DOI: 10.35854/2219-6242-2020-3-84-93 УДК 004.056

О. А. Чабукиани, Е. А. Зорина, В. В. Солодовник

Способы противодействия киберпреступности

O. A. Chabukiani, E. A. Zorina, V. V. Solodovnik. **Ways of Counteraction to Cybercrime**

В статье рассмотрены способы противодействия киберпреступности. Обращено внимание на то, что в настоящее время в России отсутствует правовая база, которая бы в полной мере регулировала все цифровые отношения, выступающие объектом одного из самых опасных видов международной преступности — киберпреступности. Противодействие ей возможно лишь при проведении совместных исследований учеными в области различных наук.

Ключевые слова: правовое регулирование, киберпреступность, информационная безопасность, противодействие киберпреступности.

Контактные данные: **Чабукиани О. А.:** 190005, Санкт-Петербург, 7-я Красноармейская ул., д. 6/8; (812) 458-97-18; e-mail: oksana_kartohina@mail.ru | **Зорина Е. А.:** 196105, Санкт-Петербург, Московский пр., д. 149; (812) 369-96-37; e-mail: zorina_lena@mail.ru | **Солодовник В. В.:** 188662, г. Ленинградская область, ул. Лесная, д. 18; (812) 595-51-04; e-mail: slaviik_bel@mail.ru.

The article discusses ways to counter cybercrime. Attention is drawn to the fact that at present in Russia there is no sufficient legal framework that regulates all digital relations that are the object of one of the most dangerous types of international crime - cybercrime, thus countering it is possible only with joint studies of scientists of various sciences.

Keywords: legal regulation, cybercrime, information security, countering cybercrime.

Contact Details: **Chabukiani O. A.:** 7 Krasnoarmeyskaya 6/8, St. Petersburg, Russia, 190005; (812) 458-97-18; e-mail: oksana_kartohina@mail.ru | **Zorina E. A.:** Moskovskiy Ave 149, St. Petersburg, Russia, 196105; (812) 369-96-37; e-mail: zorina_lena@mail.ru | **Solodovnik V. V.:** Lesnaya Str. 18, Leningrad Region, Russia, 188662; (812) 595-51-04; e-mail: slaviik_bel@mail.ru.

Изучение способа совершения преступлений является предметом нескольких наук: уголовного права (способ как признак объективной стороны преступления), криминологии (способ совершения общественно опасного деяния помогает определить личность лица, совершающего преступления, виктимологические признаки и выявить наиболее эффективные профилактические меры), уголовного процесса (определяет особенности доказательственного права, количества следственных действий и последовательность принятия процессуальных решений), криминалистики (от способа совершения зависят выдвигаемые следственные версии, выбираемые тактические способы производства и техническая оснащен-

Оксана Алексеевна Чабукиани — доцент кафедры уголовного права и уголовного процесса Санкт-Петербургского государственного экономического университета, кандидат юридических наук, доцент.

Елена Андреевна Зорина — начальник кафедры трудового права Санкт-Петербургского университета Государственной противопожарной службы МЧС России, кандидат юридических наук, доцент.

Вячеслав Викторович Солодовник — доцент кафедры общеправовых дисциплин Ленинградского областного филиала Санкт-Петербургского университета МВД Российской Федерации, кандидат юридических наук.

ность при выявлении, раскрытии и расследовании преступлений), теории оперативно-розыскной деятельности.

Способы противодействия киберпреступлениям будут зависеть от вида предотвращаемого общественно опасного деяния: хакинга, кардлинга, фрикинга, диффамации, спаминга, фишинга, киберхулиганства, кибертерроризма, нюкинга и других. Безопасность в интернете может быть достигнута путем предупредительных мер на различных уровнях (общесоциальном, специальном, индивидуальном). С учетом специфики способа совершения киберпреступлений важное значение в профилактике и выработке мер безопасности имеет должное взаимодействие правоохранительных органов, как на государственном уровне, так и на международном.

На международном уровне активно принимаются меры, направленные на предупреждение, выявление и пресечение таких преступлений, как:

1) использование ботнетов — сетей устройств, зараженных вредоносными программами без ведома их пользователей для передачи вирусов, которые получают незаконное дистанционное управление устройствами, крадут пароли и отключают антивирусную защиту;
2) создание «бэкдоров» на скомпрометированных устройствах для кражи денег и данных или удаленного доступа к устройствам для создания ботнетов;
3) создание онлайн-форумов для торговли хакерским опытом;
4) непробиваемый хостинг и создание контрантивирусных сервисов;
5) отмывание традиционных и виртуальных валют;
6) совершение онлайн-мошенничества, например, через платежные системы в режиме онлайн и социальную инженерию (картинг);
7) различные формы сексуальной эксплуатации детей в интернете, включая распространение в интернете материалов о сексуальном насилии над детьми и прямую трансляцию сексуального насилия над детьми;
8) интернет-операции, связанные с продажей оружия, фальшивых паспортов, поддельных и клонированных кредитных карт, а также наркотиков и хакерских услуг.

В России на законодательном уровне защита персональных данных физических и юридических лиц, а также безопасности при операциях с денежными средствами гарантируется Федеральными законами «О персональных данных» от 27 июля 2006 г. № 152 (в редакции от 24 апреля 2020 г.) [1], «О банках и банковской деятельности» от 2 декабря 1990 г. № 351-1 (в редакции от 27 декабря 2019 г.) [2], «О Центральном банке Российской Федерации (Банке России)» от 10 июля 2002 г. № 86-ФЗ (с изменениями и дополнениями от 20 июля 2020 г.) [3], «О национальной платежной системе» от 27 июня 2011 г. № 161-ФЗ (с изменениями и дополнениями от 20 июля 2020 г.) [4], «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 г. № 187-ФЗ [5], Кодексом РФ об административных нарушениях от 30 декабря 2001 г. № 195-ФЗ (в редакции от 31 июля 2020 г.) [6], Уголовным кодексом РФ от 13 июня 1996 г. (в редакции от 31 июля 2020 г.) [7] и др.

В рамках международного сотрудничества гарантии противодействия определены в Модельном законе стран-участников СНГ «О персональных данных» [8]; Соглашении о сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере компьютерной информации, заключенном 1 июня 2001 г. [9]; Дополнительном протоколе к Конвенции о преступлениях в сфере компьютерной информации относительно введения уголовной ответственности за правонарушения, связанные с проявлением расизма и ксенофобии, совершенные посредством

компьютерных систем (ETS № 189), от 28 января 2003 г. [10]; Директиве Европейского парламента и Совета Европейского союза 2002/58/ЕС «В отношении обработки персональных данных и защиты конфиденциальности в секторе электронных средств связи», принятой в Брюсселе 12 июля 2002 г. (с изменениями и дополнениями от 25 ноября 2009 г.) [11]; Директиве 2013/40/ЕС «Об атаках на информационные системы и о замене Рамочного решения 2005/222/ПВД Совета ЕС» [12]; Рамочном решении Совета Европейского союза 2001/413/JHA «О противодействии мошенничеству и подделке безналичных платежных средств» от 28 мая 2001 г. [13]; Регламенте Европейского парламента и Совета Европейского союза 2016/679 «Об общей защите данных».

Быстрое развитие информационных технологий, использование различных электронных девайсов, доступ в сеть Интернет делает уязвимым не только имущество, но и персональные данные, личную информацию. В соответствии с «Основными направлениями информационной безопасности кредитно-финансовой среды на период 2019–2021 годов» формирование регуляторного воздействия в сфере информационной безопасности и киберустойчивости осуществляется по следующим направлениям [14]:

1) выявление в сети Интернет сайтов, используемых для мошеннических действий в кредитно-финансовой сфере. Требуется ограничение в пределах, установленных нормативно-правовыми актами, доступа потребителей финансовых услуг к таким сайтам. Для реализации данного положения требуется закрепление за Банком России определенных полномочий, позволяющих своевременно блокировать в сети Интернет различные сайты, связанные с предоставлением некачественных финансовых услуг либо используемые для распространения информации о финансовых пирамидах, вредоносных программах и т. п.;
2) выстраивание единого канала обмена информации, требуемой для оперативного реагирования на выявленные факты киберпреступлений: о мобильном устройстве, абоненте номера мобильного телефона. Сведения должны в случае необходимости передаваться между операторами связи и банками, некредитными финансовыми организациями;
3) формирование комплексных предложений Банка России по совершенствованию механизмов использования усиленной квалифицированной электронной подписи и действующего законодательства по выстраиванию единой системы удостоверяющих центров и кредитно-финансовой сфере;
4) создание условий для должного, безопасного оборота цифровых финансовых активов путем установления необходимых требований к информационной безопасности и защите информации. Требования Банка России к защите информации должны зависеть от уровня рисков, объема и характера осуществляемых организаций кредитно-финансовой сферы операций, уровня и сочетания присущих ее деятельности рисков;
5) координация деятельности участников финансового рынка в рамках национальной программы «Цифровая экономика Российской Федерации».

Способы противодействия таким преступлениям будут определяться в зависимости от выбранного преступниками способа совершения преступления (уничтожения, блокирования, копирования, модификации, использования информации через непосредственный доступ к компьютерной информации или опосредованный доступ); способа использования и сокрытия полученной через компьютерные системы информации; мотивов совершения преступления (корыстных, т. е. распространение вредоносных программ, получение безвозмездного программного обеспечения, бесплатного доступа в Интернет, хищение денежных средств; хули-

ганских побуждений, мести, коммерческого шпионажа, содействия террористической деятельности, иных).

Сложность предупреждения, выявления и расследования киберпреступлений определяется с учетом следующих обстоятельств:

1) место совершения преступления и место наступления общественно опасных последствий существенно отделено и может быть не только на территории одного государства;
2) скорость обмена криминологической информацией, имеющей значение для конкретного уголовного дела в случаях удаленности органа уголовного преследования от виновного или потерпевшего;
3) сложность в формировании доказательственной базы, требующей направления запросов о правовой помощи, необходимости проверки совершаемых процессуальных действий иными субъектами процесса;
4) получение согласительных процедур по получению доступа к компьютерной информации;
5) оказание помощи в розыске и задержании скрывающегося на территории иного государства преступника;
6) обеспечение соблюдения сроков и процедуры выдачи виновного иностранному государству;
7) обеспечение восстановления нарушенных прав всех лиц, потерпевших в результате совершения киберпреступления [15, с. 179–180; 16, с. 1186–1187; 17, с. 39].

Сложность противодействия будет зависеть от личности лица, совершившего киберпреступления, виктимологических особенностей личности, проводимых оперативно-розыскных мероприятий, направленных на выявление и раскрытие преступлений, а также возможностей легализации результатов их проведения [18, с. 15–16].

Помимо практической сложности противодействия киберпреступности, трудности возникают и на научном уровне. Например, чтобы выработать единую нормативно-правовую базу противодействия, необходимо обеспечить единообразное понимание материального права. При разных правовых семьях это сложно: разный подход к содержанию общественной опасности, возрасту уголовной ответственности, конструкции составов, разнообразие способов совершения преступления, исходя из технического прогресса конкретного государства, разное понимание вины в уголовном праве. Как следствие — разные качественные и количественные показатели преступности, разное понимание профилактической работы, сложности в определении признаков личности преступника, виктимологических признаков. Уголовно-правовые и криминологические аспекты ведут к отсутствию единых элементов криминалистической характеристики, разному подходу к институту доказательств в уголовном процессе.

Таким образом, противодействие киберпреступности возможно лишь при проведении совместных исследований учеными в области различных наук: социологии, психологии, уголовного права, криминологии, уголовного процесса, криминалистики. Отсутствие единых научных разработок не может привести к единому практическому пониманию проблемы. Так, согласно Информационному письму Банка России от 14 августа 2018 г. № ИН-014-12/54 «О национальной оценке рисков ОД/ФТ», уязвимым местом при противодействии легализации (отмыванию) преступных доходов, рисков финансирования терроризма является «длительное рассмотрение запросов о правовой помощи и сложности с получением такой помощи, а также информации в отношении конечных бенефициаров от компетентных органов отдельных стран».

Все меры противодействия могут быть представлены по таким направлениям, как правовые, организационные, криминалистические [19, с. 27–29]. В правовом аспекте следует выработать единую концепцию по взаимодействию при выявлении, пресечении, раскрытии и разрешении киберпреступлений, определении единой формы запроса и возможного предоставления информации, имеющий значение для уголовного дела; выработке надежных способов защиты персональных данных и проведению совместных научных исследований по выявлению положительного опыта противодействия киберпреступлениям.

В июле 2015 г. на базе Главного управления безопасности создан Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (FinCERT), основными задачами которого служит анализ данных о кибератаках и подготовка аналитических материалов, предоставление рекомендаций по обеспечению безопасности при осуществлении денежных переводов, координация обмена информацией между правоохранительными органами и финансовыми организациями. Результаты работы отражаются в отчетах, опубликованных для всеобщего информирования.

Несмотря на геополитические факторы, Российская Федерация активно участвует в международном взаимодействии по обмену информацией о киберугрозах, содействует внедрению единых стандартизированных подходов в области обеспечения кибербезопасности, а также выстраиванию обмена опытом по регулированию и внедрению финансовых технологий. Банк России участвует в международном взаимодействии по следующим направлениям:

1) обеспечение участия экспертов Банка России в деятельности международных организаций по вопросам противодействия киберпреступлениям (например, Международная организация по стандартизации, Международная электротехническая комиссия, Международный союз электросвязи и др.;
2) укрепление кибербезопасности путем взаимодействия с центральными (национальными) банками иностранных государств при предоставлении финансовых услуг;
3) координация деятельности подразделений безопасности по созданию центров реагирования по компьютерным инцидентам в национальных банках стран — участников ЕАЭС;
4) взаимодействие с международными компаниями при подготовке и проведении обучения по реагированию на киберугрозы.

Большой вклад в это направление вносят Интерпол и Европейский центр по борьбе с киберпреступностью (European Cybercrime Centre, EC3), созданный в январе 2013 г. С момента создания EC3 участвовал в десятках громких операций и сотнях развертываний оперативной поддержки на месте, что явилось результатом сотни арестов; проверке сотни тысяч файлов, большинство из которых оказались вредоносными.

В организационном плане на государственном уровне необходимо проводить разъяснительные беседы с лицами, приобретающими цифровую и микропроцессорную технику, повышать правовую культуру населения, вырабатывать требования к подбору, проверке и инструктажу персонала, допускаемому к ресурсам, содержащим персональные данные, проводить плановые и внеплановые проверки соблюдения режима секретности при функционировании компьютерных систем. Целесообразна проверка должного исполнения действующего законодательства в части охраны, передачи и сбора персональных данных. Ежегодно EC3 публикует оценку угрозы организованной преступности в интернете (IOCTA), свой флагманский стратегический доклад о ключевых выводах и новых угрозах, событиях в области киберпреступности [20].

В докладе основное внимание уделяется областям преступности, которые подпадают под мандат ЕСЗ. В настоящее время в цикле политики ЕС-влияния определены приоритеты киберпреступности: киберзависимая преступность, детская сексуальная эксплуатация в режиме онлайн, платежное мошенничество.

Киберзависимая преступность включает в себя:

1) использование бот-сетей — сетей устройств, зараженных вредоносными программами без ведома их пользователей, для передачи вирусов, которые получают незаконный удаленный контроль над устройствами, крадут пароли и отключают антивирусную защиту;
2) создание «задних дверей» на скомпрометированных устройствах для обеспечения кражи денег и данных или удаленного доступа к устройствам в целях создания бот-сетей;
3) создание онлайн-форумов для обмена опытом в области хакерства;
4) пуленепробиваемый хостинг и создание антивирусных сервисов;
5) отмывание традиционных и виртуальных валют;
6) совершение мошенничества в интернете, например, с помощью систем онлайн-платежей, карточных и социальных сетей;
7) различные формы сексуальной эксплуатации детей в интернете, включая распространение материалов о сексуальном насилии над детьми и прямую трансляцию сексуальных надругательств над детьми;
8) онлайн-хостинг операций, связанных с продажей оружия, поддельных паспортов, поддельных и клонированных кредитных карт, наркотиков и услуг по взлому.

В области сексуальной эксплуатации детей Европол выявил следующие ключевые угрозы: 1) одноранговые (P2P) сети и анонимный доступ, такие сети, как Darknet (например, Tor), т. е. компьютерные среды остаются основной платформой для доступа к материалам о жестоком обращении с детьми и основными средствами некоммерческого распространения; 2) прямая трансляция сексуального насилия над детьми. В подразделении Европола — Internet Organised Crime Threat Assessment (IOCTA) — дана оценка угроз организованной преступности в интернете, рассматривается дополнительная криминальная область — криминальные онлайн-рынки, как на поверхности сети, так и на Darknet. Это относится и к конвергенции терроризма и кибертерроризма.

Другим типичным направлением деятельности IOCTA являются междисциплинарные факторы, способствующие преступности, факторы, которые охватывают более чем одну область преступности, но не обязательно сами по себе являются преступными. Эти средства включают в себя:

1) фишинг (smishing);
2) компромисс деловой почты;
3) пуленепробиваемый хостинг;
4) инструменты анонимизации;
5) преступное злоупотребление криптовалютой;
6) деньги (более 90 % транзакций денежных мулов связаны с киберпреступностью).

Нелегально полученные деньги часто поступают от фишинга, атак с использованием вредоносных программ, мошенничества на онлайн-аукционах, мошенничества с электронной почтой (bec) и мошенничества с бронированием, в том числе праздников, путешествий.

К одним из существенных нарушений, позволяющих совершать киберпреступления, относятся:

1) неконтролируемый допуск сотрудников к компьютерной информации;
2) использование сотрудниками личных USB-флеш-накопителей;
3) бесконтрольность за компьютерами, содержащими информацию о персональных данных;
4) использование в организациях компьютеров, не имеющих контрольной защиты, должных антивирусных программ;
5) несовершенство парольной системы защиты от несанкционированного доступа к рабочей станции и ее программному обеспечению, не обеспечивающей достоверную идентификацию пользователя;
6) использование при работе с базами данных сохраненных паролей;
7) отсутствие должных проверок соблюдения режима секретности;
8) отсутствие договоров с сотрудниками (расписок) о неразглашении данных, ставших известными при работе с компьютерной информацией, персональными данными, коммерческой или служебной тайной, либо иной конфиденциальной информацией;
9) все сотрудники, имеющие доступ к персональным данным, информации, содержащей коммерческую, служебную или иную, охраняемую законом тайну, должны проходить инструктаж с разъяснением ответственности за несоблюдение порядка работы с такими сведениями.

В качестве криминалистических мер противодействия киберпреступлениям выступают:

1) использование в расследовании последних научных достижений;
2) совершенствование теории доказательств, позволяющих признать доказательством не только вещественные доказательства и документированную информацию, но и виртуальную, электронную информацию;
3) создание единых баз, позволяющих идентифицировать лиц, совершающих киберпреступления.

В соответствии с циклом противодействия киберпреступности ЕС3 предложил несколько приоритетных направлений на период 2018–2021 гг.:

1) пресечение преступной деятельности, связанной с информационными системами, особенно теми, которые следуют бизнес-модели Crime-as-a-Service и работают в качестве стимуляторов для онлайн-преступности;
2) противодействие сексуальному насилию над детьми и сексуальной эксплуатации детей, включая производство и распространение материалов о жестоком обращении с детьми;
3) противодействие преступникам, практикующим мошенничество и подделку безналичных платежных средств, в том числе противодействие крупномасштабному мошенничеству с платежными картами, устранению угроз безналичным платежным системам.

Единообразная практика расследования и использование научных достижений в ходе пресечения, выявления и расследования преступлений позволят своевременно установить лицо, совершившее преступление, и привлечь его к уголовной ответственности. Неизбежность наказания обеспечит не только сокращение преступлений, но и поможет защитить высшую ценность государства — права и законные интересы человека.

Таким образом, способы противодействия киберпреступлениям состоят из профилактики, своевременного выявления и расследования данных преступлений, а также своевременного и неотвратимого наказания виновных. Цифровая экономика (экономическая деятельность, в которой ключевым фактором производства являются данные в цифровой форме), несмотря на ее широкое распространение в различных сферах, в России не имеет должного правового регулирования. Существующие за-

коны, программы развития, стратегии помогают лишь определить некоторые направления первоначального пути. К существенным проблемам относятся защита персональных данных, имущества, надлежащее регулирование правил торговли, налоговое регулирование доходов, полученных в результате деятельности в интернет-среде, определение места криптовалюты в национальной валюте.

Сложность законодательного закрепления норм в этой сфере заключается в необходимости обеспечения единообразного понимания основных определений цифровой экономики. Обеспечение безопасности в информационном пространстве требует особого внимания со стороны всех государств, поскольку киберпреступность — глобальная угроза национальным интересам каждой страны. Своевременное изучение методов, причин и условий киберпреступности, разработка методов развития и укрепления материально-технической базы кибербезопасности, качественная подготовка сотрудников правоохранительных органов, готовых и способных обеспечить такую безопасность, могут быть достигнуты следующим образом:

1) совершенствовать информационные ресурсы (информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления), позволяющих своевременно выявлять, предупреждать и устранять последствия компьютерных атак;
2) обеспечить повышение квалификации сотрудников и должностных лиц, в обязанности которых входит выявление, предупреждение, раскрытие, расследование и ликвидация последствий кибератак;
3) разработать на международном уровне единые способы реагирования на выявленные факты кибератак; установить формы взаимодействия для обеспечения своевременного предупреждения.

Итак, анализ действующего законодательства РФ в области цифровой экономики и защиты персональных данных показывает необходимость фундаментальных разработок на стыке многих фундаментальных наук: экономики (выделение обязательных условий для должного развития всех систем в условиях цифровой трансформации), гражданского права (изменение подхода к предмету гражданских прав), информационных технологий (формирование единых правил взаимодействия в рамках технологического прогресса), уголовного права (изучение влияния на институты Общей части причинения вреда с использованием искусственного интеллекта, особенностей предмета хищения при признании виртуальных денег в перечне имущества), уголовного процесса (существенное изменение института доказательств и способов доказывания), экономической социологии (изучение готовности общества к трансформации экономики), криминологии (виктимологические особенности, личность преступника и профилактика преступлений в сфере цифровой экономики), криминалистики (технические разработки по выявлению, пресечению и расследованию преступлений рассматриваемой категории) и др.

Сложности правового регулирования предопределены отсутствием единого подхода к отдельным институтам гражданского права, новых управленческих моделей, а также методов и способов прогнозирования новых цифровых платформ. Скорость технического прогресса и возможности интернет-ресурсов не позволяют своевременно выработать алгоритм защиты и контроля за качеством сделок, соответствием условий к сторонам договора. Все это приводит к новым способам совершения преступлений и отсутствию возможности привлечения виновных к уголовной ответственности. На законодательном уровне должны быть разработаны единые правила противодействия киберпреступлениям, требования к гражданско-правовым сделкам, а также стимулирование мотивации образования населения и повышения уровня правовой, технической грамотности.

Литература

1. О персональных данных [Электронный ресурс]: федер. закон от 27 июля 2006 г. № 152 (в ред. 24 апреля 2020 г.) // Справ.-правовая система «Гарант». URL: https://base.garant.ru/12148555/ (дата обращения: 20.08.2020).
2. О банках и банковской деятельности [Электронный ресурс]: федер. закон от 2 декабря 1990 г. № 351-1 (в ред. от 27 декабря 2019 г.) // Справ.-правовая система «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_5842 (дата обращения: 12.08.2020).
3. О Центральном банке Российской Федерации (Банке России) [Электронный ресурс]: федер. закон от 10 июля 2002 г. № 86-ФЗ (с изм. и доп. от 20 июля 2020 г.) // Справ.-правовая система «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_37570/- (дата обращения: 12.08.2020).
4. О национальной платежной системе [Электронный ресурс]: федер. закон от 27 июня 2011 г. № 161-ФЗ (с изм. и доп. от 20 июля 2020 г.) // Справ.-правовая система «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_115625/- (дата обращения: 21.08.2020).
5. О безопасности критической информационной инфраструктуры Российской Федерации [Электронный ресурс]: федер. закон от 26 июля 2017 г. № 187-ФЗ // Справ.-правовая система «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения: 20.07.2020).
6. Кодекс Российской Федерации об административных нарушениях [Электронный ресурс]: федер. закон от 30 декабря 2001 г. № 195-ФЗ (в ред. от 31 июля 2020 г.) // Справ.-правовая система «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_34661/ (дата обращения: 10.09.2020).
7. Уголовный кодекс Российской Федерации [Электронный ресурс]: федер. закон от 13 июня 1996 г. (в ред. от 31 июля 2020 г.) // Справ.-правовая система «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 20.08.2020).
8. О персональных данных [Электронный ресурс]: модельный закон: принят в г. Санкт-Петербурге 29 ноября 2018 г. постановлением 48-9 на 48-ом пленарном заседании Межпарламентской ассамблеи государств-участников СНГ // Справ.-правовая система «КонсультантПлюс». URL: chttp://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=INT&n=54461#03396751247025789 (дата обращения: 20.08.2020).
9. Соглашение о сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере компьютерной информации от 1 июня 2001 г. [Электронный ресурс] // Справ.-правовая система «Гарант». URL: https://base.garant.ru/12123778/ (дата обращения: 20.08.2020).
10. Дополнительный протокол к Конвенции о преступлениях в сфере компьютерной информации относительно введения уголовной ответственности за правонарушения, связанные с проявлением расизма и ксенофобии, совершенные посредством компьютерных систем ETS № 189 (Страсбург, 28 января 2003 г.) [Электронный ресурс] // Справ.-правовая система «Гарант». URL: https://base.garant.ru/4084840/ (дата обращения: 21.07.2020).
11. В отношении обработки персональных данных и защиты конфиденциальности в секторе электронных средств связи [Электронный ресурс]: директива Европейского парламента и Совета Европейского союза 2002/58/ЕС (Директива о конфиденциальности и электронных средствах связи): принята в Брюсселе 12 июля 2002 г. (с изм. и доп. от 25 ноября 2009 г.) // Справ.-правовая система «Гарант». URL: https://base.garant.ru/2570354/ (дата обращения: 24.07.2020).
12. Об атаках на информационные системы и о замене Рамочного решения 2005/222/ПВД Совета Европейского союза [Электронный ресурс]: директива Европейского парламента и Совета Европейского союза 2013/40/ЕС от 12 августа 2013 г. // Справ.-правовая система «Гарант». URL: https://base.garant.ru/70557982/ (дата обращения: 25.07.2020).
13. О противодействии мошенничеству и подделке безналичных платежных средств [Электронный ресурс]: рамочное решение Совета Европейского союза 2001/413/JHA от 28 мая 2001 г. // O J L 149. 2001. 2 июня. С. 1–4.

14. Основные направления развития информационной безопасности кредитно-финансовой сферы на период 2019–2021 гг. [Электронный ресурс] // Центральный банк РФ. 2019. 26 с. URL: https://cbr.ru/Content/Document/File/83253/onrib_2021.pdf (дата обращения: 24.07.2020).
15. *Гончар В. В.*, *Захаров Д. Н*. Вопросы совершенствования деятельности правоохранительных органов по предупреждению, раскрытию и расследованию киберпреступлений в финансовой сфере // Вестник Московского университета МВД России. 2019. № 3. С. 177–180. DOI 10.24411/2073-0454-2019-10160
16. *Хрусталев Е. Ю.*, *Костюрин Г. А.* Киберугрозы: причины и рекомендации по предотвращению // Национальные интересы и безопасность. 2019. Т. 15. № 6 (375). С. 1185–1194. DOI: 10.24891/ni.15.6.1185
17. *Пракаш С. У.*, *Новианди Нур П. Е.* Анализ кибершпионажа в международном праве и индонезийском праве // Обзоры гуманитарных и социальных наук. 2019. Т. 7. № 3. С. 38–44.
18. *Фурнелл С.*, *Доулинг С.* Киберпреступность: портрет ландшафта // Журнал криминологических исследований, политики и практики. 2019. Т. 5. № 1. С. 13–26.
19. *Сухаренко А.* Противодействие киберугрозам в России: состояние, динамика и тенденции // Диалог: политика, право, экономика. 2018. № 2 (9). С. 26–35.
20. Internet Organised Crime Threat Assessment (IOCTA) // Europol. URL: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment/ (дата обращения: 21.08.2020).