УДК 343.3/.7

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

ПРОТИВОДЕЙСТВИЯ ЭКОНОМИЧЕСКИМ ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ В ИНФОРМАЦИОННОЙ СФЕРЕ

Ключевые слова: киберпреступления, киберпространство, информационная сфера, защита конфиденциальных данных, информационная безопасность, экономические преступления.

Статья посвящена рассмотрению мероприятий по борьбе с экономическими преступлениями, совершаемыми в информационной сфере. Определены ключевые меры противодействия преступлениям в IT-сфере. Конкретизируются понятия «киберпространства» и «киберпреступлений» и на этой основе выявляются виды преступлений, совершаемые с использованием информационных-коммуникационных технологий. Выявляются меры, направленные на обеспечение защиты, сохранности и предотвращения утечек конфиденциальных данных в компаниях. Выделены основные факторы стремительного роста преступлений в информационном обществе в России. Рассмотрены организационные, правовые и технические меры по обеспечению защиты и сохранности конфиденциальных данных. Обоснована необходимость постоянного совершенствования для организаций качества информационной безопасности. Сформулированы наиболее важные рекомендации по повышению информационной безопасности в современных условиях. Отмечен недостаточный уровень мер по борьбе с экономическими преступлениями, совершаемыми в информационной сфере.

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

COUNTERACTION TO ECONOMIC CRIMES COMMITTED IN THE INFORMATION SPHERE

Keywords: cybercrimes, cyberspace, information sphere, protection of confidential data, information security, economic crimes.

The article is devoted to the consideration of measures to combat economic crimes committed in the information sphere. The key measures to counteract crimes in the IT sphere have been identified. The concepts of «cyberspace» and «cybercrime» are specified and on this basis the types of crimes committed using information and communication technologies are identified. Measures aimed at ensuring the protection, safety and prevention of leaks of confidential data in companies are identified. The main factors of the rapid growth of crimes in the information society in Russia are identified. Organizational, legal and technical measures to ensure the protection and safety of confidential data are considered. The necessity of continuous improvement for organizations of the quality of information security is substantiated. The most important recommendations for improving information security in modern conditions are formulated. An insufficient level of measures to combat economic crimes committed in the information sphere was noted.

Информационные технологии стали неотъемлемой частью современного мира, их появление отразилось на развитии всех сфер жизни общества. К сожалению, информационной сетью и телекоммуникациями стали пользоваться злоумышленники в своих личных и корыстных целях, что обусловило возникновение новых видов преступлений, в том числе экономических. В связи с этим появилась необходимость разрабатывать и осуществлять меры борьбы с противоправными действиями, осуществляемыми в информационной сфере.

Киберпреступная деятельность отличается от других видов преступлений использованием компьютерной техники и информационных технологий. Кроме того, нестандартность выступает отличительным признаком киберпреступлений, поскольку представляется невозможным определить следующие действия преступника и ход событий.

Ввиду вышесказанного, тема исследования является актуальной и своевременной в современных реалиях.

Целью исследования является выявление мер противодействия экономи-

ческим преступлениям, совершаемым в информационной сфере.

Материал и методы исследования

Выполненное исследование базируется на научных трудах российских и зарубежных ученых в области мероприятий по борьбе с экономическими преступлениями, совершаемыми в информационной сфере, 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

Киберпреступлением признается незаконная деятельность, возникающая с целью завладения компьютером, вычислительной сетью или сетевым оборудованием.

На рисунке 1 представлены отличительные особенности киберпреступлений.

Киберпреступлением признается незаконная деятельность, возникающая с целью завладения компьютером, вычислительной сетью или сетевым оборудованием.

В частых случаях киберпреступной деятельностью занимаются кибернарушители или компьютерные взломщики. В редких случаях киберпреступления совершаются по политическим или личным причинам. Преступления в сети могут совершаться как группой людей, так и отдельными лицами.

На рисунке 2 представлена статистика по киберпреступлениям за 2017 – 2021 гг.

Каждый день преступники находят новые способы избежать заданные барьеры противодействия. В 2018 г. прирост по зафиксированным киберпреступлениям составил 33,85% по сравнению с аналогичным периодом. За 2019 год – 142,82%, за 2020 год – 73,36%, а за 2021 год – всего лишь 1,4%. Следует понимать, что данная статистика ведется по возбужденным делам, и как следствие, настоящая проблема более обширна.

Существуют различные виды киберпреступлений. Они могут включать в себя финансовые преступления, связанные с кражей данных и денежных средств с банковских карт, внедрение вредоносных программ, таких как компьютерные вирусы, взломы паролей, распространение информации, имеющей противоправный характер и многое другое [6].

В связи с появлением киберпреступников появилась необходимость регулировать деятельность в информационном пространстве. Главным документом, регулирующим преступную деятельность в сети, выступает глава 28 УК РФ «Преступления в сфере компьютерной информации», которая сводом статей регулирует противоправные действия в сети [1]. Также, у компаний существует личная политика защиты информации (качество системы безопасности, оптимальный расчет основных рисков в случае происшествия, различные виды договоров).

Стоит отметить, что количество совокупных преступлений становится меньше, вместе с этим количество преступлений, совершаемых в экономической сфере все также является высоким (рисунок 4).

Основной фактор данного явления – цифровизация в обществе. На данный момент все больше людей имеют доступ к сети Интернет, что, безусловно, является положительным явлением, однако вместе с этим данный факт существенно облегчает жизнь преступникам.

В соответствии с рисунком 4, удельный вес преступлений, совершенных в экономической сфере в 2021 году составил 41%. За период январь-декабрь 2021 года МВД России подвел итоги и оценил ущерб в 641,9 млрд. руб. от экономических преступлений.

В сфере экономической деятельности большее количество преступлений составили хранение, перевозку и сбыт поддельных денежных средств и ценных бумаг.

МВД России также отметил значительное количество случаев легализации денег, а также ведения незаконной предпринимательской деятельности.

В структуре преступности России за 2021 год 33% экономических преступлений были совершены против государственной и частной собственности (кража, мошенничество и т.д.).

Рис. 1. Отличительные особенности киберпреступлений [4]

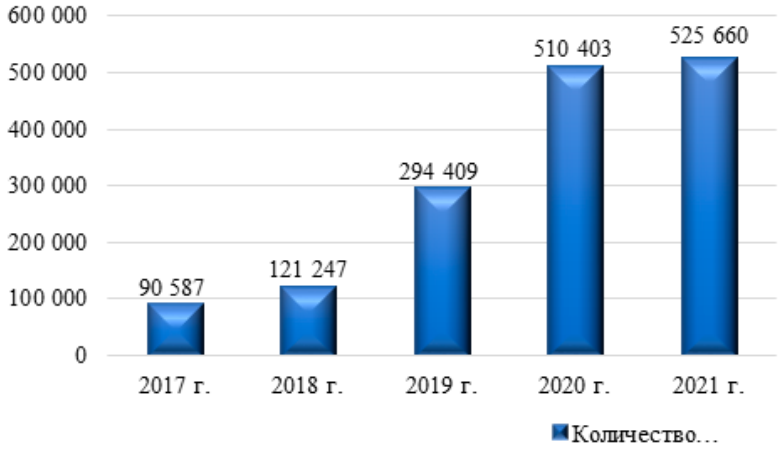

Рис. 2. Статистика киберпреступлений за 2017 – 2021 гг. (Источник: МВД России)

Рис. 3. Классификация киберпреступлений [7]

Рис. 4. Структура преступности в России за 2021 год, в % (Источник: МВД России)

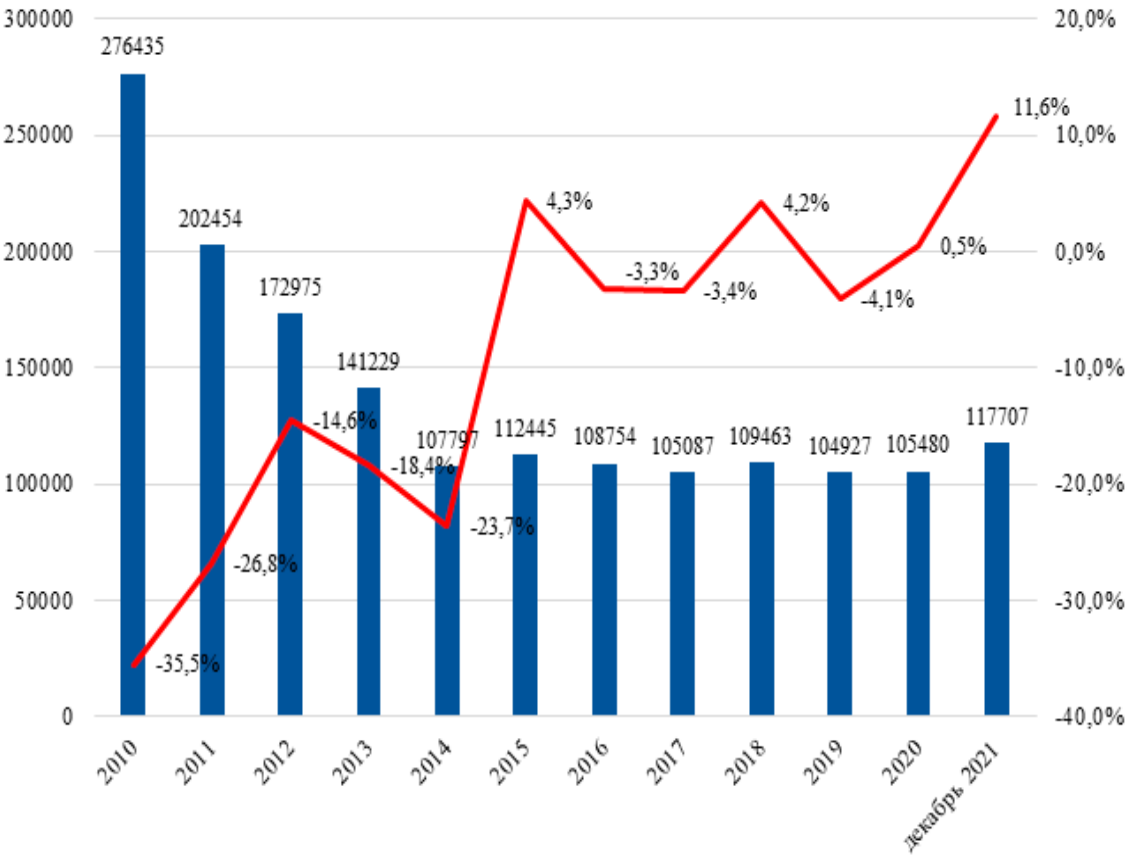

Рис. 5. Зарегистрированные преступления экономической направленности [8]

Около 17,5% преступлений пришлось на экономические преступления против органов власти и интересов государственной службы. К данным экономическим преступлениям в основном относится получение взятки (ст. 290 УК РФ).

Примерно 6% экономических преступлений совершались в сфере налогов.

Экономические преступления в сумме за 2021 г. составили 117,7 тыс., что выше на 11,6%, чем за 2020 г.

Несмотря на то, что экономические преступления зачастую связаны с киберпреступлениями, динамика расходится. Киберпреступления растут с достаточно большим темпом, а экономические преступления растут более сдержанно, что даёт мысль о том, что в современном мире киберпреступления все меньше связаны с экономической сферой, а именно: незаконная банковская деятельность, лжепредпринимательство, легализация (отмывание) денежных средств или иного имущества, приобретенных незаконным путем, незаконное получение кредита, злостное уклонение от погашения кредиторской задолженности, преднамеренное банкротство, коммерческий подкуп, уклонение от уплаты налогов, контрабанд.

Из общего числа экономических преступлений высокая доля не раскрываемости как следует из статистики.

В текущее время в Российской Федерации задачи формирования информационной безопасности финансовых организаций и так же развитие защищённости цифровой отрасли является одним из главных приоритетов Банка России.

Выделяют следующие основные факторы стремительного роста преступлений в информационном обществе в России:

1. Недостаточно проработанное законодательство в области уголовного права, заключающееся в обширности, запутанности норм, несистематизации, относительно легком наказании, узкой базе преступлений. Для примера можно привести законодательство США, где предусмотрены достаточно строгие меры наказания за кибепреступления. За взлом и проникновение в компьютерные сети наказывается сроком до 30 лет лишения свободы без права долгосрочного освобождения. В российском законодательстве максимальный срок лишения свободы за IT-преступления составляет 7 лет.

2. Низкий уровень квалификации сотрудников ведомственных органов, занимающихся раскрытием киберпреступлений. Необходимо отметить, что преступления в сети являются наиболее сложными в расследовании, поскольку требуют от сотрудников определенные знания и опыт в данной области.

3. Формирование киберпреступной отрасли: низкий порог входа в следствии высокой доступности к информации в Интернете. Сегодня любой гражданин может изучить основы кибердеятельности (взломы сайтов, распространение вредоносных программ и так далее), поскольку в сети Интернет вся информация предоставляется в свободном доступе.

4. Низкий уровень культурного образования населения: минимальное представление об информационной и компьютерной безопасности. В России граждане не уделяют достаточное внимание проблеме распространения киберпреступности.

Для компаний немаловажной задачей является обеспечение защиты конфиденциальных данных. Это связано с тем, что разглашение важной информации способно привести к потере клиентской базы и снижению доходов фирмы, что негативно может отразиться на ее репутации. Для предотвращения утечки конфиденциальной информации компании применяют комплекс различных мероприятий. Выделяют организационные, правовые и технические меры по обеспечению защиты и сохранности конфиденциальных данных [5].

Организационные меры защиты информации ориентированы на формирование безопасных условий работы компаний, располагающих конфиденциальными данными. К организационным мероприятиям по защите и охране секретной информации в организации относятся:

– разработка положений и регламентов по обеспечению информационной безопасности, которые должны быть четко структурированы на основе бизнес-процессах, протекающих в компании;

– организация политики безопасности компании, которая формируется на основе анализа рисков и содержит

решения экономических, информационных, технических и юридических вопросов безопасности;

– назначение должностных лиц, отвечающих за безопасность секретных материалов;

– создание системы по допуску работников к разным по степени секретности документам;

– проведение мероприятий по профессиональной подготовке и переподготовке персонала.

Правовые меры связаны с контролем за исполнением норм права безопасности в информационной сфере. Данные мероприятия помогают компаниям, владеющим ценными данными, проводить служебные расследования, по результатам которых можно выявить рассекретил ли какой-либо сотрудник информацию.

Существуют два основных закона, регулирующих защиту информации – ФЗ №149 «Об информации, информационных технологиях и о защите информации» и ФЗ №152 «О персональных данных». Опираясь на закон 149-ФЗ, компании могут определить, какие данные будут являться секретными, и когда следует ограничивать к ним доступ. Кроме того, этот документ определяет ключевые требования работы с конфиденциальной информацией и устанавливает ответственность за нарушения этих требований [2]. Закон 152-ФЗ затрагивает практически любую организацию, которая хранит конфиденциальную информацию о своих клиентах и работниках. Он определяет правила должного обращения с персональной информацией граждан России, а также обеспечивает ее защиту [3].

Охрана информации также осуществляется при помощи технических средств и специального оборудования. Такие мероприятия предназначены для предупреждения и предотвращения несанкционированного разглашения данных. В компаниях, владеющих секретными данными, предполагается наличие устройств для отслеживания и обнаружения прослушивания.

Технические меры информационной безопасности предполагают:

– установку системы контроля и управления доступом (СКУД) и ее отдельных элементов, предупреждающих о возможном проникновении в помещение;

– использование специальных аппаратных и программных устройств с целью аутентификации и авторизации пользователей;

– установку аппаратуры, предполагающей обеспечение сохранности секретных и ценных сведений при попытке их утечки;

– применение антивирусных программ.

Для организации особенно важно постоянно совершенствовать качество информационной безопасности. Для этого можно выделить 8 наиболее важных рекомендаций в настоящий момент.

1. Обеспечение безопасности сотрудникам, работающим в удаленном доступе.

Сегодняшняя ситуация как в России, так и во всем мире вынуждает заменять ежедневное посещение офиса на работу дома. Необходимо правильно производить оценку распределения целесообразности допуска каждого отдельного сотрудника к определенным базам.

2. Менеджмент с упором на риск.

Основная рекомендация заключается в том, чтобы не распыляться, а сконцентрироваться на действительно существующих проблемах, которые несут потенциальную угрозу бизнесу. Вместо массовой оценки следует использовать аналитику угроз, которая позволяет оценить активность киберпреступников и возможные последствия от их действий.

3. Использование системы Extended Detection and Response.

Данная система позволяет обнаруживать и быстро реагировать на потенциальные угрозы взлома. Эта платформа обладает рядом преимуществ, необходимых для комплексного решения проблем: абсолютный мониторинг, быстрое реагирование на кибератаки, простота в использовании.

4. Использование облачных сервисов охраны данных.

Облачные сервисы помогают предприятию защищать личные данные путем маршрутизации трафика чрез облачные системы безопасности. К примеру, SASE, который используется в виде службы облачных вычислений, подклю-

ченное непосредственно к источнику, а не к центру обработки данных.

5. Контроль доступа к облаку.

Контроль доступа можно выполнять через определенные системы, например, CASB, который позволяет провести моментальную блокировку в случае необходимости.

6. Применение политики DMARC.

DMARC позволяет бороться с интернет-мошенничеством в сети, отсеивая и блокируя email-рассылки и спам. Данная политика распознает и идентифицирует почтовый домен адресанта сообщения. Однако DMARC не следует использовать как отдельный самостоятельный продукт, он должен применяться системно с другими методами защиты безопасности. Данная спецификация позволяет проводить дополнительную проверку сети и предотвращать многие угрозы кибератак.

7. Система беспарольного входа.

В следствии того, что работники зачастую не используют комплексные пароли для защиты данных (даты рождения, имя домашнего питомца и так далее), то возможно применение различных систем беспарольной аутентификации. Данный подход позволяет обезопасить важную информацию компании.

8. Разработка эффективной системы отбора кадров. Правильно организованный процесс подбора персонала соответствующей квалификации позволит руководству компании повышать результативность работы. Оценка компетенций потенциального сотрудника может осуществляться различными способами, включая кибер-ранжирования и киберсимуляции.

Выводы

На данный момент статистика показывает, что в большинстве своем, не смотря на обширный инструментарий, принятые меры являются недостаточными. Любая организация и частное лицо могут снизить вероятность оказаться жертвой киберпреступников, если помимо использования представленных мер будут более осведомлены об основных трендах в киберпреступном обществе. Кроме того, организации будут разрабатывать и постоянно модернизировать имеющуюся у них политику информационной безопасности.

Библиографический список

1. «Уголовный кодекс Российской Федерации» от 13.06.1996 N 63-ФЗ (ред. от 01.07.2021).

2. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ (последняя редакция).

3. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ (последняя редакция).

4. Николюк М. С. Влияние пандемии на угрозу со стороны киберпреступности в России и мире. 2020.

5. Информационная безопасность – SearchInform. Меры по обеспечению информационной безопасности. [Электронный ресурс]. URL: https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/osnovnye-aspekty-informatsionnoj-bezopasnosti/osnovnye-printsipy-obespecheniya-informatsionnoj-bezopasnosti/mery-po-obespecheniyu-informatsionnoj-bezopasnosti/ (дата обращения 15.06.2022).

6. «Лаборатория Касперского». Советы по защите от киберпреступников. [Электронный ресурс]. URL: https://www.kaspersky.ru/resource-center/threats/what-is-cybercrime

7. Киберпреступность: история развития, проблемы практики расследования. [Электронный ресурс]. URL: https://www.computer-museum.ru/articles/materialy-mezhdunarodnoy-konferentsii-sorucom-2014/629/ (дата обращения 15.06.2022).

8. Портал правовой статистики. [Электронный ресурс]. URL: http://crimestat.ru/offenses_chart (дата обращения 07.06.2022).