации. Информационная сфера — одна из наиболее динамичных и быстро развивающихся сфер общественных отношений, нуждающихся в адекватном правовом регулировании. Нельзя не отметить, что в последние годы активно продолжилось формирование законодательства в информационной сфере и оформление информационного права в качестве самостоятельной отрасли, предпосылкой чему послужила необходимость правового регулирования отношений, объектом которых являются информация, повсеместное внедрение информационных технологий и бурный рост информатизации общества.

В Уголовный кодекс РФ регулярно вносятся изменения, касающиеся криминализации деяний, связанных с информационным оборотом и информационными ресурсами. Так, например, в 2014 г. появилась ст.330.2 УК РФ, установившая уголовную ответственность за неисполнение обязанности по подаче уведомления о наличии у гражданина Российской Федерации гражданства (подданства) иностранного государства либо вида на жительства или иного действительного документа, подтверждающего право на его постоянное проживание в иностранном государстве. В 2012 г. были введены наказания за новые виды мошенничества, одним из которых является мошенничество в сфере компьютерной информации, в 2010 г. появи-

лась ст.185.3, предусматривающая ответственность за манипулирование рынком путем распространение через средства массовой информации, в том числе электронные, информационно-телекоммуникационные сети (включая сеть Интернет), заведомо ложных сведений и т.д., ст.185.6, предусматривающая ответственность за неправомерное использование инсайдерской информации.

В связи с этим назрела необходимость выяснения роли и значения информации в уголовном праве.

В соответствии со ст.3 Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации, основывается на следующих принципах:

1) свободы поиска, получения, передачи, производства и распространения информации любым законным способом;

2) установления ограничений доступа к информации только федеральными законами;

3) открытости информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;

4) равноправии языков народов Российской Федерации при создании информационных систем и их эксплуатации;

5) обеспечении безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;

6) достоверности информации и своевременности её предоставления;

7) неприкосновенности частной жизни, недопустимости сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;

8) недопустимости установления нормативными правовыми актами каких-либо преимуществ применения одних ин-

формационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

В пособии раскрываются понятие и признаки преступлений, посягающих на различные виды информации, дается их краткая характеристика. По каждой теме предлагаются теоретические вопросы и задания для лучшего закрепления материала. Кроме того, имеются практические задания, решая которые, студент приобретает навыки правильной квалификации преступлений и их уголовно-правовой оценки.

Пособие адресовано студентам дневной и заочной форм обучения, изучающих дисциплину «Охрана информации уголовно-правовыми средствами».

В результате освоения дисциплины обучающийся должен:

• знать понятия, признаки, виды охраняемой уголовным законом информации; признаки составов преступлений, предусматривающих ответственность за посягательство на различные виды охраняемой информации;

• уметь применять нормативно-правовые акты, предусматривающие уголовную ответственность за посягательство на различные виды охраняемой информации;

• владеть навыками квалификации преступлений, посягающих на охраняемую информацию.

В результате освоения дисциплины должны быть сформированы следующие компетенции: способность применять нормативные правовые акты; реализовывать нормы материального и процессуального права в профессиональной деятельности, а также юридически правильно квалифицировать факты и обстоятельства.

Тема 1. Информация в уголовном праве: понятие, признаки, виды

Одной из важнейших характеристик современного этапа развития цивилизации является массовая информатизация всех сторон общественной жизни.

Информация является неотъемлемой частью любого современного общества. Современное общество получило название «информационное» и большинство аналитиков связывают процессы глобализации современного мирового сообщества с развитием информационной революции.

Последнее десятилетие характеризуется все возрастающими темпами усиления информационной зависимости людей и увеличением объема потребляемой и используемой информации. Информационная сфера — одна из наиболее динамичных и быстро развивающихся сфер общественных отношений, нуждающихся в адекватном правовом регулировании. Нельзя не отметить, что в последние годы активно продолжилось формирование законодательства в информационной сфере и оформление информационного права в качестве самостоятельной отрасли, предпосылкой чему послужила необходимость правового регулирования отношений, объектом которых являются информация, повсеместное внедрение информационных технологий и бурный рост информатизации общества.

Как отмечает Л.А. Букалерова: «Проблемой является тот факт, что на сегодняшний день нет легального определения термина «информация» для целей уголовного права, хотя уголовный закон им оперирует»[1].

Возможно, и нет необходимости в исключительно уголовно-правовом термине «информации». Достаточно было бы универсального, единого для всех отраслей правового понятия «информации».

---

[1] Букалерова Л.А. Уголовно-правовая охрана официального информационного оборота / под ред. В.С. Комиссарова, Н.И. Пикурова. М.: Юрлитинформ, 2006.

Если обратиться к словарям, то, как правило, указывается, что информация − «сведения об окружающем мире и протекающих в нем процессах, воспринимаемые человеком или специальным устройством (спец) 2. Сообщения, осведомляющие о положении дел, о состоянии чего-нибудь»[2].

Обращаясь к специалистам в области информационного права, мы увидим достаточно сложное и громоздкое определение информации как «воспринимаемую и понимаемую человеком характеристику окружающего мира во всем его разнообразии, которая возникает в процессе познания последнего и позволяет на основе измерения свойств предметов, явлений, процессов, фактов и отражения их в различных формах восприятия отличать их признаки, значения и устанавливать связи и зависимости всего многообразия проявления материального, духовного, идеологического мира».

В уголовно-правовом аспекте информация выступает, прежде всего, как признак составов преступлений и поэтому для целей уголовного права необходимо остановится на понятии, роли и значении информации в структуре признаков составов преступлений.

Федеральный закон от 27.07.2006 г. №227-ФЗ «Об информации, информационных технологиях и о защите информации» в ст.2 дает определение информации как сведениях (сообщениях, данных) независимо от формы их предоставления. Представляется, что данное определение слишком широкое и не может быть положено в основу уголовно-правовой регламентации.

Более развернутым видится определение, содержащееся в Модельном Законе «Об информатизации, информации и защите информации», принятом на 26-м пленарном заседании Межпарламентской ассамблеи государств-участников СНГ,

---

[2] Ожегов С.И., Шведова Н.Ю. Толковый словарь русского языка: 80 000 слов и фразеологических выражений. М., 1999.

где в ст.2 сказано, что информация – сведения или данные, порядок использования которых независимо от способа их представления, хранения или организации, подлежит правовому регулированию в соответствии с настоящим Законом и иными национальными законами.

Таким образом, речь идет не просто о сведениях, сообщениях, а о данных, оборот которых подлежит правовому регулированию.

Для целей уголовного права необходимым признаком информации выступает ее правовое значение и ее нахождение в правовом поле.

Обращаясь к нормам уголовного права, можно придти к выводу, что информация может выступать как в качестве объекта уголовно-правовой охраны (ст. 137, 183, 311, 320 УК РФ и др.), так и определять способ совершения преступления (ст. 159.1, 170, 176, 185.3 УК РФ и др.). Кроме того, ряд преступлений предусматривает ответственность за сокрытие информации или отказ от предоставления информации, подлежащей обязательному предоставлению (ст. 140, 287, 330.1, 330.2 УК РФ), а также ответственность за распространение «вредной» информации, распространение которой ограничивается или запрещается (ст. 129.1, 205.2, 242, 242.1 УК РФ).

Исходя из вышеизложенного, в зависимости от уголовно-правового значения всю информацию можно подразделить на:

− охраняемую информацию, то есть информацию, которая защищается уголовным законом и за собирание которой предусмотрена уголовная ответственность;

− заведомо ложную информацию, выступающую средством совершения преступлений;

− информацию, подлежащую обязательному предоставлению, то есть речь идет об информации, которую лицо обязано предоставить в соответствии с законодательством, а в случае непредоставления наступает уголовная ответственность;

− «вредную» информацию, то есть информация, распространение которой причиняет вред различным сферам общественной жизни (нравственности, безопасности).

Теоретические вопросы и задания

1.Что такое информация? Ознакомьтесь с нижеприведенными определениями. Чем они отличаются друг от друга?

Информация – это сведения (сообщения, данные) независимо от формы их предоставления (ФЗ «Об информации, информационных технологиях и о защите информации» от 27.07.2006).

Информация – сведения или данные, порядок использования которых, независимо от способа их представления, хранения или организации, подлежит правовому регулированию в соответствии с настоящим законом и иными национальными законами (Модельный закон об информатизации, информации и защите информации, принят на 26-м пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ от 18.11.2005).

2.Ознакомьтесь с ФЗ РФ «Об информации, информационных технологиях и о защите информации» от 27.07.2006. Какие виды информации выделяются в законе, каково их правовое значение?

3.Назовите виды информации в зависимости от ее уголовно-правового значения.

4.Найдите в Уголовном кодексе РФ составы преступлений, где информация выступает:

а) как объект охраны;

б) как способ совершения преступлений;

в) как подлежащая обязательному предоставлению;

г) как «вредная».

Тема 2. Информация как объект уголовно-правовой охраны

При изучении данной темы необходимо остановиться на вопросах определения охраняемой информации, на признаках, характеризующих информацию как объект уголовно-правовой защиты.

Во-первых, следует выяснить, какая же информация подлежит защите?

В ст.5 Федерального закона от 27.07.2006 г. №227-ФЗ «Об информации, информационных технологиях и о защите информации» указано, что информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа). К общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен. Что касается информации ограниченного доступа, то ограничение доступа к ней устанавливается федеральными законами и обязательным является соблюдение ее конфиденциальности

Представляется, что предметом уголовно-правовой охраны выступает именно информация ограниченного доступа.

Что касается нормативной определенности, то данный признак, безусловно, должен присутствовать для отнесения информации к числу охраняемой, что непосредственно вытекает из положений Федерального закона от 27.07.2006 г. №227-ФЗ «Об информации, информационных технологиях и о защите информации», где в ст.9 сказано, что ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Исходя из анализа положений вышеупомянутого закона, к информации ограниченного доступа следует относить: сведения, составляющие государственную тайну, коммерческую

тайну, служебную тайну, профессиональную тайну, личную или семейную тайну, а также иную тайну, обязательность соблюдения конфиденциальности которой устанавливается федеральными законами.

На сегодняшний день действующим является Перечень сведений конфиденциального характера, утвержденный Указом Президента РФ от 06.03.97 г. №188, к которым относятся: сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях; сведения, составляющие тайну следствия и судопроизводства, а также сведения о защищаемых лицах и мерах государственной защиты; служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна); сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее); сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна); сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Большинство из этих сведений получили свое закрепление в качестве предметов уголовно-правовой охраны в Уголовном кодексе РФ. В частности, следующие:

− личная или семейная тайная (ст.137, УК РФ);

− служебная тайна (ст.155 УК РФ − тайна усыновления (удочерения), ст.310 УК РФ − данные предварительного рас-

следования, ст. 311, 320 УК РФ − сведения о мерах безопасности, применяемых в отношении судьи и участников уголовного процесса и в отношении должностных лиц правоохранительных и контролирующих органов);

− коммерческая, банковская, налоговая тайна (ст.183 УК РФ); инсайдерская информация (ст.186.6 УК РФ);

− государственная тайна (ст. 275, 276, 283, 283.1, 283.2 УК РФ).

Не получили своего непосредственного закрепления в Уголовном кодексе РФ врачебная, адвокатская, нотариальная тайны. Представляется, что эти сведения в определенных случаях можно отнести к личной или семейной тайне.

Таким образом, следует отметить, что информация как объект уголовно-правовой охраны представляет собой сведения или данные, порядок доступа к которым и их распространение независимо от способа их представления, хранения или организации, подлежит правовому регулированию в соответствии с законами и иными нормативно-правовыми актами.

Далее следует остановиться на вопросах классификации информации как объекта уголовно-правовой охраны.

Для целей уголовного права информацию как объект уголовно-правовой охраны следует классифицировать по следующим основаниям:

− в зависимости от содержания на: информацию, содержащую личную или семейную тайну; сведения, составляющие государственную тайну; данные, входящие в служебную тайну; информацию, составляющую профессиональную тайну; сведения, составляющие коммерческую, налоговую, банковскую тайну.

В зависимости от носителя: на документированную и недокументированную. Документированную в свою очередь можно также подразделить на информацию, зафиксированную на бумажном носителе, на электронном носителе, видеофиксация, звуковая фиксация.

В заключении следует отметить, что охраняемая информация это всего лишь небольшая часть информационного ресурса, являющего предметом уголовно-правового регулирования. Уголовное право призвано охранять не только саму информацию от несанкционированного распространения, но и защищать субъектов он «вредной» информации, которая огромным потоком льется из различных телекоммуникационных систем.

Теоретические вопросы и задания

1. Раскройте понятие и признаки охраняемой уголовным законом информации.

2. Как вы считаете, достаточно ли полно уголовный закон охраняет различные виды информации?

3. Предложите свои варианты уголовно-правовой защиты информации.

Практические задания

1.А. совместно с Б. ночью проникли в офис фирмы «ХоМ» и похитили ноутбук фирмы Lenovo IdeaPad G7070 стоимостью 32 тыс. руб. с находящимися в нем файлами, содержащими информацию о коммерческой деятельности фирмы, его бухгалтерской отчетности, документации. Кроме того, они взяли смартфон фирмы Samsung Galaxy стоимостью 45тыс. руб., содержащий информацию о личной SMS-переписке владельца телефона со своими друзьями и многочисленные его фотографии.

Что будет предметом данного преступления? Квалифицируйте действия указанных лиц. Предложите несколько вариантов решения.

2.Адвокат И. рассказал своему приятелю П. о том, что к нему обратился Ф. − их общий знакомый с просьбой оказать ему юридические услуги по представлению его интересов в суде о бракоразводном процессе.

Имеются ли в действиях И. признаки состава преступления?

3.А. и Р. организовали притон для занятия проституцией и для «продвижения своего» бизнеса организовали рассылку SMS-сообщений с информацией об открытии «салона» и скидках на номера телефонов, содержащихся в базах данных, которые были ими скачены из Интернета. Всего было отправлено около 600 сообщений.

Имеются ли в действиях указанных лиц признаки составов преступлений?

4.В газете было размещено объявление о продаже нового омолаживающего средства, обладающего уникальными свойствами. Рекламное объявление содержало информацию о том, что за две недели применения крема достигается эффект как от пластической хирургии и полностью разглаживаются мимические морщины.

Женщины, купившие данное средство, обещанного эффекта не получили.

Является ли данная информация «вредной» и подлежат ли лица, разместившие данное объявление, уголовной ответственности?

Тема 3. Уголовно-правовая охрана частной жизни лица

В соответствии с Конституций РФ «Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени» (ст.23 Конституции РФ) и «сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются» (ст.24 Конституции РФ)[3]. Таким образом, Конституция РФ гарантирует каждому неприкосновенность его частной жизни, личной и семейной тайны.

Уголовный кодекс РФ предусматривает ответственность за нарушение неприкосновенности частной жизни лица, которое выражается в незаконном собирании или распространении сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или в средствах массовой информации.

Прежде всего, необходимо остановиться на вопросе определения объекта рассматриваемого состава преступления. Родовым объектом нарушения неприкосновенности частной жизни лица будут выступать отношения, обеспечивающие безопасность личности. Личность как носитель и обладатель различных прав и обязанностей, как субъект и объект различного рода отношений, в том числе и правовых поставлена под защиту государства. Первостепенное значение уделяется именно вопросам охраны личности, ее прав, законных интересов.

Видовым объектом данного преступления выступают отношения, обеспечивающие защиту конституционных прав и свобод личности.

---

[3] Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 г.) // СПС «Гарант».

Непосредственным объектом преступления, предусмотренного ст.137 УК РФ будут выступать общественные отношения, обеспечивающие неприкосновенность частной жизни лица. Речь идет о конституционном праве на неприкосновенность частной жизни лица, его личной и семейной тайны.

С вопросом объекта тесно связана проблема определения предмета данного преступления, в качестве которого выступают сведения о частной жизни лица, составляющие его личную или семейную тайну. Исходя из нормы уголовного закона, можно сделать вывод, что предметом преступления являются не любые сведения о частной жизни лица, а только такие сведения, которые составляют его личную или семейную тайну. Отсюда следует, что личная или семейная тайна выступает в качестве составляющей частной жизни лица. Хотя Конституция РФ не отождествляет эти понятия, а рассматривает их в качестве равноценных, перечисляя их в ст.23, гарантирующей всем неприкосновенность частной жизни лица, его личной, семейной тайны.

Если обратиться к понятию частной жизни лица, то следует отметить, что в литературе существует огромное количество определений частной жизни лица, к которым относят, в частности, сведения о состоянии здоровья, сексуальной ориентации лица, о его политических, религиозных взглядах и убеждениях, о его имущественном положении, о взаимоотношениях в семье, в кругу друзей и т.д. Одно из определений частной жизни лица было дано Конституционным Судом РФ, который дал следующее разъяснение «в понятие частная жизнь» включается та область жизнедеятельности человека, которая относится к отдельному лицу, касается только его и не подлежит контролю со стороны общества и государства, если носит не противоправный характер»[4].

[4]Определения Конституционного Суда Российской Федерации от 9 июня 2005 г. № 248-О, от 26 января 2010 г. № 158-О-О и от 27 мая 2010 г. № 644-О-О // СПС «Гарант».

Речь идет о такой сфере жизнедеятельности человека, которая не подлежит контролю со стороны общества и государства. Таким образом, если информация о личности отнесена к сведениям, подлежащим предоставлению, то она не может относится к частной жизни лица (например, фамилия, имя и отчество лица, его семейное положение). Кроме того, эта сфера должна носить непротивоправный характер, то есть, не подлежат уголовно-правовой защите сведения о совершенных лицом преступлениях, правонарушениях. Нельзя говорить о семейной тайне, если речь идет о жестоком обращении с детьми в семье как элементах воспитания.

Кроме того, как уже было отмечено выше, исходя из нормы уголовного закона уголовно-правовой охране подлежат не любые сведения о частной жизни лица, а только те, которые составляют его личную или семейную тайну. К сведениям, составляющим личную тайну, могут относится любые сведения о лице, касающиеся его интересов, убеждений, взглядов, привычек, взаимоотношений, которые он стремиться сохранить в тайне от окружающих. То есть такие сведения, в отношении которых потерпевшим принять меры, обеспечивающие их конфиденциальность и сохранность от третьих лиц. Обязательным условием отнесения тех или иных сведений к личной тайне является их недоступность третьим лицам. Не может рассматриваться в качестве личной тайны информация, доступ к которой не ограничен.

При квалификации по ст.137 УК РФ должно учитываться не только мнение потерпевшего о том, что это его личная тайна, но и субъективная сторона виновного, который должен понимать, что собирает сведения, составляющие тайну личную или семейную. Как указано в Постановлении Пленума Верховного Суда РФ от 25 декабря 2018 г. № 46 «О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (ст. 137, 138, 138.1, 139, 144.1, 145, 145.1 Уголовного кодекса Российской Федерации)»: «При решении вопроса о

наличии в действиях лица состава преступления, предусмотренного частью 1 или 2 статьи 137 УК РФ, суду необходимо устанавливать, охватывалось ли его умыслом, что сведения о частной жизни гражданина хранятся им в тайне»[5].

Соответственно, если доступ не ограничен, нет никаких препятствий к ознакомлению с информацией, то и лицо не может осознавать противозаконность своих действий.

Кроме того, в постановлении также указывается, что «с учетом положений указанных норм уголовного закона в их взаимосвязи с положениями пункта 1 статьи 152.2 Гражданского кодекса Российской Федерации не может повлечь уголовную ответственность собирание или распространение таких сведений в случаях, если сведения о частной жизни гражданина ранее стали общедоступными либо были преданы огласке самим гражданином или по его воле»[6].

На сегодняшний день, самыми распространенными сведениями, составляющими личную тайну по материалам судебной практики, выступают фотоизображения в обнаженном виде, которые были получены путем неправомерного доступа к компьютерной информации или были переданы самому виновному.

В диспозиции статьи указывается на три действия, образующих объективную сторону рассматриваемого преступления: незаконное собирание сведений о частной жизни лица без его согласия, незаконное распространение сведений о

---

[5] Постановление Пленума Верховного Суда РФ от 25 декабря 2018 г. № 46 «О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (ст. 137, 138, 138.1, 139, 144.1, 145, 145.1 Уголовного кодекса Российской Федерации)» // СПС «Гарант».

[6] Постановление Пленума Верховного Суда РФ от 25 декабря 2018 г. № 46 «О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (ст.137, 138, 138.1, 139, 144.1, 145, 145.1 Уголовного кодекса Российской Федерации)» // СПС «Гарант».

частной жизни лица без его согласия и распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации.

Обязательным признаком собирания и распространения этих сведений является их незаконность и отсутствие согласия потерпевшего.

Субъективная сторона рассматриваемого состава характеризуется только прямым умыслом. Виновное лицо должно знать, что оно собирает сведения, составляющие личную или семейную тайну.

Обращаясь к квалифицированному составу рассматриваемого преступления, можно отметить, что в качестве лица, использующего свое служебное положение, следует рассматривать должностных лиц, государственных и муниципальных служащих, не являющихся должностными лицами и лиц, выполняющих управленческие функции в коммерческой или иной организации. Данный вывод основывается на анализе положений Постановлений Пленумов Верховного Суда РФ, разъясняющих аналогичные квалифицирующие признаки. В частности, в Постановлении Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» в п.29. указывается, что «Под лицами, использующими свое служебное положение при совершении мошенничества, присвоения или растраты (часть 3 статьи 159, часть 3 статьи 159.1, часть 3 статьи 159.2, часть 3 статьи 159.3, часть 3 статьи 159.5, часть 3 статьи 159.6, часть 3 статьи 160 УК РФ), следует понимать должностных лиц, обладающих признаками, предусмотренными п. 1 примечаний к ст. 285 УК РФ, государственных или муниципальных служащих, не являющихся должностными лицами, а также иных лиц, отвечающих требованиям, предусмотренным п. 1 примечаний к ст. 201 УК РФ (например, лицо, которое использует для совершения хищения чужого имущества свои служебные полномочия, включающие организационно-распорядительные или административно-хозяйственные обязанности в коммер-

ческой организации)»[7]. В целях единообразного подхода к основным понятиям, содержащимся в Уголовном кодексе, следует данные разъяснения распространить и на преступление, предусмотренное ст.137 УК РФ.

Часть 3 ст.137 УК РФ предусматривает ответственность за «незаконное распространение в публичном выступлении, публично демонстрирующемся произведении, средствах массовой информации или информационно-телекоммуникационных сетях информации, указывающей на личность несовершеннолетнего потерпевшего, не достигшего 16-летнего возраста, по уголовному делу, либо информации, содержащей описание полученных им в связи с преступлением физических или нравственных страданий, повлекшее причинение вреда здоровью несовершеннолетнего, или психическое расстройство несовершеннолетнего, или иные тяжкие последствия»[8].

В данном случае речь идет о таком объекте уголовно-правой охраны, как отношения, обеспечивающие защиту прав и законных интересов несовершеннолетних потерпевших от преступлений. Распространение информации о несовершеннолетних потерпевших причиняет вред не столько частной жизни лица, сколько нормальному психическому, нравственному развитию несовершеннолетнего. Такие дети часто подвергаются унижениям и гонениям со стороны сверстников и даже педагогов, что причиняет им существенные страдания и зачастую приводит к печальным последствиям.

Непосредственным объектом рассматриваемого преступления выступают не общественные отношения, обеспечивающие неприкосновенность частной жизни лица, а отношения, обеспечивающие защиту прав и интересов несовершеннолетних потерпевших.

---

[7] Постановлении Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» // СПС «Гарант».

[8] Уголовный кодекс РФ 1996 // СПС «Гарант».

Предметом преступления по ч.3 ст. 137 УК РФ будут выступать две группы сведений: первая – это сведения, указывающие на личность потерпевшего по уголовному делу, не достигшего 16-летнего возраста. К таким сведениям будет относиться любая информация, по которой можно идентифицировать несовершеннолетнего (фамилия, имя, отчество, его фотографии, изображения). Вторая группа сведений – это информация, которая содержит описание полученных несовершеннолетним в связи с совершением в отношении него преступления страданий, как физических, так и нравственных.

Объективная сторона характеризуется рядом признаков. Во-первых, это деяние, которое заключается в распространении информации о несовершеннолетнем потерпевшем или о полученных им страданиях публично. Обязательным признаком выступает публичность, то есть сведения должны распространяться в СМИ, через информационно-телекоммуникационные сети, в публичных выступлениях, произведениях, демонстрирующихся публично. Если информация передается в личной беседе, разговоре, то состава преступления не будет. Распространение будет в тех случаях, когда к этим сведениям предоставляется доступ неограниченного круга лиц, когда она размещается в социальных сетях.

Обязательным признаком объективной стороны выступают последствия, в качестве которых законодатель указывает на вред здоровью несовершеннолетнего, или психическое расстройство несовершеннолетнего, или иные тяжкие последствия.

Последствие в виде вреда здоровью предполагает причинение легкого вреда здоровью, признаки которого раскрыты в ст.115 УК РФ и средней тяжести вреда здоровью, признаки которого предусмотрены в ст. 112 УК РФ. Если же последствия выражаются в причинении тяжкого вреда здоровью потерпевшему, то возникает вопрос о дополнительной квалификации по ст.111 УК РФ, предусматривающей ответственность за умышленное причинение тяжкого вреда здоровью человека.

Еще одно последствие, указанное в диспозиции ч.3 ст.137 УК РФ – иные тяжкие последствия. Данный признак достаточно часто встречается в Уголовном кодексе РФ и носит оценочный характер. Верховный Суд РФ в своем Постановлении Пленума от 04.12.2014 №16 «О судебной практике по делам о преступлениях против половой неприкосновенности и половой свободы личности» к иным тяжким последствиям, которые могут наступить в результате изнасилования, отнес «самоубийство или попытку самоубийства потерпевшего лица»[9]. Думается, что вполне уместно распространить данное разъяснение и на рассматриваемое преступление. Как уже было отмечено выше, очень часто жертвы преступлений, особенно несовершеннолетние подвергаются гонениям и унижениям со стороны сверстников, соседей, что причиняет и нравственные страдания и может привести к самоубийству лица.

Не менее сложным является и вопрос определения субъективной стороны данного преступления. В диспозиции статьи не указывается на форму вины. В связи с чем напрашивается вывод, что в данном случае преступление может быть совершено как умышленно, так и по неосторожности. Но возможность умышленной формы вины в данном случае вызывает сомнения. Рассматриваемое преступление относится к категории средней тяжести, что касается умышленного причинения тяжкого вреда здоровью и доведения до самоубийства, то они относятся к категории тяжких и особо тяжких (если доведение до самоубийства осуществляется в отношении несовершеннолетнего). Таким образом, можно сделать вывод, что диспозицией ч.3 ст.137 УК РФ охватывается умышленное причинение легкого и средней тяжести вреда здоровью, наступивших в результате публичного распространения сведений о потерпевшем несовершеннолетнем, а также наступ-

[9] Постановлении Пленума Верховного Суда от 04.12.2014 №16 «О судебной практике по делам о преступлениях против половой неприкосновенности и половой свободы личности» // СПС «Гарант».

ления последствий в виде тяжкого вреда здоровью или самоубийства несовершеннолетнего по неосторожности. В случае же, если умыслом лица охватывались последствия в виде тяжкого вреда здоровью или самоубийства жертвы, то требуется дополнительная квалификация по ст.111 УК РФ и п. «а» ч.2 ст.110 УК РФ.

Теоретические вопросы и задания

1.Что такое частная жизнь лица?

2.Раскройте понятие личной и семейной тайны.

3.Назовите случаи законного собирания сведений о частной жизни лица.

4.Что такое специальные технические средства, предназначенные для негласного получения информации? Кто решает вопрос о принадлежности того или иного технического средства к числу предназначенных для негласного получения информации?

5.Ознакомьтесь с Постановлением Правительства РФ от 10.03.2000 г. «Об утверждении положения о ввозе в Российскую Федерацию и вывозе из Российской Федерации специальных технических средств, предназначенных для негласного получения информации, и списка видов специальных технических средств, предназначенных для негласного получения информации, ввоз и вывоз которых подлежат лицензированию», а также с Постановлением Правительства Российской Федерации № 287 от 12 апреля 2012 г. «Об утверждении положения о лицензировании деятельности по разработке, производству, реализации и приобретению в целях продажи специальных технических средств, предназначенных для негласного получения информации» и Федеральным законом № 99-ФЗ от 4 мая 2011 г. «О лицензировании отдельных видов деятельности». Каков порядок законного производства, приобретения и сбыта специальных технических средств, предназначенных для негласного получения информации?

6.Проведите отграничение ст.138.1 УК РФ, предусматривающей ответственность за незаконный оборот специальных

технических средств, предназначенных для негласного получения информации от ст.20.23 КоАП РФ, предусматривающей административную ответственность за нарушение правил производства, хранения, продажи и приобретения специальных технических средств, предназначенных для негласного получения информации.

7.Подготовьте доклады по вопросам уголовно-правовой защиты частной жизни лица в уголовном законодательстве зарубежных государств. Проведите сравнительно-правовой анализ.

Практические задания

1.21 октября 2020 г. Р., находясь на работе во время отсутствия Д., своей коллеги, на рабочем месте осуществила доступ к информации, хранящейся на служебном компьютере Д. в их общем кабинете отдела ЗАГС. Обнаружив на указанном компьютере фотоизображения Д. и её сестры К.Е. в обнаженном виде, без их согласия скопировала и на свой служебный компьютер фотоизображения. На следующий день, находясь в своем рабочем кабинете отдела ЗАГС, без согласия Д. и К.Е. продемонстрировала Е. и К. на экране монитора своего служебного компьютера скопированное ранее фотоизображение Д. и К.Е. в обнаженном виде.

Дайте уголовно-правовую оценку содеянному.

2.Р. и М. наняли С., няню для своего ребенка. В целях контроля за действиями няни они в своей квартире установили видеокамеры, не предупредив об этом С. В процессе просмотра видеозаписи они узнали о том, что няня привязывает ребенка к кровати, а сама в это время общается в Интернете в социальных сетях.

Имеются ли в действиях Р. и М. признаки состава преступления.

3.Р., увидев на сайте знакомств фотографию своей бывшей одноклассницы Т., сообщил об этом всем свои бывшим одноклассникам, дав ссылки на адрес ее странички.

Являются ли действия Р. преступными?

4.П., 65-летняя пенсионерка, каждый день, сидя у окна, записывала, кто с кем и во сколько заходил в подъезд и выходил из него. Несколько раз она видела свою соседку Н. в сопровождении незнакомого ей молодого человека, о чем она сообщила мужу Н.

Имеются ли в действиях П. признаки состава преступления?

5.О. неоднократно втайне от своего 16-летнего сына просматривала на его ноутбуке историю поиска в браузере и читала его переписку с одноклассниками, друзьями.

Можно ли квалифицировать действия О. по ст. 137 УК РФ и ст.138 УК РФ?

Л. прислала на телефон своего бывшего приятеля Ф. свои фотографии в обнаженном виде с побережья Средиземного моря. Ф. направил посредством почтовой связи в УМВД РФ по Липецкой области, где работает Р., обращение на имя начальника УМВД РФ генерал-майора полиции К. с приложением имеющихся у него 6 фотографий интимного характера с изображением Р. в обнаженном виде и в различных позах, объясняя тем, что сотрудники инспекции по работе с личным составом УМВД России обязаны знать и видеть, чем занимаются сотрудники УМВД в рамках проведения индивидуально-воспитательной работы.

Имеются ли в действиях Ф. признаки состава преступления?

7.Н. и потерпевшая Н. находились в зарегистрированном браке, в течение которого совместно пользовались Интернет-ресурсами. Подсудимый имел в своем распоряжении пароли, которые использовала потерпевшая при посещении интернет-сайтов. После расторжения брака потерпевшая Н. указанные пароли не сменила и не запретила своему бывшему супругу использовать их, равно, как и не запретила посещать используемые ранее ими обоими интернет-сайты, а Н., с учетом сложившихся между ним и потерпевшей отношений после развода, использовал ранее известные ему пароли для обнародования факта их с Н. развода.

Дайте оценку содеянному Н.?

8. Ш., подозревая свою жену в неверности, 29 января 2020 г. приобрел у С. видеокамеру, закамуфлированную под настольные часы.

Дайте уголовно-правовую оценку содеянному. Что такое специальные технические средства, предназначенные для негласного получения информации? Ознакомьтесь с Постановлением Правительства РФ от 10.03.2000 г. «Об утверждении о ввозе в Российскую Федерацию и вывозе из Российской Федерации специальных технических средств, предназначенных для негласного получения информации, и списка видов специальных технических средств, предназначенных для негласного получения информации, ввоз и вывоз которых подлежат лицензированию», а также Постановлением Правительства Российской Федерации № 287 от 12 апреля 2012 г. «Об утверждении положения о лицензировании деятельности по разработке, производству, реализации и приобретению в целях продажи специальных технических средств, предназначенных для негласного получения информации» и Федеральным законом № 99-ФЗ от 4 мая 2011 г. «О лицензировании отдельных видов деятельности».

9.В офисе коммерческой фирмы у сотрудников стали пропадать деньги, ценные вещи. Директор фирмы О. поручил службе безопасности установить в офисе под видом бытовых приборов видеокамеры и прослушивающие устройства.

Вскоре видеокамеры зафиксировали, как один из сотрудников во время обеденного перерыва и в отсутствие остальных сотрудников похищает деньги и вещи из верхней одежды.

Дайте уголовно-правовую оценку содеянному.

10. К. 21 июня 2020 г., находясь возле входа на станцию метро «Чистые пруды», расположенного по адресу: город Москва, Чистопрудный бульвар, возле дома № 2, осуществил сбыт оперативному сотруднику 11-го отдела Бюро специальных технических мероприятий ГУ МВД России по городу Москве Б.Р.А., действующему в рамках проведения ОРМ – «проверочная закупка», наручных часов со встроенной мини-

атюрной видеокамерой и диктофоном, ранее приобретенных у неустановленного следствием лица, являющихся специальным техническим средством, предназначенным для негласного получения информации.

Квалифицируйте действия К. Окончено ли преступление, если сбыт осуществляется сотрудниками правоохранительных органов, действующих в рамках проведения ОРМ – «проверочная закупка»?

11.Р., директор ООО «Телесистемы» разработал специальные технические средства, предназначенные для негласного получения и регистрации акустической информации – устройства дистанционного контроля «Телефонное ухо» и «УДАК», организовал их производство и сбыт. Таким образом, были изготовлены и реализованы 47 устройств.

Квалифицируйте действия указанного лица. Каковы критерии отнесения того или иного технического средства к числу предназначенных для негласного получения информации?

12.Л. из мести за якобы совершенную измену без согласия У. и под псевдонимом (ником) «Alex Юпитер» на Интернет-ресурсе «ВКонтакте» (http://vk.com/Alex001), предназначенном для обмена информацией между пользователями данного Интернет-ресурса, в публичном доступе, используя для этого сотовый телефон с возможностью выхода в сеть Интернет, разместил на стене пользователя «Alex Юпитер» социальной сети «ВКонтакте» четыре фотографии обнаженной У., создав условия для просмотра и скачивания данных фотографий зарегистрированным пользователям Интернет-ресурса «ВКонтакте». В результате чего фотографии интимного характера У. в ленте новостей и на стене страницы «Alex Юпитер» на Интернет-ресурсе «ВКонтакте» просмотрели и оценили не менее 21 пользователя социальной сети «ВКонтакте», что подтверждается наличием в сумме 21 «лайка» под фотографиями и тем, что в друзьях У. в социальной сети «ВКонтакте» числится 1703 лица, которые имели доступ к указанным фотографиям.

Квалифицируйте действия Л.

13.В период с января по апрель 2020 г. А.А. Пермяков, находясь у себя дома, обладая познаниями в области информационных технологий, с использованием программного обеспечения «IP Scanner», находясь в сети Интернет, являющейся средством массовой информации, произвел несанкционированный вход в персональный компьютер Д., обнаружив два графических файла с изображением обнаженной Д., произвел их копирование в свой персональный компьютер. Далее, 24 июня 2020 г. А.А. Пермяков, находясь в сети Интернет и являясь участником группы «MENDELEEVSK ANONYMOUS GOSSIPS» в социальной сети «ВКонтакте», направил в личное сообщение администратору указанной группы под именем «Максим Максимов», под которым зарегистрирована Д., ранее добытые незаконным путем два графических файла с изображением обнаженной Д., которые были размещены на странице группы «MENDELEEVSK ANONYMOUS GOSSIPS».

Квалифицируйте действия А.А. Пермякова.

Тема 4. Уголовно-правовая охрана коммерческой, налоговой и банковской тайны

Одним из видов охраняемой информации выступает информация, представляющая экономическую ценность. Уголовный кодекс предусматривает ответственность за незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну (ст.183 УК РФ).

Родовым объектом рассматриваемого преступления являются общественные отношения в сфере экономики. Видовым объектом являются отношения в сфере экономической деятельности. Непосредственным объектом будут выступать общественные отношения, обеспечивающие неприкосновенность и защиту сведений, составляющих коммерческую, налоговую и банковскую тайны.

Обязательным признаком объекта по ст.183 УК РФ выступает предмет. Предметом будут выступать, во-первых, сведения, составляющие банковскую тайну, во-вторых, сведения, составляющие налоговую тайну и, в-третьих, сведения, составляющие банковскую тайну.

В соответствии с Федеральным законом «О коммерческой тайне» от 29.07.2004 № 98-ФЗ под информацией, составляющей коммерческую тайну, понимаются сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны.

При отнесении тех или иных сведений к коммерческой тайне следует руководствоваться рядом признаков, присущих данным сведениям. Во-первых, благодаря неизвестности этих сведений третьим лицам, обладатель этих сведений извлекает

доходы либо избавляется от расходов, то есть они имеют экономическую ценность. Обязательным признаком сведений, составляющих коммерческую тайну, является факт неизвестности третьим лицам, который достигается путем ограничения к ним доступа третьим лицам. В отношении данных сведений должен быть введен режим коммерческой тайны, который предполагает их правовую, организационную и техническую защиту от неправомерного доступа.

К налоговой тайне в соответствии со ст.102 Налогового кодекса относятся любые полученные налоговым органом, органами внутренних дел, следственными органами, органом государственного внебюджетного фонда и таможенным органом сведения о налогоплательщике, плательщике страховых взносов. Фактически, речь идет о любых сведениях, которые стали известны в процессе осуществления своих профессиональных функций налоговым органам, органам внутренних дел.

Банковской тайной, согласно ст.26 Федерального закона от 02.12.1990 № 395-1 (ред. от 30.12.2020) «О банках и банковской деятельности», выступают сведения об операциях, о счетах и вкладах своих клиентов и корреспондентов.

Одна и та же информация может быть и банковской, и налоговой, и коммерческой. В частности, в ст.102 Налогового кодекса указывается, что, к разглашению налоговой тайны относится, в частности, использование или передача другому лицу информации, составляющей коммерческую тайну (секрет производства) налогоплательщика, плательщика страховых взносов и ставшей известной должностному лицу налогового органа, органа внутренних дел, следственного органа, органа государственного внебюджетного фонда или таможенного органа, привлеченному специалисту или эксперту при исполнении ими своих обязанностей.

Объективная сторона ч.1 ст.183 УК РФ состоит в собирании сведений, составляющих коммерческую, налоговую или банковскую тайны. Под собиранием понимается любой спо-

соб их получения. Причем в диспозиции статьи приводится примерный перечень способов собирания, к которым относятся: похищение документов, подкуп или угрозы, а также иной незаконный способ. На сегодняшний день основным способом собирания сведений является неправомерный доступ к компьютерной информации путем взлома систем безопасности, использования вирусных программ и т.д.

Состав рассматриваемого преступления является формальным и преступление считается оконченным с момента собирания сведений, то есть когда сведения стали доступны лицу и у него появилась возможность их использовать.

Субъективная сторона преступления характеризуется прямым умыслом, виновное лицо должно знать о том, что он собирает сведения, составляющие коммерческую, налоговую или банковскую тайну.

Субъектом преступления, предусмотренного ч.1 ст.183 УК РФ, является физическое, вменяемое лицо, достигшее 16-летнего возраста.

Особенностью данного состава выступает то, что ч.2 ст.183 УК является не квалифицированным составом, как это обычно бывает, а самостоятельным преступлением. Диспозиция ч.2 ст.183 предусматривает ответственность за незаконное разглашение или использование сведений, составляющих коммерческую, налоговую или банковскую тайну, без согласия их владельца лицом, которому она была доверена или стала известна по службе или работе.

Таким образом, объективная сторона части второй выражается в двух альтернативных действиях: незаконное разглашение сведений, составляющих коммерческую, налоговую и банковскую тайны либо их использование.

Незаконное разглашение заключается в сообщении этих сведений хотя бы одному лицу, не имеющему к ним доступа. Преступление считается оконченным с момента, когда сведения становятся известны третьим лицам.

Использование заключается в применении данных сведений по назначению, извлечение пользы и выгоды за счет этих сведений.

Субъективная сторона характеризуется только прямым умыслом.

Особенностью ч.2 ст.183 УК РФ является то, что здесь предусмотрен специальный субъект преступления, а именно, лицо, имеющее доступ к этим сведениям по службе или работе.

Часть третья ст.183 УК РФ содержит квалифицированный состав, предусматривающий повышенную ответственность в случае, если в результате незаконных действий был причинен крупный ущерб или они были совершенны из корыстной заинтересованности.

Размер крупного ущерба определен в ст. 170.2 УК РФ, он составляет 2250000 руб. Крупный ущерб включает в себя как реальные убытки, так и упущенную выгоду.

Признак корыстной заинтересованности означает стремление лица, совершающего незаконные действия извлечь выгоду имущественного характера.

В ч.4 ст.183 УК предусмотрен особо квалифицированный признак – тяжкие последствия. К тяжким последствиям можно отнести особо крупный ущерб, организационный вред, который может выразиться в банкротстве предприятия или организации.

Теоретические вопросы и задания

1.Определите признаки и структуру информации с ограниченным доступом.

2. Назовите виды информации с ограниченным доступом.

3. На основании Федерального закона от 29.07.2004 «О коммерческой тайне» раскройте понятие коммерческой тайны, определите, какие сведения могут относиться к информации, составляющей коммерческую тайну, и какие меры по охране информации должны приниматься ее обладателем.

4. На основании положений Налогового кодекса РФ дайте понятие налоговой тайны, определите, какие сведения могут относиться к налоговой тайне.

5. Ознакомьтесь с Федеральным законом от 02.12.1990 г. №395 «О банках и банковской деятельности». Раскройте понятие банковской тайны.

6.Что такое служебная и профессиональная тайны? Кто является субъектом разглашения служебной и профессиональной тайны?

Практические задания

1.А. совместно с П. установил на банкомате нештатное электронное устройство, предназначенное для считывания информации с магнитных полос пластиковых платежных карт, в том числе индивидуальных номеров банковских карт, то есть информацию, вводимую посредством клавиатуры пользователем банкомата, в том числе о ПИН-кодах платежных пластиковых карт. Данное устройство позволило собрать сведения путем копирования ПИН-кодов пользователей и электронных данных с магнитных полос 365 платежных пластиковых карт клиентов.

Можно ли ПИН-код отнести к банковской тайне? Квалифицируйте действия указанных лиц.

2.К., работая в должности помощника ЗАО «Русская телефонная компания», которое по договору является коммерческим представителем ОАО «Мобильные ТелеСистемы», имея по роду своей трудовой деятельности свободный доступ к программе, содержащей базу персональных данных абонентов ОАО «МТС», при помощи указанной программы по просьбе друга осуществил запрос в базу данных абонентов ОАО «МТС» о предоставлении информации о владельце абонентского номера. Программа вывела на экран монитора запрашиваемую информацию, тем самым К. получил персональные данные об абоненте, а именно фамилию, имя, отчество абонента и адрес проживания.

Дайте уголовно-правовую оценку содеянному. Относятся ли персональные данные лица к сведениям, составляющим коммерческую тайну?

З.В., увлекаясь администрированием сетевых ресурсов, будучи активным пользователем сети Интернет, обнаружил в сети Интернет сайт komilfocentr.ru, созданный и обслуживаемый ООО «к.а. АРТполитика», защищенный от неправомерного доступа логином и паролем и относящийся к коммерческой тайне указанной организации.

Ради интереса В. зашел путем подбора парольно-кодовой информации на интернет-страницу, предназначенную для управления базами данных komilfocentr.ru (в веб-интерфейс), и, получив права администратора, скопировал на свою ПЭВМ базу данных указанного сайта.

Положением ООО «к.а. «АРТполитика» от 11 января 2019 г. «О коммерческой тайне» (п. 7.6) базы данных сайтов отнесены к категории охраняемой законом коммерческой тайны.

Дайте уголовно-правовую оценку содеянному. Имеет ли значение для квалификации мотив совершения преступления?

4.Т., являясь начальником отдела продаж кормовых фосфатов ЗАО «ФосАгро АГ», имел доступ к рабочему компьютеру начальника управления продаж минеральных удобрений на экспорт дирекции по продажам ЗАО «ФосАгро АГ» Д.В. Аксенова. На данном компьютере была установлена настройка «Представитель», при помощи которой Т. незаконно получил доступ к рабочей электронной переписке Д.В. Аксенова с представителями иностранных компаний, занимающихся производством и продажей минеральных удобрений, содержащей сведения коммерческой тайны ЗАО «ФосАгро АГ» − особенностей коммерческих переговоров руководства ЗАО «ФосАгро АГ», сведений о производстве удобрений внутри ЗАО «ФосАгро АГ» и условиях их поставок на экспорт, не имея в соответствии с действующими нормативными документами ЗАО «ФосАгро АГ» к ним доступа. Данные сведения

он скопировал через корпоративную сеть на свой личный почтовый ящик.

В последующем данные сведения были им переданы В.В. Вершинину − сотруднику российского представительства американской компании «Transammonia» (головной офис в Швейцарии. Далее − компания «Трансаммония»), являющаяся крупным торговцем на мировом рынке минеральных удобрений и прочей продукции. В дальнейшем компания «Трансаммония» использовала вышеуказанные сведения для получения преимуществ над ЗАО «ФосАгро АГ» при заключении с ними сделок по закупке минеральных удобрений и прочей продукции.

Дайте уголовно-правовую оценку содеянному. Какие сведения относятся к сведениям, составляющим коммерческую тайну? Как определяется режим коммерческой тайны?

5.А. Петров, состоящий в должности инженера-химика ООО «Порт», М. Винокуров – инженер-механик ООО «Порт» под роспись были ознакомлены с договором о защите конфиденциальной информации, Положением о коммерческой тайне ООО «Порт»», а также письменно предупреждены о том, что они в течение трех лет с момента прекращения трудовых отношений обязаны не разглашать коммерческую тайну, полностью или частично, третьим лицам, не должны использовать информацию для своей собственной выгоды, кроме как в целях реализации своих должностных обязанностей. Они в период трудовой деятельности для использования в служебных целях были ознакомлены с патентами: № 2210501 «Способ изготовления длинномерных профильных изделий из композиционных материалов и устройство для его осуществления», № 2220049 «Стержень для армирования бетона», № 2404201 «Нанокомпозитный материал», № 2410505 «Арматурный элемент», а также им стали известны по работе иные сведения, составляющие коммерческую тайну ООО «Порт». После расторжения трудового договора с ООО «Порт» А. Петров и М. Винокуров в арендованных помещениях, незаконно используя сведения, составляющие коммерческую тай-

ну ООО «Порт», изготовили и реализовали от имени жены Петрова А., зарегистрированной в качестве индивидуального предпринимателя, композитную арматуру на сумму 3 090 014 руб., линию по производству композитной арматуры на сумму 2 500 000 руб., узлы и оборудование для последующей сборки двух линий по производству композитной арматуры на сумму 3 600 000 руб., причинив ООО «Порт» ущерб на общую сумму 9 190 014 руб.

Квалифицируйте действия Петрова и Винокурова.

6.26.05.2010 г. директор ООО «Правовой вестник Сибири» Б. позвонил главному государственному налоговому инспектору отдела камеральных проверок №2 Инспекции федеральной налоговой службы (ИФНС) России по Заельцовскому району г. Новосибирска С., которую спросил о возможности получения сведений об ООО НПК «Современные строительные технологии» (ИНН 5402158879), касающихся финансово-хозяйственной деятельности этой организации.

При встрече с Б. С. сообщила, что получить сведения о финансово-хозяйственной деятельности общества можно из движения денежных средств по его расчётным счетам. Наделенная полномочиями должностного лица, имевшего доступ к информации о налогоплательщике, С. предложила Б. передать ей вознаграждение в виде денег в сумме 15 тыс. руб., за что она в свою очередь направит запросы в банки для получения сведений о движении денег по расчетным счетам ООО НПК «Современные строительные технологии» и счетам возможного контрагента указанной организации - ООО «Альянс проект».

Находясь 09.06.2020 г. в очередном отпуске и не имея на тот момент в производстве каких-либо материалов проверок, в рамках которых в соответствии с пп. 1, 2 ст. 86 Налогового кодекса РФ можно было бы направлять запросы в кредитные организации и получать от них информацию, С. подготовила и подписала у своего руководства запросы в ОАО Банк «Алемар», Филиал ОАО «Ханты-Мансийский Банк» Центральное отделение №139 Сибирского банка Сбербанка России о

предоставлении сведений о движении денежных средств по расчетным счетам ООО НПК «Современные строительные технологии» (ИНН 5402158879), ООО НПК «Современные строительные технологии» (ИНН 5401321811) и ООО «Альянс проект» (ИНН 5405316770), которые были направлены в указанные кредитные учреждения. В период с 09.06.2020 г. по 28.06.2020 г., получив эти сведения, С. сообщила об этом Б., за что получила 15 000 руб.

Дайте уголовно-правовую оценку содеянному Б. и С. Что такое налоговая тайна?

Тема 5. Уголовно-правовая охрана сведений, составляющих государственную тайну

Государственная тайна – одна из самых защищаемых и особо охраняемых тайн. Сведения, составляющие государственную тайну, относятся к особо охраняемым сведениям, незаконное собирание и распространение которых влечет наиболее строгую уголовную ответственность.

В соответствии с Федеральным законом от 27.07.1993 № 5485-1 «О государственной тайне» под государственной тайной понимаются защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

Уголовный кодекс РФ предусматривает пять составов преступлений, предметом которых выступают сведения, составляющие государственную тайну, к которым относятся: ст. 275 УК РФ, предусматривающая ответственность за государственную измену; ст.276 УК РФ, содержащая признаки шпионажа; ст.283 УК РФ Разглашение государственной тайны; ст. 283.1 УК РФ, предусматривающая ответственность за незаконное получение сведений, составляющих государственную тайну и ст.284 УК РФ Утрата документов, содержащих государственную тайну. Все эти преступления описаны в разделе X Преступления против государственной власти, гл.29 Преступления против основ конституционного строя и безопасности государства.

Таким образом, родовым объектом рассматриваемых преступлений будут выступать общественные отношения, обеспечивающие безопасность государственной власти, видовым объектом являются отношения, обеспечивающие защиту основ конституционного строя и безопасности государства.

Статья 275 УК РФ предусматривает ответственность за государственную измену.

Основным непосредственным объектом будут выступать общественные отношения, обеспечивающие внешнюю безопасность Российской Федерации. Данное преступление ориентировано на защиту безопасности страны от внешних угроз.

Исходя из анализа ст.275 УК РФ, можно выделить три формы государственной измены.

Первая форма государственной измены − шпионаж. Признаки шпионажа содержатся в ст.276 УК РФ. В зависимости от предмета шпионажа можно выделить два вида.

В первом виде шпионажа предметом выступают сведения, составляющие государственную тайну.

Объективная сторона заключается в совершении одного из альтернативных действий, таких как собирание, похищение, хранение и передача сведений, составляющих государственную тайну иностранному государству, международной либо иностранной организации или их представителям. Собирание сведений заключается в любом способе их получения, это может быть подкуп лиц, имеющих к таким сведениям доступ, использование технических средств, предназначенных для негласного получения информации, путем неправомерного доступа к компьютерной информации и т.д. Похищение сведений предполагает их незаконное изъятие у лиц, имеющих к ним доступ путем кражи, грабежа, мошенничества. Хранение означает действия, обеспечивающие сохранность таких сведений, например, использование тайников, хранилищ и т.д. Передача предполагает сообщение сведений, составляющих государственную тайну иностранному государству, международной либо иностранной организации или их представителям. Обязательным признаком выступает адресность передачи. Особенностью данного состава является то, что сведения передаются именно иностранному государству, международной либо иностранной организации или их представителям. Преступление считается оконченным с момента совершения хотя бы одного действия, перечисленного в диспозиции.

Субъективная сторона характеризуется только прямым умыслом, лицо осознает, что собирает, похищает, хранит сведения, составляющие государственную тайну, обязательным признаком является цель – передача этих сведений иностранному государству, международной либо иностранной организации или их представителям.

Во втором виде шпионажа предметом выступают любые сведения, которые собираются по заданию иностранной разведки и передаются иностранной разведке или лицу, действующему в ее интересах. Таким образом, здесь могут быть любые сведения, которые представляют интерес для иностранной разведки. Объективная сторона состоит в их собирании и передаче иностранной разведке или лицу, действующему в ее интересах.

Субъектом государственной измены в форме шпионажа является физическое, вменяемое лицо, достигшее 16 лет, гражданин РФ.

Второй формой государственной измены является выдача сведений, составляющих государственную тайну иностранному государству, международной либо иностранной организации или их представителям доверенную лицу или ставшую известной ему по службе, работе, учебе или в иных случаях, предусмотренных законодательством Российской Федерации. Обязательным признаком выдачи является ее адресность, сведения выдаются иностранному государству, международной либо иностранной организации или их представителям. Субъектом выдачи может быть только лицо, которое имеет доступ к таким сведениям.

Третья форма государственной измены − это оказание лицом финансовой, материально-технической, консультационной или иной помощи иностранному государству, международной либо иностранной организации или их представителям в деятельности, направленной против безопасности Российской Федерации. Речь идет о любой помощи иностранным

государствам или их представителям в деятельности, враждебной Российской Федерации.

Субъективная сторона всех форм государственной измены характеризуется только прямым умыслом, направленным на деятельность, враждебную Российской Федерации.

Субъект – специальный, только гражданин РФ, достигший 16 лет.

Статья 276 УК РФ предусматривает уголовную ответственность за шпионаж, совершенный иностранным гражданином или лицом без гражданства. Отличие государственной измены в форме шпионажа от ст.276 УК РФ заключается только в субъекте. Субъектом государственной измены в форме шпионажа может быть только гражданин РФ, а субъектом шпионажа, предусмотренного ст.276 УК РФ, может быть только иностранный гражданин или лицо без гражданства.

Статья 283 УК РФ предусматривает ответственность за разглашение сведений, составляющих государственную тайну, лицом, которому она была доверена или стала известна по службе, работе, учебе или в иных случаях, предусмотренных законодательством Российской Федерации, если эти сведения стали достоянием других лиц, при отсутствии признаков преступлений, предусмотренных ст. 275, 276 УК РФ.

Объектом данного преступления будут выступать общественные отношения, обеспечивающие защиту сведений, составляющих государственную тайну и режим секретности. Обязательным признаком является предмет преступления, в качестве которого выступают сведения, составляющие государственную тайну.

Объективная сторона заключается в разглашении этих сведений, то есть сообщение их хотя бы одному лицу, не имеющему доступа к таким сведениям. Следует отметить, что если эти сведения передавались иностранному государству, международной либо иностранной организации или их представителям, то действия следует квалифицировать по ст.275

УК РФ, как выдача сведений, составляющих государственную тайну.

Субъективная сторона характеризуется умышленной формой вины. Следует отметить, что у лица нет цели передать эти сведения иностранным государствам или их представителям, которые бы их использовали в ущерб внешней безопасности РФ.

Субъект – специальный, это лицо, которому она была доверена или стала известна по службе, работе, учебе или в иных случаях, предусмотренных законодательством Российской Федерации.

Часть 2 ст.283 УК РФ содержит отягчающее обстоятельство, в качестве которого выступают тяжкие последствия, наступившие в результате разглашения сведений.

Статья 283.1 предусматривает ответственность за незаконное получение сведений, составляющих государственную тайну.

Объектом данного преступления будут выступать общественные отношения, обеспечивающие защиту сведений, составляющих государственную тайну. Обязательным признаком объекта будет предмет – это сведения, составляющие государственную тайну.

Объективная сторона заключается в незаконном получении данных сведений. В диспозиции ст.283.1 УКУ РФ приводится примерный перечень способов незаконного их получения, к которым относятся похищение, обман, шантаж, принуждение, угроза применения насилия либо иной незаконный способ. К иному незаконному способу можно отнести неправомерный доступ к компьютерной информации. Особенностью состава является то, что в действиях лица не должно быть признаков государственной измены или шпионажа. А это предполагает, что сведения собираются не для передачи иностранной организации, иностранному государству, международной организации или их представителям.

Состав преступления формальный, преступление считается оконченным с момента получения данных сведений лицом, не имеющим права доступа к ним.

Субъективная сторона – прямой умысел, лицо осознает, что получает сведения, составляющие государственную тайну.

Часть вторая предусматривает квалифицирующие признаки незаконного получения сведений, составляющих государственную тайну, к которым относятся: совершение данного преступления группой лиц; применение насилия; если оно повлекло наступление тяжких последствий; если совершено с использованием специальных и иных технических средств, предназначенных для негласного получения информации; и в случае если оно сопряжено с распространением сведений, составляющих государственную тайну, либо с перемещением носителей таких сведений за пределы Российской Федерации.

Еще один состав, предусматривающий уголовную ответственность за действия, посягающие на государственную тайну, содержится в ст.284 УК РФ, где речь идет об утрате документов, содержащих государственную тайну.

Объектом рассматриваемого преступления будут являться общественные отношения, обеспечивающие порядок обращения с документами, содержащими государственную тайну или с предметами, сведения о которых составляют государственную тайну.

Предметом соответственно будут документы, содержащие государственную тайну или предметы, сведения о которых составляют государственную тайну. Документы могут быть как на бумажных, так и на электронных носителях.

Объективная сторона заключается в нарушении правил обращения с указанными предметами. Данная норма является бланкетной и отсылает нас к правилам обращения с документами и предметами, сведения о которых составляют государственную тайну. Следует отметить, что в каждой организации, работающей со сведениями, составляющими государственную

тайну разработаны свои правила работы с ними. Эти правила касаются порядка их хранения, передачи, получения.

Обязательным признаком объективной стороны выступают последствия. В качестве последствий закон указывает на утрату документов, содержащих государственную тайну, либо утрата предметов, сведения о которых составляют государственную тайну и тяжкие последствия. В качестве тяжких последствий могут выступать такие последствия, как переход этих документов и предметов представителям иностранной разведки, серьезные затраты на восстановление этих документов или предметов и т.д. Таким образом, данный состав относится к числу материальных. Если последствия не наступили, то уголовная ответственность исключается.

Субъективная сторона рассматриваемого состава характеризуется неосторожной формой вины.

Субъект специальный, физическое, вменяемое лицо, достигшее 16 летнего возраста, имеющее доступ к государственной тайне.

Теоретические вопросы и задания

1.Ознакомьтесь с Законом РФ от 21.07.1993 г. «О государственной тайне». На основе положений закона раскройте понятие государственной тайны. Какие сведения составляют государственную тайну?

2.Проведите разграничение между составом государственной измены (ст.275 УК РФ) и составом разглашение государственной тайны (ст.283 УК РФ).

3.Проведите отграничение между составом государственной измены (ст.275 УК РФ) и составом незаконного получения сведений, составляющих государственную тайну (ст.283.1 УК РФ).

4.Подготовьте доклады по вопросам уголовно-правовой защиты информации ограниченного доступа в уголовном законодательстве зарубежных государств. Проведите сравнительно-правовой анализ.

Практические задания

1.Ф., являясь старшим научным сотрудником особо важного учреждения Минобороны России, имел доступ к секретным и совершенно секретным сведениям, составляющим государственную тайну. Будучи осведомленным о проявляемом иностранными спецслужбами интересе к тематике решаемых его учреждением вопросов, в поисках источников получения иностранной валюты для последующего выезда на постоянное жительство за границу, Ф. сумел войти в контакт с сотрудником посольской резидентуры ЦРУ, работавшим под прикрытием в дипломатической должности. Проинформировав его о своих возможностях, Ф. получил от него официальное предложение о сотрудничестве. Выразив согласие, Ф. на одной из назначенных ему конспиративных встреч передал представителю иностранной разведки собранные им секретные и особо секретные сведения об интересовавшем иностранную разведку изделии и направлениях его дальнейшей разработки. Тогда же Ф. получил присвоенный ему оперативный псевдоним, инструкции об условиях и порядке связи, а также денежное вознаграждение.

Квалифицируйте действия Ф.

2.А., отдыхая в Египте, решив произвести впечатление, рассказал случайным знакомым о том, что он сотрудник крупного российского концерна по производству оружия. В ходе беседы он сообщил о разработке новых видов оружия, их будущих характеристиках.

Дайте уголовно-правовую оценку содеянному.

3.Ж., имея двойное гражданство (России и Израиля) и проживая в США по заданию американской контрразведки, находился в России в гостях у своего родственника П., проживающего неподалеку от места дислокации особо важного военного объекта, пытался собрать сведения об эксплуатации этого объекта, его назначении. С этой целью он вел беседы с жителями городка, во время длительных пеших прогулок в

сторону военной базы фотографировал, записывал, какие машины, военная техника проезжают в сторону базы.

Квалифицируйте действия Ж.

4.В. (гражданин Германии) занимался сравнительным правоведением. Для написания научной статьи о коррупционной преступности России и Германии ему необходима была информация о состоянии преступности в России. С этой целью он познакомился со следователем по особо важным делам отдела по расследованию особо важных дел (о преступлениях против государственной власти и в сфере экономики) следственного управления Следственного комитета РФ П. В ходе беседы он попросил у П. предоставить ему отчет о состоянии коррупционной преступности в РФ за 5 последних лет, за что обещал ему заплатить 10 000 руб. П. согласился и, пользуясь служебным положением, получил эти сведения и передал их В.

Имеются ли в действиях П. и В. признаки составов преступлений. Какие сведения не могут относиться к государственной тайне и подлежать засекречиванию?

Тема 6. Уголовно-правовая охрана компьютерной информации

Компьютерным преступлениям посвящена гл.28 УК РФ, которая называется «Преступления в сфере компьютерной информации». Видовым объектом преступлений, входящих в эту главу, будут являться общественные отношения, обеспечивающие безопасность компьютерной информации.

Статья 272 УК РФ предусматривает ответственность за неправомерный доступ к компьютерной информации.

Объектом данного преступления выступают общественные отношения, обеспечивающие безопасность компьютерной информации. Обязательным признаком преступления является предмет – компьютерная информация, под которой в соответствии с примечанием к ст.272 УК РФ понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. Но предметом преступления будет не любая компьютерная информация, а только охраняемая. Под охраняемой законом понимается информация, для которой законом установлен специальный режим ее правовой защиты (например, государственная, служебная и коммерческая тайна, персональные данные и т.д.).

Объективная сторона состава преступления включает в себя: действие, состоящее в неправомерном доступе к охраняемой законом компьютерной информации (информации ограниченного доступа); последствие (альтернативно) в виде уничтожения, блокирования, модификации, копирования компьютерной информации, и причинно-следственную связь между указанным действием и любым из названных последствий.

Законодателем не уточнено понятие доступа к информации. Указанное понятие содержится в п. 6 ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»: «доступ к информации − возможность получения информации и ее использования». Соответственно, неправомерный доступ к компью-

терной информации − это незаконное либо не разрешенное собственником или иным ее законным владельцем использование возможности получения компьютерной информации.

Состав данного преступления носит материальный характер и предполагает обязательное наступление одного из последствий:

а) уничтожение информации − это приведение информации или ее части в непригодное для использования состояние независимо от возможности ее восстановления;

б) блокирование информации − результат воздействия на компьютерную информацию или технику, последствием которого является невозможность в течение некоторого времени или постоянно осуществлять требуемые операции над компьютерной информацией полностью или в требуемом режиме, то есть совершение действий, приводящих к ограничению или закрытию доступа к компьютерному оборудованию и находящимся на нем ресурсам, целенаправленное затруднение доступа законных пользователей к компьютерной информации, не связанное с ее уничтожением;

в) модификация информации − внесение изменений в компьютерную информацию (или ее параметры);

г) копирование информации − создание копии имеющейся информации на другом носителе, то есть перенос информации на обособленный носитель при сохранении неизменной первоначальной информации, воспроизведение информации в любой материальной форме − от руки, фотографированием текста с экрана дисплея, а также считывания информации путем любого перехвата информации и т.п.

Субъективная сторона характеризуется как умыслом, так и неосторожностью, так как в диспозиции статьи нет указания на форму вины.

Субъект − физическое, вменяемое лицо, достигшее 16 лет.

Часть 2 предусматривает квалифицированные составы неправомерного доступа к компьютерной информации, к ко-

торым относятся наличие крупного ущерба (свыше 1 млн. рублей) либо наличие корыстной заинтересованности у лица.

В части 3 содержатся особо квалифицированные признаки рассматриваемого состава, к которым относится совершение данного преступления группой лиц по предварительному сговору или организованной группой либо с использованием своего служебного положения. Под использованием служебного положения, предусмотренного в диспозиции ч. 3 ст. 272 УК РФ, понимается использование возможности доступа к компьютерной информации, возникшей в результате выполняемой работы (по трудовому, гражданско-правовому договору) или влияния по службе на лиц, имеющих такой доступ (в данном случае субъектом преступления не обязательно является должностное лицо), то есть тех, кто на законных основаниях использует компьютерную информацию и средства ее обращения (программисты, сотрудники, вводящие информацию в память компьютера, другие пользователи, а также администраторы баз данных, инженеры, ремонтники, специалисты по эксплуатации электронно-вычислительной техники и прочие).

В части четвертой содержится особо квалифицированный состав неправомерного доступа к компьютерной информации, если это повлекло тяжкие последствия или угрозу их наступления. К таким последствиям можно отнести причинение особо крупного материального ущерба, серьезное нарушение деятельности предприятий и организаций, наступление аварий и катастроф, причинение тяжкого и средней тяжести вреда здоровью людей или смерти, уничтожение, блокирование, модификация или копирование привилегированной информации особой ценности, реальность созданной угрозы.

Статья 273 УК РФ предусматривает ответственность за создание, использование и распространение вредоносных компьютерных программ.

Объектом данного преступления будут выступать общественные отношения, обеспечивающие безопасность в сфере компьютерной информации.

Объективная сторона заключается в создании, распространении или использовании компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации. Речь идет о «вирусах», то есть программах, которые приводят к уничтожению, блокированию или модификации компьютерной информации либо нейтрализации средств защиты компьютерной информации.

Создание программ представляет собой деятельность, направленную на разработку, подготовку программ, способных по своему функционалу несанкционированно уничтожать, блокировать, модифицировать, копировать компьютерную информацию или нейтрализовать средства защиты компьютерной информации.

Под распространением таких программ понимается предоставление доступа к ним любому постороннему лицу любым из возможных способов, включая продажу, прокат, бесплатную рассылку по электронной сети, то есть любые действия по предоставлению доступа к программе сетевым или иным способом.

Использование программы − это работа с программой, применение ее по назначению и иные действия по введению ее в хозяйственный оборот в изначальной или модифицированной форме. Под использованием вредоносных программ понимается их применение (любым лицом), при котором активизируются их вредные свойства.

Рассматриваемое преступление будет окончено с момента создания, использования или распространения таких программ или информации, создающих угрозу наступления указанных в законе последствий, вне зависимости от того, насту-

пили реально эти последствия или нет. Состав преступления формальный.

Субъективная сторона состава преступления, предусмотренного ч. 1 ст. 273 УК РФ, характеризуется виной в виде прямого умысла. При этом виновный должен осознавать, что создаваемые или используемые им программы заведомо приведут к указанным в законе общественно опасным последствиям. Мотив и цель не влияют на квалификацию преступления.

Субъект преступления общий − вменяемое лицо, достигшее 16 лет.

В части второй данной статьи предусмотрены квалифицирующие признаки, к которым относятся совершение деяния группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или совершенные из корыстной заинтересованности. В части четвертной в качестве особо квалифицированного признака указано на наступление тяжких последствий или угрозу их наступления.

В соответствии со ст. 274 УК РФ уголовная ответственность наступает за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Объектом нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, являются общественные отношения, обеспечивающие безопасное использование средств хранения, обработки или передачи компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также общественные отношения, обеспечивающие соблюдение правил доступа к информационно-телекоммуникационным сетям.

В качестве дополнительного объекта будут выступать отношения собственности. Состав нарушения правил эксплуатации средств хранения, передачи и обработки компьютерной

информации и информационно-телекоммуникационных сетей относится к числу двухобъектных преступлений.

В качестве предмета преступления законодателем указывается на средства хранения, обработки или передачи компьютерной информации, информационно-телекоммуникационные сети и оконечное оборудование. Под средства хранения, обработки или передачи компьютерной информации подпадает большое количество различного рода предметов, начиная от ЭВМ, ПК, смартфонов, ноутбуков и заканчивая банкоматами, флешкартами и картами памяти. Фактически это любые предметы, на которых может содержаться компьютерная информация, под которой, согласно примечанию к ст.272 УК РФ, понимаются сведения (сообщения, данные), представленные в форме электрических сигналов. Поэтому к таким средствам могут относиться и пластиковые карты со встроенными чипами и магнитными полосами, иммобилайзеры, датчики и т.д.

Что касается информационно-телекоммуникационных сетей, то данное определение содержится в ФЗ от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», где в ст. 4 сказано, что «информационно-телекоммуникационная сеть − технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники». Подобного рода системы могут быть локальными и глобальными, к которой относится и Интернет.

Оконечное оборудование в соответствии с ФЗ от 07.07.2003 №126 – ФЗ «О связи», это технические средства для передачи и (или) приема сигналов электросвязи по линиям связи, подключенные к абонентским линиям и находящиеся в пользовании абонентов или предназначенные для таких целей.

Объективная сторона заключается в двух видах нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей. Первый вид заключается в

нарушении правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб.

Второй вид выражается в нарушении правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб. Основное отличие этих двух видов заключается в действиях, последствия совпадают у обоих видов.

Следует отметить, что данная норма относится к числу бланкетных и отсылает к конкретным инструкциям и правилам, устанавливающим порядок работы со средствами хранения, обработки или передачи охраняемой компьютерной информации, информационно-телекоммуникационными сетями и оконечным оборудованием в ведомстве или организации. Эти правила должны устанавливаться правомочным лицом. Общих правил эксплуатации, распространяющихся на неограниченный круг пользователей глобальной сети Интернет, не существует. Правила доступа и эксплуатации, относящиеся к обработке информации, содержатся в различных положениях, инструкциях, уставах, приказах, ГОСТах, проектной документации на соответствующую автоматизированную информационную систему, договорах, соглашениях и иных официальных документах.

На сегодняшний день многие организации, учреждения предусматривают свои правила эксплуатации средств хранения, обработки, передачи компьютерной информации, к которым в частности относятся запреты на использование ресурсов сети Интернет во внеслужебных целях, запрет менять и обновлять программное обеспечение, использовать при работе на служебных компьютерах собственные носители информации (флешкарты, диски), нельзя допускать к работе с компью-

терной информацией лиц, не обладающих соответствующими правами и т.д.

Естественно, что лицо, нарушающее правила, должно быть ознакомлено с ними. Как правило, это указывается в должностной инструкции либо в договоре.

Законодатель также предусмотрел ответственность за нарушение правил доступа к информационно-телекоммуникационным сетям, тем самым расширив сферу применения данной статьи.

В объективную сторону ст.274 УК РФ, помимо деяния, заключающееся в нарушении правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, входят в качестве обязательного признака последствия. Последствия носят сложный характер и заключаются, во-первых, в уничтожении, блокировании, модификации либо копировании компьютерной информации, и, во-вторых, в крупном ущербе.

Крупный ущерб определен в примечании к ст.272 УК РФ, он составляет сумму свыше 1 млн руб.

Таким образом, состав ст.274 УК РФ является материальным составом и преступление считается оконченным с момента наступления неблагоприятных последствий.

Субъективная сторона характеризуется неосторожной формой вины, но может быть и умысел, так как в диспозиции статьи не указано на форму вины. Субъектом рассматриваемого преступления, исходя из диспозиции ст.274 УК РФ, является физическое, вменяемое лицо, достигшее возраста 16 лет.

В 2017 г. гл.28 УК РФ была дополнена новой статьей 274.1, которая предусматривает ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации. Понятие критической информационной инфраструктуры, ее правовое регулирование содержится в Федеральном законе от 26.07.2017 №187-ФЗ «О

безопасности критической информационной инфраструктуры Российской Федерации». На основе анализа действующего законодательства можно сделать вывод, что под критической информационной инфраструктурой следует понимать информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

В целом ст.274.1 УК РФ объединяет в себе признаки ст. ст. 272, 273, 274 УК РФ, но применительно к критической информационной инфраструктуре РФ.

Часть первая с.274.1 УК РФ предусматривает ответственность за создание, распространение и (или) использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в ней, или нейтрализации средств защиты указанной информации. То есть фактически речь идет о признаках ст.273 УК РФ. Особенностью является то, что вирусные программы создаются, распространяются и используются в целях воздействия на критическую информационную инфраструктуру РФ.

В части второй речь идет о неправомерном доступе к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, в том числе с использованием компьютерных программ либо иной компьютерной информации, которые заведомо предназначены для неправомерного воздействия на кри-

тическую информационную инфраструктуру Российской Федерации, или иных вредоносных компьютерных программ, если он повлек причинение вреда критической информационной инфраструктуре Российской Федерации. Фактически здесь описаны признаки ст.272 УК РФ, но применительно к объектам критической информационной инфраструктуры РФ.

Часть третья предусматривает ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, или информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, сетей электросвязи, относящихся к критической информационной инфраструктуре РФ, либо правил доступа к указанным информации, информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления, сетям электросвязи, если оно повлекло причинение вреда критической информационной инфраструктуре Российской Федерации. Здесь можно провести параллель со ст. 274 УК РФ.

Части четвертая и пятая ст.274.1 УК РФ предусматривают квалифицирующие признаки, такие как: совершение преступления группой лиц по предварительному сговору или организованной группой, или лицом с использованием своего служебного положения (ч.4 ст.274.1 УК РФ), если они повлекли тяжкие последствия (ч.5 ст.274.1 УК РФ).

Теоретические вопросы и задания

1.Дайте понятие компьютерной информации.

2.Что понимается под неправомерным доступом к компьютерной информации (ст.272 УК РФ)?

3.Раскройте понятия «уничтожение информации», «блокирование информации», «модифицирование информации», «копирование информации» как признаки объективной стороны ст.272 УК РФ.

4.Как определяется крупный ущерб применительно к ст.272, 273, 274 УК РФ?

5.В чем отличие создания от использования компьютерных программ или иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации (ст.273 УК РФ)?

6.В каких источниках содержатся правила эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации или информационно-телекоммуникационных сетей и оконечного оборудования, ответственность за нарушение которых предусмотрена ст.274 УК РФ?

7.Подготовьте доклады по вопросам уголовно-правовой защиты компьютерной информации в уголовном законодательстве зарубежных государств. Проведите сравнительно-правовой анализ.

Практические задания

1. С. занимал должность старшего инженера-программиста УГИБДД при ГУВД и по роду службы выполнял функции системного администратора, обладающего неограниченным правом доступа к информации, содержащейся в базе данных АИПС (автоматизированная информационно-поисковая система, содержащая информацию о всех протоколах о совершении гражданами административных правонарушений в области дорожного движения, в том числе за управление автотранспортом в состоянии алкогольного опьянения и информацию о результатах рассмотрения административного дела судом). Зная о том, что в случае обращения гражданина с заявлением об утере оригинала водительского удостоверения сотрудниками межрайонного экзаменационного отдела УГИБДЦ при ГУВД в обязательном порядке проводится проверка указанного гражданина по различным базам данных, в

том числе и по базе данных АИПС на предмет наличия административных правонарушений, связанных с лишением права управления транспортными средствами. А дубликат водительского удостоверения может быть выдан гражданину только в случае, если в указанной базе данных отсутствуют сведения о лишении гражданина права управления транспортными средствами. За вознаграждение С. согласился удалить из базы данных сведения о лишении гражданина А. водительского удостоверения. 23.07.2020 г. С., зная пароль администратора базы данных и имея доступ, единственно необходимый для удаления либо изменения информации без отметки в протоколе изменений, удалил из базы данных сведения о лишении гражданина А. водительского удостоверения, после чего ему выдали дубликат.

Имеются ли в действиях С. признаки состава преступления, предусмотренного ст.272 УК РФ? Что понимается под неправомерным доступом к компьютерной информации?

2.Б. и А. каждый признан виновным в покушении на тайное хищение чужого имущества (кражу) группой лиц по предварительному сговору, в особо крупном размере, а также в неправомерном доступе к охраняемой законом компьютерной информации, повлекшей копирование компьютерной информации, совершенным из корыстной заинтересованности, группой лиц по предварительному сговору.

Так, они в ноябре 2019 г. приобрели устройство (комплект) для получения (перехвата) информации с магнитных полос пластиковых платежных карт и соответствующих ПИН-кодов. 28 ноября они прибыли к дополнительному офису № 1209 Краснопресненского отделения Московского банка ОАО «Сбербанк России», где установили на банкомат № 890003 вышеуказанный комплект.

После чего, в этот же день в 11 час 51 мин, спустя некоторое время, достаточное для того, чтобы клиенты банков воспользовались услугами банкомата, а информация с их платежных банковских карт, необходимая для дальнейшего сня-

тия денежных средств, была скопирована с помощью установленного комплекта технических средств, Б., используя заранее приготовленную отвертку, снял установленный ранее комплект устройств, в то время как А. наблюдал за окружающей обстановкой. Однако оба были задержаны сотрудниками полиции.

Всего с помощью установленного комплекта оборудования была отсканирована 81 банковская карта клиентов ОАО «Сбербанк России», остаток денежных средств на которых составлял 1 975 156 руб. 69 коп.

Правильно ли квалифицированы действия указанных лиц?

3.26.06.2020 г. в раздевалке ОАО «Теплосети» Г. подсмотрел номер банковской карты «ВТБ-24», принадлежащей Р., срок её действия и код. Со своего мобильного телефона посредством использования услуги «Unique RUS MOSCOW FONBET», путем отправления SMS-сообщений специального формата, представленного в форме электрических сигналов Г. в период с 26.06.2020 по 03.09.2020 г., списал со счета банковской карты принадлежащие Р. денежные средства на общую сумму 17 650 руб.

Квалифицируйте действия Г.

4.Приговором суда установлено, что В.П., являясь генеральным директором ЗАО «Хром», в начале июля 2020 г. с целью создания условий для разрыва деловых отношений, установленных между ОАО «Ассо» и ООО «Аэро» по оказанию обществом услуг по продаже электронных авиабилетов ОАО «Ассо», и устранения конкурента своей фирмы в данной сфере, принял решение дискредитировать ООО «Аэро» как надежную фирму. Для этого В.П., вступив с подчиненным ему ведущим специалистом службы информационной безопасности ЗАО «Хром» П., а также с А.И. и А.Д., занимавшихся оказанием «хакерских услуг», в предварительный сговор, в период с 15 июля 2020 г. по 24 июля 2020 г. осуществили, имея в своем пользовании созданную А.И. и А.Д. сеть зараженных

компьютеров (бот-сеть), компьютерную DdoS-атаку (типа «отказ в обслуживании») на информационные ресурсы ООО «Ассо», которая заключалась в одномоментном обращении множества компьютеров, входящих в бот-сеть, с запросом на обслуживание. В результате этого работа системы ЭВМ ООО «Ассо», объединенной в единую платежную сеть, была блокирована, в связи с чем её пользователям было отказано в возможности приобретения электронных билетов на сайте ОАО «Ассо». Осуществление данной компьютерной атаки привело к блокированию работы системы оплаты и приобретения электронных билетов на сайте ОАО «Ассо» на весь период атаки.

Квалифицируйте действия указанных лиц.

5.Б., ради интереса, путем подбора пароля вскрыл электронную почту своего коллеги У. и ознакомился с его перепиской и узнал, что У. является пользователем услуг эротического сайта.

Дайте уголовно-правовую оценку содеянному. Можно ли квалифицировать действия Б. по ст.272 УК РФ, предусматривающей ответственность за неправомерный доступ к компьютерной информации?

6.Анисимов А.В. на основании трудового договора № 76/43 от 12.04.2019 работал и занимал различные должности в отделе технической поддержки UNIX Общества с ограниченной ответственностью (далее - ООО) «Приват Трейд».

26.09.2019, согласно изменению к договору, Анисимов А.В. был переведен на должность ведущего системного администратора UNIX отдела технической поддержки UNIX.

С Анисимовым А.В. было заключено соглашение о сохранении служебной и коммерческой тайны, которое обязывает сотрудника ООО «Приват Трэйд» не разглашать сведения, содержащие служебную тайну, какому-либо лицу и подчиняться правилам, существующим на предприятии, и указаниям должностных лиц, направленных на защиту служебной

тайны (п.3), которое было им – Анисимовым А.В. изучено и собственноручно подписано. Анисимов А.В. был ознакомлен с должностной инструкцией, согласно которой ведущий системный администратор UNIX поддерживает в рабочем состоянии программное обеспечение рабочих станций с серверов (п.2.6), обеспечивает своевременное копирование, архивирование и резервирование данных (п.2.8), обеспечивает сетевую безопасность (п.2.18), сохраняет конфиденциальность служебной информации (п.2.26), которое было им – Анисимовым А.В. изучено и собственноручно подписано.

С Анисимовым А.В. было заключено соглашение о конфиденциальности для работников ООО «Приват Трейд», согласно которому конфиденциальной информацией является техническая, технологическая, коммерческая (финансовая), организационная или иная используемая в коммерческой деятельности информация, которая обладает действительной или потенциальной коммерческой ценностью в силу ее неизвестности неограниченному кругу третьих лиц и к которой нет свободного доступа на законном основании (ч.1), вне зависимости от степени её защиты в соответствии с законами РФ (ч.2), которая будет использоваться в целях наиболее полного и качественного оказания услуг и защищена от распространения и передачи третьим лицам (ч. 4), доступ к которой будет ограничен минимально необходимым кругом лиц (п.1 ч.4), передача которой исключена (п.3 ч.4), как и ее самостоятельное использование (ч.4 п.5), которое было им – Анисимовым А.В. изучено и собственноручно подписано.

25.11.20 Анисимов А.В. скопировал на USB-носитель информацию из базы данных ООО «Приват Трэйд», а именно: не менее 45 000 записей, содержащих не прошедших проверку имен, фамилий, никнеймов (имена, которые используется при регистрации на интернет-сайтах), а также адресов электронной почты. После чего Анисимов А.В. передал вышеуказанную информацию В.

Вышеуказанные действия Анисимова А.В. причинили ущерб ООО «Приват Трэйд», который выражается в следующих вынужденных действиях, которые были проведены сотрудниками ООО «Приват Трэйд», а именно:

- восстановление доступа к базе данных ООО «Приват Трэйд» после смены всех паролей сотрудников, имеющих доступ к VPN-серверам, а также смена паролей в учетных записях серверов и сервисов ООО «Приват Трэйд» (общие затраты 388 000 руб.);

- проведение комплекса мероприятий, направленных на поиск лица (Анисимова А.В), которое копировало информацию из базы данных ООО «Приват Трэйд» (общие затраты 153 000 руб.);

- средний простой 115 сотрудников ООО «Приват Трэйд», имеющих доступ к VPN-серверам, из-за необходимости перенастройки VPN-серверов, составил 12 часов, то есть суммарно 920 часов на ожидание восстановления доступа к VPN-серверам, которые были оплачены ООО «Приват Трэйд» (общие затраты 414 000 руб.);

- покупка оборудования для сотрудников ООО «Приват Трэйд» взамен изъятого у Анисимова А.В. по окончании служебной проверки (общие затраты 45 330 руб.);

- введение дополнительных средств учета лиц, осуществляющих доступ к базе данных ООО «Приват Трэйд», а также механизмов сохранения информации, направленных на недопущение копирования информации без согласования с руководством ООО «Приват Трэйд» (общие затраты 155 270 руб.).

Дайте уголовно-правовую оценку содеянному.

7.А.Н. Половинкин, обладающий навыками в пользовании компьютерной техникой, имеющий персональный компьютер, выделенный канал доступа к сети Интернет, предоставленный провайдером ЗАО «Ростелеком», в период с апреля 2015 г. по август 2019 г. скопировал и установил на накопительный жесткий магнитный диск своего персонального компьютера программу, позволяющую обмениваться файлами

между пользователями данной системы, запустил данную программу и зарегистрировался в системе под псевдонимом «pion» пользователя IP-адресом 95.79.140.209. При регистрации, в соответствии с условиями использования системы, А.Н. Половинкин ознакомился с правилами работы в системе и был предупрежден о категорическом запрете размещения нелегальных материалов и об уголовной ответственности за совершение преступлений, предусмотренных прим.1 ст. 242, ст. 242, 146, 272 – 274 УК РФ.

А.Н. Половинкин в период с апреля 2015 г. по 2019 г. путём копирования с носителей информации на накопительный жёсткий магнитный диск своего персонального компьютера создал 1 файл, присвоив ему имя «Порно Малолетка В клубе в приват-комнате.wmv», размером 9,26 Мб, представляющий собой видеоролик продолжительностью 33 с, содержащий элементы порнографического характера.

А.Н. Половинкин предоставил возможность любому желающему пользователю системы для повышения своего рейтинга скопировать и приобрести указанные файлы в целях заработать рейтинг пользователя (абонента) ЗАО «Ростелеком».

Квалифицируйте действия Половинкина.

8.В сентябре-ноябре 2020 г. Ф., являясь программистом, совершил изменение в программе начисления заработной платы на предприятии так, что у работников, которым начислялась заработная плата свыше 1 000 руб., списывалось по 10 руб. Эти средства поступали на счет, откуда их впоследствии снял Ф.

Квалифицируйте действия Ф.

9.Л., работая врачом-рентгенологом в ООО «Мультимед», решил записать данные исследования пациента, произведенного на спиральном компьютерном томографе. Предварительно не проверив флешкарту на наличие «вирусов», вставил карту в системный блок. В результате записи данных исследования на флешкарту в программном обеспечении компьютерного томографа произошел сбой, который привел к выводу из

строя дорогостоящего медицинского оборудования и необходимости длительного его ремонта с привлечением специалистов авторизованного технического сервиса.

Дайте оценку действиям Л. Каковы условия привлечения к уголовной ответственности по ст. 273 УК РФ?

Список нормативно-правовых актов и иных официальных документов

1.Конституция РФ (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // СПС «Гарант».

2.Уголовный кодекс РФ от 13.06.1996 № 63-ФЗ (с последними изменениями и дополнениями).

3.Налоговый кодекс РФ от 31.07.98 г. №146-ФЗ.

4.Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г. №149-ФЗ.

5.Закон РФ «О государственной тайне» от 21.07.1993 г. №5485-I.

6.ФЗ «О коммерческой тайне» от 29.07.2004 №98-ФЗ.

7.ФЗ «О персональных данных» от 27.06.2006 №152-ФЗ.

8.ФЗ «О банках и банковской деятельности» от 02.12.1990 №395-1.

9.ФЗ «Об основах охраны здоровья граждан в Российской Федерации» от 21.11.2011 №323-ФЗ.

10.ФЗ «О государственной защите судей, должностных лиц правоохранительных и контролирующих органов» от 20.04.1995 г. №45-ФЗ.

11.ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства» от 20.08.2004 г. №119-ФЗ.

12.ФЗ от 06.03.2006 №35-ФЗ «О противодействии терроризму».

13.ФЗ от 25.07.2002 №114-ФЗ «О противодействии экстремистской деятельности».

14.ФЗ «О полиции» 07.02.2011 №3-ФЗ.

15.ФЗ «Об оперативно-розыскной деятельности» от 12.06.1995 №144-ФЗ.

16.Закон РФ «О частной детективной и охранной деятельности в РФ» от 11.03.1992 г. №248-I.

17.Постановление Пленума Верховного Суда РФ от 24.02.2005 №3 «О судебной практике по делам о защите чести и достоинства граждан, а также деловой репутации граждан и юридических лиц».

18.Постановление Пленума Верховного Суда РФ от 28.06.2011 г. №11 «О судебной практике по делам о преступлениях экстремисткой направленности».

19.Постановление Пленума Верховного Суда РФ от 09.02.2012 «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности».

Список рекомендуемой литературы

1.Бачило И. Л. Информационное право: учеб. для акад. бакалавриата вузов по юрид. направлениям и спец. / 5-е изд., перераб. и доп. М.: Юрайт, 2019.

2.Боровиков В. Б. Уголовное право. Особенная часть / В.Б. Боровиков, А. А. Смердов. М.: Изд-во «Юрайт», 2019. URL: https://www.biblioonline.ru.URL:https://www.bibliooline.ru/book/ugolovnoe-pravo-osobennaya-chast-433641;https://www.biblio-online.ru/book/cover/CF63F77A-B15D-4980-B1FD-BDB11A648096. Рус яз. ISBN 978-5-534-05286-2.

3.Внуков А. А. Защита информации. М.: Изд-во «Юрайт», 2018. 2-е изд. URL: http://www.biblio-online.ru/book/73BEF88E-FC6D-494A-821CD213E1A984E1. Рус яз. ISBN 978-5-534-01678-9.

4. Ефремова М. А. Уголовно-правовая охрана информационной безопасности: спец. 12.00.08 - Уголов. право и криминология; уголов.-исполнит. право : автореф. дис. …д-ра юрид. наук / М. А. Ефремова ; науч. консультант П. В. Агапов. М., 2018. 59 с.

5. Камалова Г. Г. Информационное право в схемах, определениях и заданиях: учеб. пособие / Г. Г. Камалова, М-во образования и науки РФ, ФГБОУ ВО «Удмуртский государ-

ственный университет», Ин-т права, соц. упр. и безопасности, Каф. криминалистики и судеб. экспертиз. Ижевск: Удмуртский университет, 2017.

6. Мухин А. А. Основы информационной безопасности: учеб. пособие / А. А. Мухин, М-во образования и науки РФ, ФГБОУ ВО «Удмуртский государственный университет», Ин-т экономики и управления, Каф. гос. и муницип. управления. Ижевск: Удмуртский университет, 2018.

7. Наумов А. В. Уголовное право: в 2 т. Т. 2: Особенная часть / А. В. Наумов, Р. З. Абдулгазиев, Е. А. Антонян, П. В. Волосюк, Т. Г. Жукова, О. К. Зателепин, Л. В. Иногамова-Хегай, Н. А. Лопашенко, И. Л. Мармута, А. Ю. Морозов, Н. И. Пикуров, Ю. В. Сапронов, А. Ю. Сичкаренко, А. А. Толкаченко, М. И. Третьяк, А. В. Шульга, Б. В. Яцеленко. М.: Юрайт, 2019. URL: https://www.biblio-online.ru. URL: https://www.biblio-online.ru/book/ugolovnoe-pravo-v-2-t-tom-2-osobennaya-chast-438660;https://www.biblioonline.ru/book/cover/A573BCC9-D813-4FA7-875E-4F78576AACDC. Рус яз. ISBN 978-5-534-04855-1.

8. Нерсесянц А. А. Защита информации. Ростов-на-Дону: Северо-Кавказский филиал Московского технического университета связи и информатики, 2010. Книга находится в Премиум-версии ЭБС IPRbooks. Рус яз.

9. Подройкина И. А. Уголовное право. Особенная часть в 2 т. Т.2 / И. А. Подройкина, Н. В. Артеменко, Ю. И. Блохин, Е. В. Безручко, А. П. Бохан, А. В. Грошев, В. Д. Иванов, П. В. Иванов, И. И. Исраилов, Е. Р. Кейдунова, А. М. Разогреева, И. А. Фаргиев, Н. Г. Шимбарева. М.: Юрайт, 2019. URL: https://www.biblio-online.ru. URL: https://www.biblio-online.ru/book/ugolovnoe-pravo-osobennaya-chast-v-2-t-tom-2-436512;https://www.biblio-online.ru/book/cover/ADCA1546-A939-4295-8A6B-F691B00402EB. Рус яз. ISBN 978-5-534-02303-9.

10. Русскевич Е. А. Уголовное право и информатизация // Журнал Российского права. 2017. № 8. С. 73-80.

11. Стяжкина С. А. Охрана информации уголовно-правовыми средствами: практикум / С. А. Стяжкина, М-во образования и науки РФ, ФГБОУ ВО «Удмуртский государственный университет», Ин-т права, соц. упр. и безопасности. Ижевск: Jus est, 2016. 35 с.

12. Уголовное право России. Особенная часть: учеб. для бакалавриата, специалитета и магистратуры вузов по юрид. направлениям. Т. 2: Преступления против общественной безопасности и общественного порядка. Преступления против государственной власти. Преступления против военной службы. Преступления против мира и безопасности человечества / П. В. Агапов, Т. А. Боголюбова, Т. А. Диканова [и др.]; под ред. О. С. Капинус. 2-е изд., перераб. и доп. М.: Изд-во «Юрайт», 2019.

Содержание

Учебное издание

Светлана Александровна Стяжкина

ОХРАНА ИНФОРМАЦИИ
УГОЛОВНО-ПРАВОВЫМИ СРЕДСТВАМИ
Учебное пособие

Авторская редакция
Подписано в печать 00.00. 2021. Формат 60x84 1/16.
Усл. печ. л. 4,12. Уч.-изд. л. 3,32.
426034, Ижевск, Университетская, д. 1, корп. 4, каб. 207
Тел./факс: + 7 (3412) 500-295 E-mail: editorial@ud