Научная статья
Original article
УДК 004.056

ОСНОВНЫЕ НАПРАВЛЕНИЯ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ

THE MAIN DIRECTIONS OF COUNTERACTION TO CYBERCRIME

Идрисов Идрис Керимович преподаватель кафедры профессиональной подготовки Уфимского юридического института МВД России, г. Уфа

Вердиев Мурад Агаджанович старший преподавал кафедры криминалистики Казанского юридического института МВД России, г. Казань

Idrisov Idris Kerimovich, e-mail: idrisov05@gmail.com

Verdiev Murad Agadzhanovich e-mail: mister.verdiew2013@yandex.ru

Аннотация

В статье раскрываются основные направления предупреждения киберпреступлений и предлагаются пути совершенствования этой деятельности. С учетом анализа официальных статистических данных о преступлениях, совершенных с использованием компьютерных и телекоммуникационных технологий, делается вывод, что абсолютное их большинство находится в латентном состоянии. В статье раскрываются основные направления предупреждения киберпреступлений и предлагаются пути совершенствования этой деятельности.

Annotation

The article reveals the main directions of cybercrime prevention and suggests ways to improve this activity. Taking into account the analysis of official statistical

data on crimes committed using computer and telecommunication technologies, it is concluded that the absolute majority of them are in a latent state. The article reveals the main directions of cybercrime prevention and suggests ways to improve this activity.

Ключевые слова: киберпространство, киберпреступность, цифровизация, меры предупреждения.

Keywords: cyberspace, cybercrime, digitalization, prevention measures.

В настоящее время, когда повсеместно в обычную жизнь людей внедряются цифровые технологии. В связи с чем такое явление, как киберпреступность, стало определенным феноменом. Сейчас мы можем увидеть, что практически каждый гражданин РФ в своей повседневной жизни использует достижения науки и техники, при этом широкое распространение получает виртуальная реальность, которая способна показать мир в будущем. Люди в последние десятилетия стали активно внедрять процессы цифровизации в различные сферы нашей жизни. Мы можем наблюдать, что происходит активное развитие мобильной связи, а также предоставление электронных услуг, совершенствование и усложнение вычислительной техники, что, в свою очередь, создает определенные риски и угрозы, в том числе и криминогенного характера. Как известно, лица, которые имеют умысел на совершение противоправных деяний, быстро проходят процесс адаптации к новым условиям. Так и с развитием цифровых технологий, а также внедрение инновационных достижений в нашу жизнь, широкое распространение получила «киберпреступность». Отсутствие своевременной реакции со стороны государства на происходящие в обществе изменение порождает пробелы в законодательстве, которые выражаются в том, что за совершение преступного деяния лицо не будет привлечено к уголовной ответственности только по тому, что отсутствует норма, предусматривающая ответственность за совершение такого рода деяния. В настоящее время, когда короновирусная инфекция заставляет большое количество людей изолироваться от общества, большое

распространение получили преступления, связанные с кражей персональных данных в сети интернет. Ежедневно в правоохранительные органы поступают обращения от граждан с просьбой восстановить их нарушенные права и свободы. Ведь персональные данные представляют большое значение для граждан. Что же можно отнести к персональным данным? Обратившись к федеральному закону «О персональных данных» можно сказать о том, что к персональным данным законодатель относит любую информацию, прямо или косвенно относящуюся определенному или определяемому лицу[1]. Из этого можно сделать вывод о том, что перечень информации, которая является персональной, является открытым, что говорит о том, что преступники могут посягать самыми разными способами для реализации своего умысла.

В связи с этим в настоящее время «киберпреступность» представляет серьезную угрозу. При этом государственно-частное партнерство, которое должно выражаться как в совместной деятельности правительства, так и в тесном взаимодействии различных международных правоохранительных органов. Это выражается в том, что большое количество кибератак совершается с территории иных государств, но и сами кибератаки по своей природе направлены не только на корпорации, но и на обычных граждан. В связи с этим руководители крупных корпораций призывают активно бороться с возникшей угрозой. «Интернет-офшоры» также представляют определенную угрозы, поэтому требуют большого внимания[2]. Ведь лица, совершившие преступные деяния, должны понимать, что, произведя определенные манипуляции, выраженные в смене домена, то таким образом не смогут уйти от ответственности. Это требует особого внимания и скорейшей выработке международных норм, которые непосредственно устанавливали и закрепляли основные положения противодействия «киберпреступности».

---

[1] Федеральный закон от 27 июля 2006 г. N 152-ФЗ "О персональных данных"//"Российская газета" от 29 июля 2006 г. N 165.

[2] Агапов П.В. Противодействие киберпреступности в аспекте обеспечения национальной безопасности / Агапов П.В., Борисов С.В., Вагурин Д.В. и др.: монография. - Москва, 2014.

На данном этапе развития общества созданы и действуют международные организация, имеющие цель, которая выражается в обеспечение кибербезопасности и активному противодействию преступности, существующей на просторах сети «Интернет». В частности, стоит выделить такую международную организацию, как международное многостороннее партнерство против киберугроз (IMPACT). Данная организация является исполнительным органом, который был учрежден ООН по вопросам, которые непосредственно касаются информационно-телекоммуникационных технологий. При этом данная организация является первым в мире объединением против проявлений киберпреступности, объединяя при этом правительства различных государств, а также ведущих специалистов и экспертов данной отрасли, что создает предпосылки для повышения уровня эффективности борьбы с проявлениями «киберпреступности».

Стоит также сказать об международном альянсе кибербезопасности (ICSPA), который объединяет правительства, международный бизнес, а также правоохранительные органы. Деятельность данных международных организаций направлена на решение следующих задач:

1) выработка единых международных стандартов кибердеяний, подлежащих криминализации;

2) формирование единой терминологии и понятийного аппарата;

3) оказание консультационной помощи при принятии соответствующих уголовно-правовых норм на национальном уровне [3].

Анализ выявленных проблем позволяет сформулировать следующие предложения по совершенствованию деятельности органов внутренних дел по направлению противодействия киберпреступности:

1. Включение общественных отношений, которые возникают в сети «Интернет» в сферу правового регулирования;

[3] Мороз Н. О. Деятельность Интерпола по координации сотрудничества в борьбе с преступностью в сфере высоких технологий // Вестник Полоцкого государственного университета. Серия D: Экономические и юридические науки. — 2011. — № 14. — С. 147.

2. Необходимо производить постоянный контроль и мониторинг сети «Интернет» с целью выявления и пресечения деятельности, которая подвергает опасности граждан. В частности, к ней можно отнести сайты, которые размещают порнографические и экстремистские материалы и т.д.

3. Следует вести учет номеров, которые мошенники используют для реализации своего преступного умысла, а также необходимо усовершенствовать процесс взаимодействия органов внутренних дел с иными правоохранительными органами, а также органами государственной власти.

4. Ужесточение ответственности за нарушения, возникающие в сфере предоставления услуг IP-телефонии, а также в совершенствовании законодательства, которое может выражаться в отказе регистрации пользователей с иностранными IP-адресами и т.д.

5. Постоянно подготавливать методические рекомендации, а также принимать меры по своевременному их обновлению, которые направлены на выявление, раскрытие и расследование преступлений, которые ежедневно совершаются в сети «Интернет».

6. Проводить качественную работу с населением, повышая при этом их уровень правосознания. Это можно достичь, к примеру, во взаимодействии со средствами массовой информации, а именно выражаться может в то, что средства массовой информации в издаваемых газетах могут включать статьи, которые информировали бы граждан о наиболее распространенных способах совершения преступлений в сети «Интернет».

7. Необходимо привлекать на службу в соответствующие правоохранительные органы и их подразделения сотрудников, обладающих соответствующими знаниями в данной сфере. При этом стоит повсеместно производить мероприятия, направленные на повышения квалификации действующих сотрудников.

Важно совершенствовать механизмы международного сотрудничества в рамках повышения эффективности реализации такого направления, как противодействие «киберпреступности». В большинстве случаев возникают

ситуации, когда невозможно установить личность лица (группы лиц), непосредственно имеющих отношение к совершенному преступлению. Мы можем отметить, что между злоумышленником и потерпевшей стороной нет непосредственного физического контакта, что говорит о том, что каких-либо фактических данных о личности преступника у органов предварительного расследования нет, что образует сложности в установлении преступника. Для установления личности преступника задействуются большие силы и средства, так как требуется детальное изучение тех следов, которые злоумышленник оставил после себя в сети «Интернет». Нередко специалисты не имеют достаточных знаний для того, чтобы работать с той информацией о совершенном преступлении, которая есть в распоряжении следователя. Бывают ситуации, когда процесс установления личности злоумышленника обрывается из-за того, что преступником были использованы качественные инструменты, которые позволили анонимно совершать какие-либо действия в сети «Интернет». нередко информативность ответа на запрос не позволяет получить в распоряжение необходимую информацию, которая поспособствует эффективному расследованию по уголовному делу. Возникает вопрос, касающийся того, что почему компетентные на дачу ответа на запрос орган относятся к исполнению запрос так халатно. В свою очередь, можно долго рассуждать на данную тему, но в качестве ответа можно предположить то, что между контактирующими странами может быть разные разногласия на политической арене либо же какие-либо конфликты, что влечет за собой то, что накладывается некий отпечаток на сотрудничество компетентных органов данных стран в рамках уголовного производства.

Как мы знаем, запрос является универсальным средством оказания эффективной помощи по уголовному делу, то есть исполнение запроса предполагает под собой то, что субъект, в чьем производстве находится уголовное дело, может не обладать той информацией, которая крайне необходима по уголовному делу, поэтому, направляя запрос в компетентных иностранный орган, надеется восполнить пробелы, имеющиеся в информации. В

частности, статья 457 УПК РФ говорит о том, что исполнение запрос осуществляется в соответствии с УПК РФ. Но также может быть применено то законодательство, которое основывается на положениях международных договорах и соглашениях. Рассмотренные выше проблемы требует особого внимания, так как с развитием общества усложняются совершаемые преступления[4].

8. Большое внимание следует уделить защите системы передачи информации, а также баз данных от несанкционированного доступа[5].

Несомненно, уголовно-процессуальное законодательство динамично развивается, но все же у практических работников нередко возникают сложности, связанные с производством расследования по данной категории дел[6].

Постоянное развитие информационных технологий и пополнение информации, находящейся в сети Интернет, даёт новые направления оперативного поиска и решить задачи, возложенные на органы, осуществляющих оперативную розыскную деятельность в направлениях, связанных с противодействием киберпреступности. Решение данных задач выполняется посредством проведения ОРМ. Однако способы осуществления ОРМ в сети Интернет не совсем традиционно, так как увеличивается спектр возможностей и способов добычи информации. Так, одним из наиболее эффективных ОРМ в сети Интернет является - опрос. При проведении данного мероприятия оперативный сотрудник может скрывать свою принадлежность к правоохранительным органам, цель проведения опроса, то есть действовать посредством создания профиля в социальной сети. Опрос может проводиться в

---

[4] Организация и планирование деятельности следственных бригад: Методическое пособие / Авт. кол.: В.И. Бенджашев, Л.Н. Викторова, М.Я. Розенталь и др.; под рук. А.А. Эйсмана; Всесоюзный научно-исследовательский институт проблем укрепления законности и правопорядка. М., 1990. С. 4.

[5] Чепрасова Ю.В., Шмарион П.В. Основные направления противодействия киберпреступности // Вестник ВИ МВД России. 2020. №3. URL: https://cyberleninka.ru/article/n/osnovnye-napravleniya-protivodeystviya-kiberprestupnosti (дата обращения: 07.02.2022).

[6] Чепрасова Ю.В., Шмарион П.В. Основные направления противодействия киберпреступности // Вестник ВИ МВД России. 2020. №3. URL: https://cyberleninka.ru/article/n/osnovnye-napravleniya-protivodeystviya-kiberprestupnosti (дата обращения: 07.02.2022).

социальных сетях и мессенджерах, например, в таких как: «ВКонтакте», «Instagram», «Facebook», «WhatsApp», «Viber», «Telegram». Он может осуществляться как посредством общения оперативного сотрудника и другого зарегистрированного пользователя в личных интернет-беседах, так называемых чатах или личных беседах, так и с группой пользователей в групповых чатах или беседах. Также часть мессенджеров предоставляют возможность использования видео-общения. Это позволяет проводить опрос, когда нет возможности встретиться с человеком лично, что позволяет использовать профайлинг в процессе опроса. Также опрос может проводиться на форумах онлайн-сайтов. Большая часть сайтов, предоставляющих какие-либо услуги или товары, содержит форумы для оценки услуг или товаров, написания отзывов, а также общения пользователей. В данном случае можно добыть информацию, представляющую оперативный интерес у пользователей сайта. Изучая персональные страницы пользователей социальных сетей, можно провести ОРМ «Отождествление личности». Традиционно такое мероприятие заключается в сопоставлении сведений, полученных о личности разрабатываемого, со сведениями сетевой активности данного субъекта. Определенную трудность в проведении данного ОРМ создает наличие анонимности сетевого общения, которую можно преодолеть с помощью выведывания дополнительных сведений о лице, представляющих оперативный интерес. Само отождествление в сетевом пространстве заключается в изучении фотографий, размещаемых пользователями на сетевых страницах в социальных сетях, пользовательских имен («ников»), адресам электронной почты, IP-адресам и т.д. Также могут использоваться и учитываться более сложные идентифицирующие особенности пользователей, например, стилистические особенности электронного общения, знания о каких-то определенных уникальных событиях, фактах, лицах. Также отождествление личности может осуществляться путем электронной рассылки фотографий или других идентифицирующих сведений разрабатываемого лицу, которое ранее было очевидцем преступления.

Таким образом, мы рассмотрели основные направления противодействия киберпреступности. Современное общество каждый день подвергается самым разным изменениям. В настоящее время, когда короновирусная инфекция заставляет большое количество людей изолироваться от общества, большое распространение получили преступления, связанные с кражей персональных данных в сети интернет. Ежедневно в правоохранительные органы поступают обращения от граждан с просьбой восстановить их нарушенные права и свободы. Ведь персональные данные представляют большое значение для граждан. Из этого можно сделать вывод о том, что перечень информации, которая является персональной, является открытым, что говорит о том, что преступники могут посягать самыми разными способами для реализации своего умысла, поэтому все это требует своевременной реакции со стороны правоохранительных органов.

Литература

1. Мороз Н. О. Деятельность Интерпола по координации сотрудничества в борьбе с преступностью в сфере высоких технологий // Вестник Полоцкого государственного университета. Серия D: Экономические и юридические науки. — 2011. — № 14. — С. 147.
2. Чепрасова Ю.В., Шмарион П.В. Основные направления противодействия киберпреступности // Вестник ВИ МВД России. 2020. №3. URL: https://cyberleninka.ru/article/n/osnovnye-napravleniya-protivodeystviya-kiberprestupnosti (дата обращения: 07.02.2022).
3. Долженко Н.И., Ярощук И.А. Киберпреступность как одна из ключевых проблем современности // Правовая парадигма. 2020. Т. 19. № 1. С. 151-157.
4. Агапов П.В. Противодействие киберпреступности в аспекте обеспечения национальной безопасности / Агапов П.В., Борисов С.В., Вагурин Д.В. и др.: монография. - Москва, 2014.

Literature

1. Moroz N. O. The activities of Interpol on the coordination of cooperation in the fight against crime in the field of high technologies // Bulletin of the Polotsk State

University. Series D: Economic and Legal Sciences. - 2011. - No. 14. - p. 147.

2. Cheprasova Yu.V., Shmarion P.V. The main directions of countering cybercrime // Bulletin of the Ministry of Internal Affairs of Russia. 2020. No. 3. URL: https://cyberleninka.ru/article/n/osnovnye-napravleniya-protivodeystviya-kiberprestupnosti (accessed: 07.02.2022).
3. Dolzhenko N.I., Yaroshchuk I.A. Cybercrime as one of the key problems of our time // The legal paradigm. 2020. Vol. 19. No. 1. pp. 151-157.
4. Agapov P.V. Countering cybercrime in the aspect of ensuring national security / Agapov P.V., Borisov S.V., Vagurin D.V. et al.: monograph. - Moscow, 2014.

© Идрисов И.К., Вердиев М.А., 2022 Научно-образовательный журнал для студентов и преподавателей «StudNet» №3/2022.

Для цитирования: Идрисов И.К., Вердиев М.А., КИБЕРПРЕСТУПНОСТЬ Как угроза современному информационному обществу// Научно-образовательный журнал для студентов и преподавателей «StudNet» №3/2022.