УДК 343.3/.7

М.В. Богданова, А.С. Полторанина
Российский государственный университет правосудия, г. Москва,
email: bogdanovamv2009@yandex.ru

ПРОФИЛАКТИКА КИБЕРПРЕСТУПЛЕНИЙ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Ключевые слова: киберпреступления, киберпространство, информационные технологии, кибербезопасность, киберугрозы.

Статья посвящена рассмотрению мероприятий по профилактике киберпреступлений с использованием информационных технологий. Дано определение понятия «киберпреступление» и на этой основе выявляются гражданский, корпоративный и государственный уровни преступлений в киберпространстве. Проведен анализ современного состояния киберпреступности в Российской Федерации. Рассмотрены законодательный, информационный, морально-этический, технический и программный аспекты, определяющие эффективность мер обеспечения безопасности в информационном пространстве. Дана характеристика направленности злоумышленников в информационном пространстве. Выявляются актуальные проблемы, связанные с киберугрозами и сформулированы основные меры, направленные на обеспечение защиты, сохранности конфиденциальных данных. Рассмотрены технические меры по обеспечению защиты и сохранности конфиденциальных данных. Раскрыта роль государства в обеспечении снижения уровню киберпреступности и развития информационной безопасности в стране.

M.V. Bogdanova, A.S. Poltoranina
Russian State University of Justice, Moscow, email: bogdanovamv2009@yandex.ru

PREVENTION OF CYBERCRIME USING INFORMATION TECHNOLOGY

Keywords: Cybercrime, cyberspace, information technology, cybersecurity, cyber threats.

The article is devoted to the consideration of measures for the prevention of cybercrime using information technology. The definition of the concept of “cybercrime” is given and on this basis the civil, corporate and state levels of crimes in cyberspace are identified. The analysis of the current state of cybercrime in the Russian Federation is carried out. The legislative, informational, moral and ethical, technical and programmatic aspects determining the effectiveness of security measures in the information space are considered. The characteristic of the orientation of intruders in the information space is given. The current problems related to cyber threats are identified and the main measures aimed at ensuring the protection and safety of confidential data are formulated. Technical measures to ensure the protection and safety of confidential data are considered. The role of the state in ensuring the reduction of cybercrime and the development of information security in the country is revealed.

Преступная деятельность является распространенной проблемой в современной культуре и обществе, при этом большинство стран уже столкнулись с неприемлемым уровнем преступности [1]. С развитием технологий, преступная деятельность смогла переместиться в цифровое пространство, что создало новые угрозы для мирового сообщества, поэтому важно подчеркнуть, что борьба с киберпреступностью является относительно новым явлением в нашей жизни.

Целью исследования является выявление мер профилактики киберпреступлений с использованием информационных технологий.

Материал и методы исследования

Выполненное исследование базируется на научных трудах российских и зарубежных ученых в области мероприятий по борьбе с киберпреступностью, документах международных и российских организаций, а также официальной статистике.

В процессе исследования применялись общенаучные и статистические методы, а также графический и табличный методы анализа.

Результаты исследования и их обсуждение

Киберпреступление – это особый вид преступлений, который соверша-

ется с использованием информационных технологий таких, как: компьютер, смартфон или с помощью любого другого устройства вычислительной техники.

Преступления в киберпространстве по своей направленности можно разделить условно на три уровня:

− Гражданский уровень (почтовые вымогатели, кража платежных данных);

− Корпоративный уровень (кража клиентской базы и копирование уникальных технологий);

− Государственный уровень (кража данных, связанных с государственной тайной).

Киберпреступления классифицируются по следующим признакам:

− По способу использования:

1. компьютер является объектом правонарушения;

2. компьютер используется как запоминающее устройство;

3. компьютер используется как средство, способствующее совершению киберпреступления.

− По наличию насилия:

1. насильственные и иные потенциально опасные (кибертерроризм, угроза физической расправы, киберпреследование, детская порнография);

2. ненасильственные (противоправное нарушение владения в киберпространстве, киберворовство, кибермошенничество).

− По способу воздействия

1. физические злоупотребления;

2. программные злоупотребления;

3. операционные злоупотребления;

4. электронные злоупотребления.

В России, как и во всем мире, ситуация с киберпреступностью только осложняется. По данным МВД России в 2021 г. было зарегистрировано 517 тыс. преступлений с использованием ИТ и это только с учетом возбужденных уголовных дел [2].

Исходя из представленных статистических данных следует отметить, что ежегодно наблюдается увеличение зафиксированных преступлений с использованием информационных технологий. Наименьший прирост количества киберпреступлений был зафиксирован в 2021 г. по сравнению с 2020 г. и составил 1,4%. Можно только предполагать, каков уровень латентности киберпреступлений, поэтому на сегодняшний день одной из важнейших задач государства является обеспечение безопасности в киберпространстве.

На рисунке 1 представлена динамика киберпреступлений за 2017 – 2021 гг.

Исходя из представленных статистических данных следует отметить, что ежегодно наблюдается увеличение зафиксированных преступлений с использованием информационных технологий. Наименьший прирост количества киберпреступлений был зафиксирован в 2021 г. по сравнению с 2020 г. и составил 1,4%. Можно только предполагать, каков уровень латентности киберпреступлений, поэтому на сегодняшний день одной из важнейших задач государства является обеспечение безопасности в киберпространстве. Обеспечение безопасности в информационном пространстве в государстве напрямую зависит от множества аспектов (см. рис. 2):

Выделяют следующие основные аспекты кибербезопасности:

1. Законодательный аспект подразумевает создание нормативно-правовой базы, которая регламентирует права и обязанности физических и юридических лиц в области информационных технологий. На данный момент отечественное законодательство насчитывает более пяти федеральных законов, связанных с информационной безопасностью, в том числе Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [3].

Также законодательную базу составляют Указы Президента, различные Положения и Постановления.

2. Информационный аспект служит инструментом доведения до граждан и бизнеса информации о том, как не стать жертвой киберпреступников. Примером может служить огласка совершённых преступлений в средствах массовой информации.

3. Морально-этический аспект предполагает создание и поддержание такой обстановки, при которой совершение противоправных деяний в области информационных технологий будет неприемлемо.

4. Технический аспект отвечает за обеспечивание государственных структур

и предприятий соответствующим оборудованием, которое позволяет хранить массивы данных.

5. Программный аспект включает в себя программное обеспечение, технологии блокчейна, машинное обучение или классические инструменты информационной безопасности – антивирусные программы.

В первую очередь, человек, компания или государственные органы в вопросе кибербезопасности обеспокоены сохранностью данных [4]. Если на гражданском уровне чаще всего происходит кража личных или платежных данных, то на уровне корпораций и государственных структур происходят более масштабные утечки, которые могут привести к фатальным последствиям.

К распространенным кибератакам на базы данных относятся следующие действия: фишинг и DDoS-атаки.

Фишинг (от англ. phishing, от fishing – «рыбная ловля») – способ интернет-мошенничества, целью которого является получение конфиденциальных данных [5]. Суть этого способа заключается в тревожных звонках о случившемся происшествии или отправке «жертве» поддельных уведомлений от банковских и государственных структур. Подобная атака, как правило, строится на социальной инженерии. Злоумышленник старается указать такую причину, которая откликнулась бы в «жертве», чтобы вторая сторона могла раскрыть конфиденциальную информацию.

На сегодняшний день существуют различные антифишинговые приложения, которые позволяют пользователю интернета идентифицировать вебстраницу или почтовое сообщение как вредоносное. Одно из таких программных решений принадлежит Лаборатории Касперского. Также эта компания ежегодно публикует свои отчеты, в которых раскрывает информацию о предотвращении переходов по фишинговым ссылкам благодаря системе «Антифишинг» (см. табл. 1) [6].

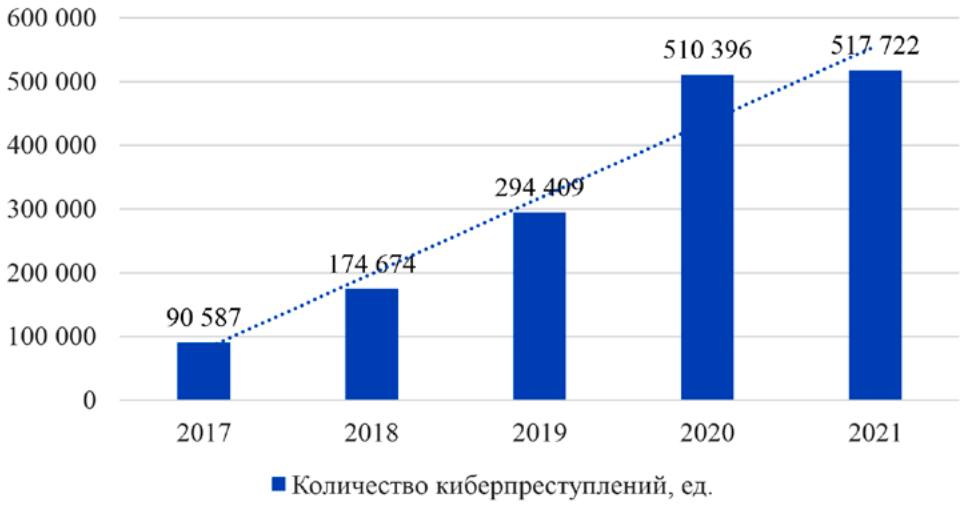

Рис. 1. Динамика зафиксированных киберпреступлений в Российской Федерации, 2017 – 2021 гг. (Источник: МВД России)

Таблица 1

Динамика предотвращения переходов по фишинговым ссылкам на основе системы «Антифишинг» от Лаборатории Касперского, 2017 – 2021 гг.

	Год	2017	2018	2019	2020	2021
Показатель						
Количество зафиксированных фишинговых ссылок, млн. шт.		246	482	467	434	253
Прирост, %		-	+95,9	-3,1	-7,1	-41,7

Источник: составлено авторами на основе отчетов Лаборатории Касперского, 2022

Рис. 2. Аспекты кибербезопасности (Источник: составлено авторами)

Представленные данные из отчета компании (табл. 1) свидетельствуют о том, что пик фишинговых кибератак пришелся на 2018 г. Количество таких атак возросло практически в 2 раза по сравнению с 2017 г. Основной причиной такого всплеска стала пенсионная реформа. Злоумышленники играли на том, что якобы можно вернуть часть пенсионных накоплений [7].

Однозначно нельзя сказать, что присутствует тенденция на снижение количества фишинговых атак. Во-первых, статистика основана только на представленных данных одной компании, во-вторых, по-прежнему остается неизвестным то, какое количество фишинговых атак остается незафиксированным, например, в виде звонков. Однако можно прогнозировать, что по итогам 2022 г. активность мошенников снова возрастет в связи с нестабильной политической ситуацией в мире.

Проблемы, связанные с кибербезопасностью, как было приведено на примере фишинга, не всегда связаны исключительно с совершенствованием информационных технологий, зачастую проблема вызвана особенностями человеческой психики, возможностью использовать ее против самой «жертвы». Даже в таком случае есть перспектива использовать превентивные меры защиты.

Государствам для повышения уровня кибербезопасности стоит обратить внимание на уже существующие программы фильтрации поступающей информации. На сегодняшний день существует множество программных решений в области защиты от фишинга, однако все они являются сторонними приложениями.

Рекомендация по совершенствованию уровня кибербезопасности заключается в том, что подобные программы должны стать неотъемлемой частью девайсов. Однако здесь возникает новая трудность, связанная с тем, что довольно сложно обязать производителей девайсов и производителей программного обеспечения внедрить антифишинговые приложения как предустановленные. Это будет возможно только в том случае, если множество государств в борьбе с киберпреступностью смогут совместно разработать систему поощрения компаний, осуществляющих внедрение антифишинговых приложений как предустановленных. Благодаря такой мере удастся более эффективно противостоять киберпреступности.

Другая угроза, которая представляет опасность для базы данных – это DDoS-атака.

DDoS-атака (от англ. Distributed Denial of Service – «отказ от обслуживания») – способ злоумышленников нарушить работоспособность веб-страницы или иной информационной системы посредством создания огромного числа клиентских запросов, превысив максимальную пропускную способность [8]. Данная кибератака нацелена на нагрузку системы до состояния «отказа». Это может быть выгодно конкурирующей компании в борьбе за рынок сбыта или для кражи информации, составляющую государственную тайну с последующей продажей такой информации.

Для того, чтобы защитить свою базу данных, компании или государственные структуры могут пойти несколькими путями: самостоятельно построить систему распределения или обратиться к компаниям, специализирующихся на защите от DDoS-атак (DDoS-Guard, Лаборатория Касперского, Ростелеком Солар и др.).

Каждый подход имеет как свои преимущества, так и недостатки. Первый подход позволяет оставаться независимым от третьих лиц и иметь полный контроль над своей инфраструктурой, однако есть риск, что сотрудник или группа сотрудников, отвечающих за кибербезопасность, могут не справиться с угрозой в связи с отсутствием необходимых знаний в этой области. Преимущества второго подхода состоит в том, что защита инфраструктуры будет передана в руки профессионалов. Стоимость защиты от DDoS-атак варьируется от 4 тыс. руб. до 6 млн. руб. за ежегодный тариф. Зачастую тарифы с самыми минимальными ценами крайне ненадежны и требуют дополнительных платных услуг. Очевидно, что не каждая компания может себе позволить эффективную защиту от такого типа кибератак.

Проанализировав данные компаний, осуществляющих профессиональную защиту от DDoS-атак, можно сделать следующие выводы:

− Количество DDoS-атак с каждым годом неуклонно растет, наибольший прирост был отмечен в 2021 г. в связи с тем, что многие компании перешли на удаленный формат работы;

− Финансовые организации и государственные структуры чаще подвергаются DDoS-атакам;

− Сфера онлайн-торговли становится привлекательной для злоумышленников в период проведения крупных акций, например, «Черная пятница».

С учетом того, что ежегодно растет количество DDoS-атак, можно прогнозировать увеличение спроса на защиту. В данном случае, компании, предоставляющие услуги в области защиты информационной структуры могут воспользоваться ситуацией и завысить стоимость тарифов.

Государство в лице Федеральной антимонопольной службы должно взять под контроль ценообразование в данной отрасли и не допустить рост цен.

Следует отметить, что в РФ функционируют ресурсы, проверяющие и повышающие цифровую грамотность населения.

На едином портале государственных услуг Российской Федерации активизирован раздел «Кибербезопасность – это просто!», обучающий население безопасному поведению в интернете.

Новый раздел на портале государственных услуг Российской Федерации является элементом всероссийской программы кибергигиены, запущенной Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации совместно с Санкт-Петербургским государственным университетом телекоммуникаций им. М.А. Бонч-Бруевича, «РТК-Солар» и АНО «Диалог Регионы».

Целью программы, реализуемой в рамках федерального проекта «Информационная безопасность» национальной программы «Цифровая экономика», является привлечение внимания к вопросам кибербезопасности и формирования у населения навыков безопасного поведения в интернете. Всероссийская программа кибергигиены предполагает организацию мониторинга уровня грамотности населения по вопросам информационной безопасности [8].

В рамках программы кибергигиены запущены спецпроекты повышения киберграмотности населения.

«КиберЗОЖ» – это сайт о простых правилах кибербезопасности: создание надежных паролей, защита мобильного устройства, проверка безопасности сайтов. Раздел «Сложные несложные пароли» содержит информацию о качественной защите аккаунта и способах создания сложных паролей, которые трудно сломать.

Особое внимание следует уделять обучению киберграмотности детей и подростков. «Кибербуллинг» – это истории блогеров в соцсетях о том, как они преодолели кибербуллинг, а также сайт для детей и подростков о борьбе с травлей в интернете [8].

В новом разделе на портале государственных услуг пользователи имеют возможность:

− Пройти тест с целью проверки умений распознавать типичные уловки интернет-мошенников и защищать свои персональные данные;

− Узнать способы защиты от различных типов угроз – от взлома аккаунта до телефонного мошенничества;

− Ознакомиться со специальными памятками по кибербезопасности, в которых рассмотрены новые схемы злоумышленников, включая похищение

средств с банковских счетов, сообщения об ошибочных платежах и поддельные предложения оформить пособие от государства, перечислены основные фразы телефонных мошенников, а также информация, которую нельзя раскрывать.

На едином портале государственных услуг Российской Федерации персональные данные пользователей надежно защищены. Однако для предотвращения большей части атак на пользователей следует строго соблюдать правила безопасного поведения в интернете, такие как надежный пароль, двухфакторная аутентификация, выявление мошеннических фишинговых писем.

Выводы

Рассмотренные действия в сфере информационных технологий, имеющие преступный характер, всегда в конечном итоге нацелены на извлечение материальной выгоды. Безусловно, быстрое развитие информационных технологий оказало большое положительное влияние и принесло в нашу жизнь множество удобств, но вместе с этим вызвало проблемы, с которыми трудно справиться. Таким образом, роль государства заключается в том, чтобы всячески способствовать снижению уровню киберпреступности и содействовать развитию информационной безопасности в стране.

Библиографический список

1. Ловцов Д.А., Богданова М.В., Лобан А.В., Паршинцева Л.С. Статистика (комп. курс): учебник для вузов / Под ред. проф. Д.А. Ловцова. М.: РГУП, 2020. 400 с.

2. Статистика и аналитика // Официальный сайт Министерства внутренних дел Российской Федерации. [Электронный ресурс]. URL: https://мвд.рф/dejatelnost/statistics (дата обращения 15.11.2022).

3. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ // Собрание законодательства Российской Федерации от 2006 г., N 31, ст. 3448 (Часть I).

4. Ловцов Д.А. Теория защищенности информации в эргасистемах: Монография. М.: РГУП, 2021. 276 с.

5. Что такое «фишинг» // Лаборатория Касперского. [Электронный ресурс]. URL: https://encyclopedia.kaspersky.ru/knowledge/what-is-phishing/ (дата обращения 15.11.2022).

6. Отчеты по спаму и фишингу // Лаборатория Касперского. [Электронный ресурс]. URL: https://securelist.ru/category/spam-and-phishing-reports/ (дата обращения 15.11.2022).

7. Фишинговых атак стало на 28% больше // Лаборатория Касперского. [Электронный ресурс]. URL: https://www.kaspersky.ru/about/press-releases/2018_28-percent-more-phishing-attacks-kaspersky-lab-told-how-fraudsters-are-trying-to-cash-in-on-internet-users (дата обращения 15.11.2022).

8. Что такое DDoS-атаки и как от них защищаться бизнесу // РБК. [Электронный ресурс]. URL: https://trends.rbc.ru/trends/industry/6062ec9e9a79477e19624d6a (дата обращения 15.11.2022).

9. Официальный сайт Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации. [Электронный ресурс]. URL: https://digital.gov.ru/ru/ (дата обращения 15.11.2022).