Уголовное право, криминология, уголовно-исполнительное право

Научная статья
УДК 346.7:004

ПРОФИЛАКТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Виктор Львович Акапьев[1], Андрей Анатольевич Дрога[2], Сергей Евгеньевич Савотченко[3]
[1, 2, 3] Белгородский юридический институт МВД России имени И.Д. Путилина, Белгород, Россия
[1] akapevvl@yandex.ru
[2] ABulet@rambler.ru
[3] savotchenko@hotbox.ru

Аннотация. *В статье проведен анализ основных мер противодействия преступлениям в сфере информационных технологий. Определены обстоятельства, способствующие совершению преступлений в информационной среде. Выделены основные группы профилактических мер предупреждения преступлений в информационной сфере. Подробно рассмотрены правовые меры, предусмотренные нормами действующего законодательства. Предложены пути снижения уровня таких видов преступлений с помощью различных механизмов профилактики.*

Ключевые слова: *киберпреступления, преступления в сфере информационных технологий, профилактика преступлений, профилактические меры*

Для цитирования: *Акапьев В.Л., Дрога А.А., Савотченко С.Е. Профилактика преступлений в сфере информационных технологий // Алтайский юридический вестник. 2022. № 4 (40). С. 84-89.*

Original article

PREVENTION OF CRIMES IN THE FIELD OF INFORMATION TECHNOLOGY

Viktor L. Akapev[1], Andrey A. Droga[2], Sergey E. Savotchenko[3]
[1, 2, 3] Putilin Belgorod Law Institute of Ministry of the Interior of Russia, Belgorod, Russia
[1] akapevvl@yandex.ru
[2] ABulet@rambler.ru
[3] savotchenkose@mail.ru

Abstract. *The article analyzes the main measures to counteract crimes in the field of information technology. The circumstances contributing to the commission of crimes in the information environment are determined. The work identifies main groups of measures to prevent crimes in the information sphere. The legal measures provided by the current legislation norms are considered in detail. Ways to reduce the level of such crimes types with the help of various prevention mechanisms are proposed.*

Keywords: *cybercrime, information technology crimes, crime prevention, preventive measures*

For citation: *Akapev V.L., Droga A.A., Savotchenko S.E. Prevention of crimes in the field of information technology. Altajskij juridicheskij vestnik = Altai Law Journal. 2022;4:84-89 (In Russ.).*

В состав структуры современной криминогенной обстановки киберпреступность вошла относительно недавно, но уже успела заявить о себе в полный голос. Сложившаяся ситуация вынуждает активизировать противодействие противоправным действиям в области информационных технологий (далее – IT), разработку новых форм и методов борьбы с ними [1]. Очевидно, что для снижения уровня преступлений в IT-сфере необходимы профилактические меры.

Статистика МВД России отмечает активное проникновение криминала в сферу сетевых информационных технологий, т.к. интернет стал выгодной платформой для киберпреступников. Более того, пандемия и самоизоляция в 2020 г. выступили особым катализатором этих процессов, и рост числа пользователей, пришедших в интернет, стимулировал высокую динамику преступности.

Перевод работников на удаленный режим работы, переход мелкого и среднего бизнеса в виртуальное пространство выступают дополнительными стимулами увеличения пользователей интернета. Как следствие, растут и финансовые потоки в этой среде [2]. На общем фоне стагнации экономики мошенники быстро пришли к выводу, что это легкое место для наживы, открывающее окна возможностей для быстрого обогащения [3].

К настоящему моменту масштабы данной проблемы стали такими, что привлекли внимание не только правоохранительных органов, но и научного сообщества, что и обусловило рост количества публикаций, посвященных противодействию преступлениям в IT-сфере [4, 5].

Следует отметить, что в современной научной литературе нет устоявшегося определения понятия «киберпреступление» [6]. Авторы в своих работах приводят различные определения данного явления [7]. Чаще всего приходится сталкиваться с трактовкой, согласно которой это противоправные действия, совершаемые в сфере информационных технологий и направленные на получение конфиденциальной информации либо персональных данных с целью извлечения прибыли.

Определенным базисом возникновения и развития киберпреступности является низкий уровень информационной культуры населения России. У большинства пользователей отсутствует или слабо сформирована информационно-технологическая компетентность в области использования IT для решения личных или служебных задач. Как следствие, они не знают, как правильно передавать, обрабатывать и защищать информацию, тем самым становятся жертвами мошенников.

Согласно статистике, преступления, совершенные в интернете, с каждым годом растут и демонстрируют серьезную динамику. Так, например, в 2015 г. было зафиксировано хищение 348 млн рублей с банковских счетов, а в 2020 г. объем краж со счетов достиг 9 млрд рублей. Следовательно, по сравнению с 2015 г. число краж со счетов увеличилось примерно в 25 раз [8]!

Если безотлагательно не предпринять конкретные меры либо не провести определенную профилактику, то непрофессиональным пользователям станет просто невозможно работать в сети, т.к. в качестве жертвы мошенников может оказаться каждый, кто войдет в интернет.

Обычно киберпреступники используют интернет с целью получения прибыли, применяя такие виды атак, как фишинг, кибервымогательство, финансовое мошенничество, кражи персональных данных, шпионаж, кибербуллинг, незаконный оборот оружия и наркотиков, кибертерроризм, спам и др. [9]. С каждым годом этот перечень расширяется с появлением новых форм атак в информационной среде. К примеру, в 2021 г. самыми распространенными преступными деяниями в интернете стали:

1. Кибершантаж – вымогательство, реализуемое с помощью компьютерных технологий. Это уже не новое преступление, отличающееся большим количеством вариаций. Сюда может быть отнесен метод действий киберпреступников, заключающийся в распространении вирусных программ, которые после проникновения в компьютер жертвы шифруют все файлы пользователя, что позволяет в дальнейшем шантажировать потерпевшего, требуя заплатить выкуп за восстановление файлов.

2. APT-атаки – это постоянные угрозы в распространении вредоносных программ, направленных на поиск ценной информации. Также данные вирусы легко приспосабливаются к антивирусным программам и могут спокойно обойти любой блокиратор. Сам поиск информации осуществляют с помощью взлома системы и посредством использования программных уязвимостей.

Появление новых видов киберпреступлений и рост их количества подталкивают к необходимости анализа уязвимостей информационных систем, способствующих их совершению. В качестве основных уязвимостей, выступающих в качестве первопричин совершения киберпреступлений, можно выделить следующие [10]:

1) слабость парольной системы безопасности, первопричиной которой является малограмотная авторизация с использованием неграмотно сформированного логина и (или) пароля, который можно легко подобрать;

2) неудовлетворительный по качеству уровень защиты системного и прикладного программного обеспечения, который не позволяет обеспечить требуемый уровень компьютерной безопасности;

3) отсутствие должностного лица, которое относилось бы к подразделениям режима секретности и следило бы за утечкой конфиденциальной информации и её безопасностью от несанкционированного к ней доступа;

4) неконтролируемый доступ сотрудников к компьютерам, развернутым на территории подразделений органов внутренних дел, что дает возможность для реализации незаконной передачи конфиденциальных данных мошенникам за денежное вознаграждение;

5) непонимание руководителями различных уровней всей серьезности проблемы преступности в информационной среде;

6) увеличение количества финансовых операций, производимых электронным способом с использованием разнообразных платежных систем, а также заключения договоров в сети без должного контроля;

7) крайне низкий уровень сформированности информационно-технологической компетентности сотрудников органов внутренних дел в части организации борьбы с преступлениями в сфере информационных технологий;

8) довольно высокий уровень латентности преступлений в сфере информационных технологий. Это приводит к тому, что основная часть противоправных действий остается неучтенной по целому ряду причин. Достаточно сказать, что в России латентность преступности в сфере информационных технологий превышает 92%, что негативно сказывается на уровне защиты российских граждан от кибератак;

9) несовершенство российского уголовного законодательства, которое, в частности, выражается в слабой проработанности в части недостаточности наказаний за несанкционированный доступ к компьютерной информации;

10) огромное количество создаваемых вирусов и практически безнаказанное распространение их в сети;

11) острая нехватка высококвалифицированных программистов в системе МВД России для борьбы с киберпреступниками, т.к. киберпреступники – это не просто мошенники, скрывающиеся за компьютером, а хорошо обученные программисты, которые знают, как скрыть свою личность в сети, что значительно осложняет их установку и идентификацию в отличие от обычного преступника. Данная проблема значительно обострилась на фоне реального снижения уровня денежного довольствия сотрудников ОВД по сравнению с доходами специалистов, работающих в государственных и коммерческих структурах.

Таким образом, существует огромное количество уязвимостей, облегчающих совершение киберпреступлений. Несмотря на всю разноплановость, их объединяет одна общая черта – содействие киберпреступнику в подготовке и совершении информационных преступлений. Чтобы усложнить им жизнь и переломить ситуацию, необходимо иметь четкое представление о наличии превентивных мер профилактики, направленных на пресечение киберпреступлений.

Можно выделить следующие основные группы профилактических мер предупреждения преступлений с использованием телекоммуникационных технологий: правовые, организационно-управленческие, технические [11]. С другой стороны, такие меры можно разделить на внутренние (национальные) и международные.

В Российской Федерации к правовым мерам предупреждения относятся нормы законодательства, сконцентрированные в статьях 272-274 Уголовного кодекса Российской Федерации 1996 г. (ред. от 30.12.2021) [12]. Нет смысла в рамках статьи давать полный пересказ указанных правовых норм, поэтому хотелось бы отметить следующий момент: российское законодательство в его существующем состоянии не отвечает веяниям времени и требованиям современного общества. Пять статей Уголовного кодекса, даже с учетом статьи 159.6 УК РФ, – это капля в бушующем море компьютерной преступности! Кроме того, все указанные нормы, с нашей точки зрения, отличаются ничем не оправданной лояльностью к правонарушителям. Достаточно провести сравнение с федеральным законодательством США, в котором за киберпреступления предусмотрено до 25 лет лишения свободы, в то время как в Российской Федерации максимальный срок достигает 10 лет.

Другой группой мер предупреждения преступлений в информационной среде являются организационно-управленческие меры, к которым можно отнести следующие:

1) устранение возможности хищения, изменения и подделывания защищенной информации, выражающееся в расширении функций, в частности, таких органов власти, как Федеральная служба безопасности, Роскомнадзор, с целью организации перманентного контроля за виртуальным пространством;

2) пресечение незаконных действий по уничтожению, изменению, копированию информации и другого незаконного вмешательства в информационные системы с использованием существующих и перспективных информационных технологий. Например, геолокации преступников с целью их задержания или блокирования аккаунтов;

3) защита государственной тайны и конфиденциальной информации. Поддерживают защиту информации данного типа различные государственные федеральные органы исполнительной власти [13];

4) гарантия прав и свобод граждан в сетевом пространстве в сфере использования информационных

технологий. Государство гарантирует соблюдение прав и свобод человека не только в реальной жизни, но и в интернете [14];

5) проведение широкой агитационной программы и разработка мероприятий, направленных на популяризацию сведений о дающей успешные результаты борьбе с преступлениями в сфере информационных технологий. В первую очередь это делается для того, чтобы преступники знали, что они могут быть пойманы и заключены под стражу. Следовательно, срабатывает принцип неотвратимости наказания даже в условиях экстерриториальности в международном уголовном законодательстве;

6) проведение разъяснительной кампании с подрастающим поколением. Так, на национальном уровне проводятся различные диалоги назначаемых лиц от правоохранительных органов с молодежью. Такие беседы проводятся в школах, университетах, колледжах для объяснения подросткам, что интернет – это не место для развлечения, это зона повышенной социальной опасности, где в любой момент могут украсть ваши персональные данные, снять деньги с вашего счета, а также выложить ваши личные фото или переписку с друзьями в интернет. Поэтому нужно быть осторожным в информационной среде, чтобы не попасться на уловки мошенников. Также необходимо пояснить молодежи, что ждет мошенников за такие деяния, ознакомить подростков со статьями 272, 273 и 274 Уголовного кодекса РФ. Чтобы снизить тенденцию к совершению противоправных деяний молодежи в информационной среде, нужно вводить в планы учебной работы образовательных учреждений дополнительные часы по дисциплине «Информатика». Благодаря этому подростки не только не будут совершать преступления в интернете, но и будут знать, как грамотно вести себя в виртуальной среде [15].

К примеру, подросток сможет обновить свое программное обеспечение для того, чтобы компьютер стал более устойчив к воздействию вредоносных программ, установить на браузер AdBlock, чтобы блокировать спам. Тинейджер получит возможность адекватно оценивать сложившуюся в сетевом пространстве ситуацию и знать, каким образом на нее реагировать, какие действия предпринимать. Так, подросток может направить свое подозрение модераторам, указав сайт, на котором возможен фишинг или который распространяет спам, либо обратиться на сайт официальной организации, где можно оставить свою жалобу.

При этом крайне важно учитывать подростковый менталитет, детский максимализм, особенности формирующейся психики и восприятия действительности.

Профилактические мероприятия правоохранительных органов должны не оставаться в виде планов и отчетов на бумаге, а обязательно реализовываться. Только тогда организационно-управленческие меры позволят значительно снизить количество преступлений в информационной среде.

В качестве следующей группы мер предупреждения информационных преступлений можно выделить технические меры – это меры, реализуемые с использованием возможностей аппаратно-программных средств информационных технологий [16].

Исходя из своего названия, они подразделяются на аппаратные и программные методы. Аппаратные методы служат для того, чтобы защищать телекоммуникационные технологии от нежелательных физических воздействий. Программные методы нужны для того, чтобы при передаче никакая информация не была похищена либо искажена кем-либо. Для этого используются различные методы шифрования данных.

Естественно, приведенную классификацию мер предупреждения нельзя считать полной и исчерпывающей. Данная проблематика закономерно требует дальнейшего исследования.

В отдельную категорию выделяют международные меры предупреждения киберпреступлений – это меры, направленные на решение проблемы на международном уровне путем проведения различных конференций либо собраний представителей государств и правоохранительных органов [17]. В настоящее время в связи с развитием информационных технологий и переходом постиндустриального общества к информационному решать проблему киберпреступности на национальном уровне становится всё тяжелее, поэтому приходится объединяться с другими государствами и решать проблему на международном уровне совместными усилиями [2].

Киберпреступность должна ограничиваться всеми субъектами, но именно от государств будет зависеть полномасштабное решение данной проблемы. Только тогда те, кто наиболее подвержен опасности от посягательств преступников, смогут спокойно находиться в интернете. Поэтому государство обязано создать беспроигрышную информационную защиту [13], для чего и было создано управление «К» в МВД. Ранее, в 2015 г., был организован Центр борьбы с киберугрозами финансового характера для того, чтобы получать всю информацию о киберпреступлениях в финансовой сфере от банков и на основе ее анализа давать рекомендации банкам по противодействию киберпреступности.

Управление «К» МВД было создано 4 декабря 2017 г. по поручению Президента РФ. Управление «К» возглавляет Министр внутренних дел РФ. Эта организация является самым засекреченным подразделением по всей России, предназначенным для пресечения преступлений в сфере компьютерной информации:

1) преступлений, направленных на распространение материалов порнографического характера с участием несовершеннолетних, т.е. преступлений, угрожающих общественной нравственности;

2) преступлений, связанных с незаконным оборотом информационных технологий, предназначенных для незаконного получения конфиденциальной информации;

3) с распространением агитации, призывающей к суициду;

4) с мошенничеством с банковскими счетами;

5) как и ФСБ, занимается выявлением и пресечением незаконного подключения и подслушивания телефонных разговоров;

6) преступлений, указанных в ст. 272, 273 и 274 УК РФ. К примеру, пресечение преступлений, связанных с распространением вирусных программ.

В заключение можно отметить, что в современном мире за преступления в информационной среде предусмотрены уголовные наказания в виде лишения свободы, но, к сожалению, киберпреступников это не останавливает, поэтому всей системе правоохранительных органов в общем и МВД России в частности необходимо включиться в активную разработку действительно действенных мер по борьбе с киберпреступлениями.

Таким образом, для того чтобы предотвратить киберпреступления, следует ужесточить уголовную ответственность за преступления в информационной среде, усилить контакты правоохранительных органов с населением, проводить различные профилактические беседы с гражданами, а также рассматривать проблему на международном уровне для создания организаций, направленных на решение проблемы киберпреступности в современном мире. В частности, необходимо:

1) разработать порядок эффективного взаимодействия правоохранительных органов с международными организациями для обмена информацией о киберпреступности и для совместной борьбы с нею;

2) благоприятствовать проведению ежегодных научных конференций по проблемам выявления, пресечения и расследования киберпреступности;

3) подготовить методические рекомендации по предупреждению, выявлению и пресечению преступлений в информационной среде;

4) создавать ведомственные подразделения либо иные межведомственные организации, направленные на борьбу с киберпреступностью;

5) в рамках повышения квалификации и профессиональной переподготовки сотрудников ОВД разработать программу подготовки специализированных кадров для работы по защите информационных технологий от угроз киберпреступников.

Все эти меры необходимы, т.к. именно государство и всё общество в целом с их помощью смогут справиться с такой серьезной проблемой, как киберпреступность.

Список источников

1. Номоконов В.А. Киберпреступность: прогнозы и проблемы борьбы // Библиотека криминалиста. 2018. № 5 (12). С. 137-150.

2. Трунцевский Ю.В. Киберпреступления в корпоративной среде: риски, оценка и меры предупреждения // Российский следователь. 2014. № 21. С. 19-22.

3. Кумышева М.К. Киберпреступность в России и в мире // Пробелы в российском законодательстве. 2019. № 3. С. 195-214.

4. Бутусова Л.И. Характеристика и сущность киберпреступлений // Алтайский юридический вестник. 2016. № 3. С. 28-31.

5. Чекунов И.Г. Понятие и отличительные особенности киберпреступности // Российский следователь. 2014. № 18. С. 53-56.

6. Кочкина Э.Л. Определение понятия «киберпреступление». Отдельные виды киберпреступлений // Сибирские уголовно-процессуальные и криминалистические чтения. 2017. № 3. С. 162-169.

7. Халиуллин А.И. Подходы к определению киберпреступления // Российский следователь. 2015. № 1. С. 34-39.

8. Гайфутдинов Р.Р. Типы компьютерных мошенников // Вестник экономики, права и социологии. 2017. № 2. С. 54-58.

9. Иванова Л.В. Виды киберпреступлений по российскому уголовному законодательству // Юридические исследования. 2019. № 1. С. 25-33.

10. Евдокимов К.Н. Причины компьютерной преступности в современной России // Российский следователь. 2017. № 2. С. 40-50.

11. Эмиров М.Б. Борьба с преступлениями в глобальных компьютерных сетях // Юридический вестник Белгородского государственного университета. 2018. № 3. С. 49-56.

12. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 30.12.2021) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

13. О государственной тайне: федеральный закон от 21.07.1993 № 5485-1-ФЗ (ред. от 09.03.2021) // Собрание законодательства РФ. 1993. № 58. Ст. 20.

14. О порядке рассмотрения обращений граждан Российской Федерации [Электронный ресурс]: федеральный закон от 02.05.2006 № 59-ФЗ (ред. от 05.09.2020). Доступ из справ.-правовой системы «КонсультантПлюс».

15. Баринов В.Б. Сущность оперативно-розыскной профилактики преступлений // Пробелы в российском законодательстве. 2020. № 2. С. 173-198.

16. Кузнецова М.В. Противодействие компьютерным преступлениям // Правоведение. 2019. № 1. С. 19-25.

17. Даненьян А.А. Международное правовое регулирование киберпространства // Наука и право. 2020. № 2. С. 239-268.

Информация об авторах

В.Л. Акапьев – кандидат педагогических наук;

С.Е. Савотченко – доктор физико-математических наук, доцент.

Information about the authors

V.L. Akapev – Candidate of Science (Pedagogy);

S.E. Savotchenko – Doctor of Science (Physics and Mathematics), Associate Professor.