Российский экономический интернет-журнал №2/2022

Научная статья
Original article
УДК 338

Киберпреступность в Российской Федерации: экономические последствия и государственные инициативы по борьбе с ней

Чугунов В.В., магистрант 2 курса направления подготовки «Государственное и муниципальное управление»,
Обнинский институт атомной энергетики – филиал Национального исследовательского ядерного университета «МИФИ», Обнинск, Россия
Найденкова К.В., к.э.н., доцент отделения социально-экономических наук
Обнинский институт атомной энергетики – филиал Национального исследовательского ядерного университета «МИФИ», Обнинск, Россия

Аннотация. Научная статья раскрывает такую важную и актуальную на сегодняшний день тему как киберпреступность. Определены основные тенденции развития киберпреступности и её воздействие на российскую экономику. Рассмотрены государственные управленческие решения по борьбе с киберпреступностью в России и США.

Ключевые слова: киберпреступность, кибербезопасность, защита информации, критическая инфраструктура

Cybercrime in the Russian Federation: economic consequences and government initiatives to deal with it

Chugunov V.V., student of master's program for «State and municipal management»
Obninsk Institute for Nuclear Power Engineering, Obninsk, Russia
Naydyonkova K.V., Candidate of Economic Sciences, associate professor of Department of social and economic sciences
Obninsk Institute for Nuclear Power Engineering, Obninsk, Russia

Annotation. The scientific article reveals such an important and relevant topic today as cybercrime. The main trends in the development of cybercrime and its impact on the Russian economy are determined. The state administrative decisions on dealing with cybercrime in Russia and the USA are considered.

Key words: cybercrime, cybersecurity, information security, critical infrastructure.

Экономическая преступная деятельность является одной из важнейших проблем не только в России, но и во всём мире. Её самым новым и наиболее активно растущим сегментом является киберпреступность. Связано это с развитием глобализации в области ИКТ и цифровизации международных отношений и публичного управления [4].

Число уникальных атак на информационное пространство РФ в 2020 году выросло на 52% по сравнению с 2019 годом и на 211% по сравнению с уровнем 2017 года, что говорит о стабильном увеличении числа преступлений за 1 год приблизительно в полтора раза по отношению к предыдущему периоду. На рис. 1 перечислены основные мотивы совершения кибератак на Российскую Федерацию.

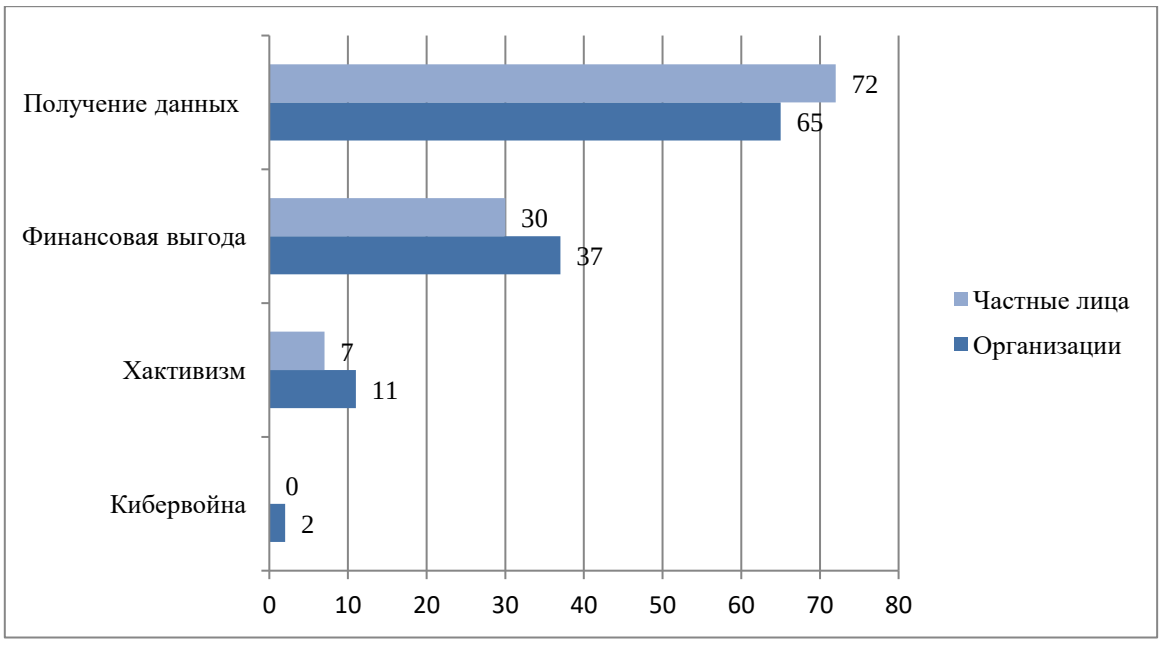

Рис. 1 – Мотивы злоумышленников, доля атак в % [5]

Вышеперечисленные данные позволяют подтвердить предварительно сделанный нами вывод о том, что примерно каждое третье киберпреступление, жертвами которого становились как частные лица, так и организации, совершалось с целью получения финансовой выгоды. Однако преступления, связанные с хищением персональных данных, также негативно влияют на состояние российской экономики, поскольку злоумышленники, в большинстве случаев, продают полученную информацию на теневых интернет-ресурсах. Особенно сильный ущерб наносится предприятиям, поскольку имея доступ к базам данных ИКТ-инфраструктуры, у преступников появляется возможность к частичной или полной остановке функционирования рабочих процессов предприятия.

Заместитель Председателя правления Сбербанка Станислав Кузнецов сообщает об общих потерях экономики от действий хакеров в 2019 году в размере 2,5 трлн. рублей, и почти 4 трлн. рублей в 2020 году. Значительный рост в 2020 году связан прежде всего с введением дистанционной занятости значительной части офисных сотрудников из-за пандемии COVID-19, что позволило злоумышленникам проводить ещё большее число атак в связи с низким уровнем защищенности средств работы с информацией этих сотрудников. В начале 2021 года руководство Сбербанка спрогнозировало увеличение потерь в полтора раза в случае непринятия экстренных мер по борьбе с киберпреступностью. Также была названа средняя сумма убытков от одной мошеннической операции: для физических лиц – 12,6 тыс.руб., для юридических лиц – 358,9 тыс.руб. По итогам 2021 года со ссылкой на руководителя российской секции Международной полицейской ассоциации Юрия Жданова РИА Новости обнародовали цифру доказанного причиненного ущерба только от телефонных мошенничеств в размере свыше 45 миллиардов рублей.

Помимо этого, были определены наиболее дорогостоящие виды атак на предприятия среднего и крупного бизнеса. Таковыми являются:

- неправомерное использование сотрудниками ИТ-ресурсов (39 млн. рублей и 2,25 млн. рублей для предприятий крупного и среднего бизнеса, соответственно);

- несоблюдение внутренних регламентов политики информационной безопасности (36,3 млн. рублей и 2,4 млн. рублей для предприятий крупного и среднего бизнеса, соответственно);

- DDoS-атаки (35,4 млн. рублей и 1,9 млн. рублей для предприятий крупного и среднего бизнеса соответственно).

При этом по данным департамента информационной безопасности Банка России, банкам удаётся вернуть только 11,8% украденных средств. Такой низкий процент возврата обусловлен тем, что самым популярным методом атак остаётся социальная инженерия – частные лица или предприятия сами выдают свои данные мошенникам, а кредитные организации не возвращают деньги, если клиент нарушил условия договора, касающиеся сохранения конфиденциальности платежной информации [2].

Категории организаций, атакованных мошенниками, представлены на рис. 2.

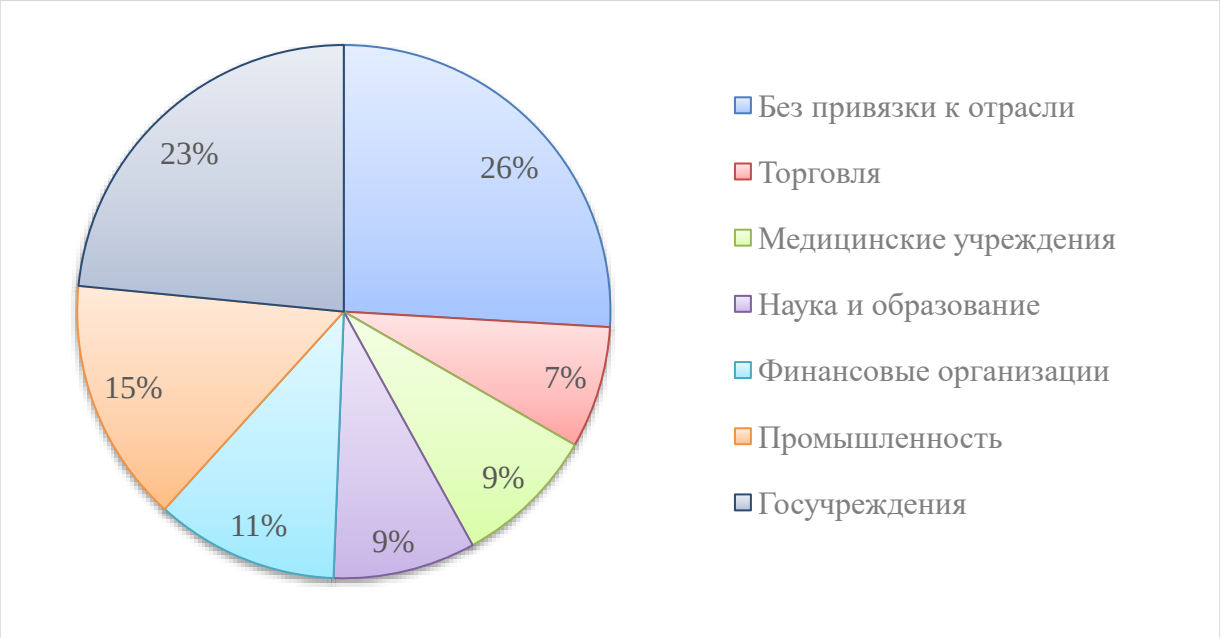

Рис. 2 – Категории организаций, атакованных мошенниками, доля атак [5]

Статистика по организациям в Российской Федерации существенно отличается от мировой. В РФ гораздо реже атакуют медицинские учреждения, но при этом более высокий процент атак на госучреждения и финансовые организации. Связано это с тем, что в зарубежных медицинских учреждениях хранится куда больший объём данных, вплоть до данных банковских карт и кодов доступа к

ним, поэтому в России этот сектор не так интересен для хакеров, а вот уровень защищенности отечественных финансовых организаций ниже других стран, поэтому доля атак на него выше среднего.

Именно поэтому рынок информационной безопасности (ИБ) Российской Федерации растёт с каждым годом, и по итогам 2020 года стал больше ещё на 25%. На 2021 год объем рынка информационной безопасности оценивается приблизительно в 98,68 млрд.руб. [4]. Существуют следующие основные причины такого роста:

- информационная безопасность, являющаяся одним из основных бизнес-процессов предприятия, становится все более важной и актуальной ввиду роста числа угроз и атак;

- необходимость расходов на поддержку ИБ становится очевидной для управляющих большинства организаций;

- информационная безопасность превратилась из планов, использовать которые собирались только в случае крайней необходимости в реально используемый инструмент [6].

Первой попыткой обеспечения дополнительной защиты кибербезопасности, со стороны государства стала разработка Советом Федерации Концепции стратегии кибербезопасности в 2013 году. Предпосылкой создания такого документа стали особенности Доктрины информационной безопасности и Стратегии развития информационного общества в Российской Федерации: оба документа не отражали серьезность киберугроз, хотя на момент рассмотрения стратегии процент атак в виртуальном пространстве и ущерб от них стремительно росли.

Авторы концепции предлагали пользоваться помощью отечественных «белых хакеров» – специалистов по обнаружению уязвимостей в виртуальной среде и не связанных с криминальными структурами. Данный метод давно используется крупнейшими корпорациями, такими как Apple и Google. Также было предложено усиление ответственности за совершение киберпреступлений и поддержка деятельности отечественных компаний по созданию средств информационной защиты через налоговые льготы.

Отметим, что концепция не была принята из-за того, что она противоречила политике РФ в данной сфере, а именно имелись проблемы с терминологией: эксперты не хотели отделять понятие «кибербезопасность» от общего понятия «информационная безопасность», которое фигурировало во всех нормативных актах в этой сфере. Однако, несмотря на то что концепцию так и оставили на этапе рассмотрения, большая часть ее основополагающих идей в дальнейшем нашла отражение в других нормативных актах и учреждениях по защите информации.

Первым эффективным государственным управленческим решением в развитии национальной стратегии кибербезопасности стало принятие концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ, утверждённой Президентом РФ в конце 2014 года. Она стала основой для последующего развития законодательной базы в сфере кибербезопасности.

В 2016 году начинают проводиться первые мероприятия, связанные с реализацией положений вышеуказанной концепции. Ключевым стало создание единой государственной системы под названием ГосСОПКА по обнаружению и ликвидации кибератак на российские критическую информационную инфраструктуру и дипломатические представительства за рубежом. В данной системе осуществляется и агрегируется информация от субъектов критической информационной инфраструктуры (КИИ) по всем компьютерным атакам и инцидентам. Технически, ГосСОПКА представляет собой систему центров, установленных на объектах КИИ и подключенных к ним техники. Причём у системы нет единого собственника, центры могут быть организованы частными организациями, имеющими лицензию в области защиты информации, так и государственными органами. В отношении частных организаций государство выступает в качестве регулятора.

В июне 2017 г. был принят главный федеральный закон в сфере национальной кибербезопасности «О безопасности критической информационной инфраструктуры Российской Федерации». Он закрепляет понятие и объекты КИИ,

требования по обеспечению их безопасности. Также закон регламентирует деятельность центров защиты ГосСОПКА, методику их деятельности и используемые средства предотвращения атак. Данный закон, безусловно, поспособствовал улучшению дел в области защиты виртуального пространства, так как он официально закрепил множество терминов и положений, отсутствовавших в Доктрине информационной безопасности и прочих законодательных актах, и сфокусировал внимание на существующих проблемах, однако, окончательно не решил их [3].

Именно для этой цели в 2018 году был основан Национальный координационный центр по компьютерным инцидентам (НКЦКИ), утвержденный приказом директора ФСБ России. Основной задачей специалистов центра является обнаружение компьютерных атак на все сферы безопасности РФ: промышленную, военную, продовольственную, энергетическую и банковскую. Ещё одной задачей НКЦКИ является координация государственных органов и компаний с собственными IT-системами из вышеперечисленных сфер.

К концу 2020 года Россия, благодаря принятым государством мерам, уже вошла в десятку стран с наивысшим глобальным индексом кибербезопасности, однако на современном этапе ей все ещё не хватает уникальных методов защиты киберпространства, которые имеют страны с самым высоким индексом защищенности в области кибербезопасности, поэтому целесообразно рассмотреть управленческие решения страны с самым высоким индексом защищенности в сфере кибербезопасности, а именно: опыт США.

Соединенные Штаты Америки первыми в мире подняли вопрос о значимости кибербезопасности ещё в 80-х годах 20 века, и с тех пор их законодательство имеет наибольшее количество законопроектов, нормативных актов и успешно реализованных решений по сравнению с другими странами. Особенно строгие наказания выносятся за хищение интеллектуальной собственности американских компаний [1]. Срок тюремного заключения за подобные преступления составляет в среднем 15-20 лет. Если злоумышленник при этом проник

в критические информационные инфраструктуры, то срок увеличивается до 30 лет, а также теряется право на досрочное освобождение.

Из последних значимых событий, стоит отметить создание министерством юстиции США новой гражданской инициативы по борьбе с кибермошенничеством, основным положением которой является привлечение к уголовной ответственности правительственных подрядчиков, которые не смогли обеспечить себе киберзащиту, соответствующую определенным стандартам, а также тех подрядчиков, которые скрывают факты киберинцидентов от органов власти. На наш взгляд, данный опыт требует безусловного осмысления с учетом российской специфики киберпреступности и особенностей законодательства по противодействию ей и может быть частично применен при построении новой модели национальной кибербезопасности РФ.

Библиографический список:

1. Булавин А.В. О подходах США и Китая к обеспечению кибербезопасности // Общество, политика, экономика, право. – 2016. – № 3. – С. 28-32.

2. Козьминых С.И. Информационная безопасность финансово-кредитных организаций в условиях цифровой трансформации экономики // М.: Прометей, 2020. – 578 с.

3. Матвеев В.А., Цирлов В.Л. Состояние и перспективы развития индустрии информационной безопасности Российской Федерации // Вопросы кибербезопасности. – 2016. – №1 (1). – С. 61-64.

4. Официальный сайт национального провайдера технологий кибербезопасности Ростелеком-Солар [Электронный ресурс] Режим доступа: https://rt-solar.ru/ (дата обращения: 21.01.2022).

5. Смекалова М.В. Эволюция доктринальных подходов США к обеспечению кибербезопасности и защите критической инфраструктуры // Вестник московского университета. – 2021. – №5. – С. 47-69.

6. Шимко М.В. Системы сбора информации в аспекте кибербезопасности // Вестник Российской академии наук. – 2018. – №12. – С. 28-39.

References:

1. Bulavin A.V. On the approaches of the USA and China to ensuring cybersecurity // Society, politics, economics, law. – 2016. – № 3. – pp. 28-32.

2. Kozminykh S.I. Information security of financial and credit organizations in the conditions of digital transformation of the economy // Moscow: Prometheus, 2020. – 578 S.

3. Matveev V.A., Cirlov V.L. State and prospects of development of the information security industry of the Russian Federation // Cybersecurity issues. – 2016. – №1 (1). – Pp. 61-64.

4. Official website of the national provider of cybersecurity technologies Rostelecom-Solar [Electronic resource] Access mode: https://rt-solar.ru / (accessed: 01/21/2022).

5. Smekalova M.V. Evolution of US doctrinal approaches to cybersecurity and critical infrastructure protection // Bulletin of the Moscow University. – 2021. – № 5. – pp. 47-69.

6. Shimko M.V. Information collection systems in the aspect of cybersecurity // Bulletin of the Russian Academy of Sciences. – 2018. – № 12. – pp. 28-39.

Для цитирования: Чугунов В.В., Найденкова К.В., Киберпреступность в Российской Федерации: экономические последствия и государственные инициативы по борьбе с ней/ Российский экономический интернет-журнал. – 2022. – № 2. URL: