DOI 10.17150/2411-6262.2020.11(1).6 http://brj-bguep.ru

УДК 338.2:04

А.Л. Бушуев
Байкальский государственный университет, г. Иркутск, Российская Федерация
И.В. Деревцова
Байкальский государственный университет, г. Иркутск, Российская Федерация
Ю.А. Мальцева
Байкальский государственный университет, г. Иркутск, Российская Федерация
В.Д. Терентьева
Байкальский государственный университет, г. Иркутск, Российская Федерация

РОЛЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВОЙ ЭКОНОМИКИ

АННОТАЦИЯ. Современный уровень развития экономики предполагает активное использование Интернета, спутниковой связи, новых технологий обработки, хранения и передачи информации, что, в свою очередь, делает актуальной проблему защиты персональных данных и обеспечения информационной безопасности государства и предприятий. Несанкционированный доступ к информационным ресурсам организаций, уничтожение, блокирование, копирование и использование информации компаний в корыстных целях третьих лиц наносят значительный ущерб как отдельным гражданам, так предприятиям и государству. В статье рассматривается соотношение понятий информационная безопасность и экономическая безопасность, определяются существующие на сегодняшний день вызовы и угрозы экономической безопасности в условиях цифровой трансформации, проводится анализ статистических данных экономических преступлений с использованием цифровых технологий; устанавливаются возможные причины и факторы ослабления безопасности цифровой экономики. Авторами работы представлен анализа статистических данных, характеризующих количество и структуру преступлений, связанных с нарушением информационной безопасности страны и территорий. В частности, были рассмотрены такие виды преступлений, как кибератаки на веб-сайты органов государственной власти; создание, использование и распространение вредоносных компьютерных программ; мошенничество с применением электронных средств платежа.

КЛЮЧЕВЫЕ СЛОВА. Информационная безопасность, цифровая экономика, экономическая безопасность, угрозы экономической безопасности, национальная безопасность.

ИНФОРМАЦИЯ О СТАТЬЕ. Дата поступления 20 декабря 2019 г.; дата принятия к печати 2 марта 2020 г.; дата онлайн-размещения 31 марта 2020 г.

A.L. Bushuyev
Baikal State University, Irkutsk, Russian Federation
I.V. Derevtsova
Baikal State University, Irkutsk, Russian Federation
Yu.A. Maltseva
Baikal State University, Irkutsk, Russian Federation
V.D. Terentyeva
Baikal State University, Irkutsk, Russian Federation

ROLE OF INFORMATION SECURITY IN TERMS OF DIGITAL ECONOMY

ABSTRACT. The current level of economic development implies an active use of the Internet, satellite communications, and new technologies of processing, storing, and transmitting information, which, in its turn, makes the problem of protecting personal data and ensuring information security of the state and enterprises urgent. Unauthorized access to information resources of organizations, destruction, blocking, copying and use of companies' information for the deceptive purposes of third parties cause significant damage to both individuals and businesses and the state. The article examines the correlation of the concepts of information security and economic security, specifies today's existing challenges and threats to economic security in the context of digital transformation, analyzes the statistical data of economic crimes using digital technologies; it identifies possible causes and factors of weakening the security of the digital economy. The authors present an analysis of statistical data that characterize the number and structure of crimes related to violation of information security of the country and territories. In particular, they examine the following types of crimes: cyber attacks on the websites of public authorities; creation, use and distribution of malicious computer programs; fraud using electronic means of payment.

KEYWORDS. Information security, digital economy, economic security, threats to economic security, national security.

ARTICLE INFO. Received December 20, 2019; accepted March 2, 2020; available online March 31, 2020.

В современных условиях цифровой экономики существует большое количество вызовов и угроз экономической безопасности, преодоление и противодействие которым является важнейшим направлением национальной безопасности государства. Однако нарушители, посягающие на экономическую безопасность государства, организаций и граждан, все чаще находят новые и более совершенные способы осуществления своих злонамеренных действий с использованием цифровых технологий. Задача государственных органов, обеспечивающих экономическую и информационную безопасность — выявить такие способы, минимизировать их влияние в случае возможной реализации и создать условия, направленные на повышение информационной безопасности в условиях цифровой экономики [1].

«Без цифровой экономики мы не сможем перейти к следующему технологическому укладу. А без этого перехода к новому технологическому укладу у российской экономики, а значит и страны, нет будущего» — отметил президент Российской Федерации Владимир Владимирович Путин, отвечая на вопросы во время «Прямой линии» в 2017 г. Безусловно, функционирование цифровой экономики в условиях постоянной цифровой трансформации неизбежно связано с возникновением и влиянием определенного рода угроз. Вызовы и угрозы, с которыми сталкивается цифровая экономика на сегодняшний день, имеют целью подрыв информационной и экономической безопасности российского государства.

Следует отметить, что экономическая и информационная безопасности являются подсистемой национальной безопасности (рис. 1).

Исходя из стратегических целей, определяющих национальные интересы страны, вытекают задачи, позволяющие обеспечить устойчивое развитие страны в долгосрочном промежутке времени.

Экономическая безопасность в системе национальной безопасности играет фундаментальную роль, поскольку без экономического потенциала невозможно противостоять внешним угрозам со стороны мирового сообщества [3].

Рис. 1. Структура национальной безопасности [2]

Нынешнее состояние преступности характеризуется тем, что происходит переход большого количества антисоциальных злоумышленных деяний в киберсреду. По данным Генеральной прокуратуры Российской Федерации, за последние 6 лет киберпреступность выросла в 11 раз [4]. Это очень показательные значения. А если обратить внимание на масштабы и прибыльность в данной преступной сфере, то по некоторым оценкам ущерб мировой экономики от преступности в сфере цифровых и компьютерных технологий составляет от 0,7 до 3 трлн долл. И все это имеет положительную динамику[1].

Для повышения качества жизни граждан, обеспечения конкурентоспособности России, развития экономической, социально-политической, культурной и духовной сфер жизни общества, совершенствования системы государственного управления на основе использования информационных и телекоммуникационных технологий была разработана государственная программа Российской Федерации «Информационное общество»[2].

Для того чтобы определить, насколько широко распространен доступ в интернет для населения и организаций, мы решили проанализировать статистику Федеральной службы государственной статистики в отношении развития информационного общества в Российской Федерации.

Таким образом, мы определили, что по состоянию на конец 2017 г. около 80 чел. населения из 100 имеют мобильный широкополосный доступ в интернет, при этом сохраняется тенденция к увеличению количества абонентов (рис. 2). Фиксированный широкополосный доступ имеет 21 чел. из 100. Эта разница обуславливается размером необходимых инвестиций провайдерами в построение телекоммуникационных сетей. В целом, растет количество абонентов, имеющих как фиксированный, так и мобильный доступ в интернет.

[1] Портал правовой статистики : сайт / Генеральная прокуратура РФ. М., 2019. URL: http://crimestat.ru/ (дата обращения: 15.11.2019).

[2] Об утверждении государственной программы Российской Федерации «Информационное общество» : Постановление Правительства РФ от 15 апр. 2014 г. № 313 // СПС «КонсультантПлюс».

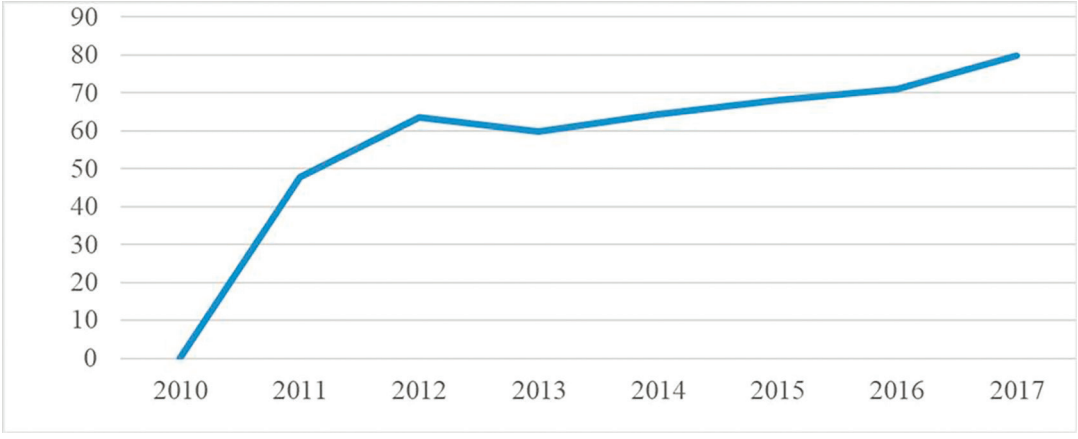

Рис. 2. Число абонентов мобильного широкополосного доступа в Интернет на 100 человек населения, чел.

Источник: Федеральная служба государственной статистики : офиц. сайт. М., 2019. URL: https://www.gks.ru/folder/14477 (дата обращения: 14.11.2019).

Среди организаций также наблюдается рост тех, кто используют интернет в своей деятельности. По состоянию на 2017 г. доля таких организаций составила 89 % (рис. 3).

Можно отметить, что, как среди организаций, так и среди населения доступ в интернет распространен достаточно широко. Значит, высока доля потенциальных жертв киберпреступлений [5]. Мы решили посмотреть, какое количество организаций используют средства защиты информации, и на 2017 г. доля подобных организаций составила 87,2 % (рис. 4). С 2010 г. доля таких организаций выросла на 17,2 %.

По данным Совета Безопасности Российской Федерации, в 2015 г было зафиксировано около 14,4 млн кибератак на веб-сайты госорганов. В 2016 г. эта цифра увеличилась более чем в 3,6 раза и составила 52,5 млн попыток взломать инфор-

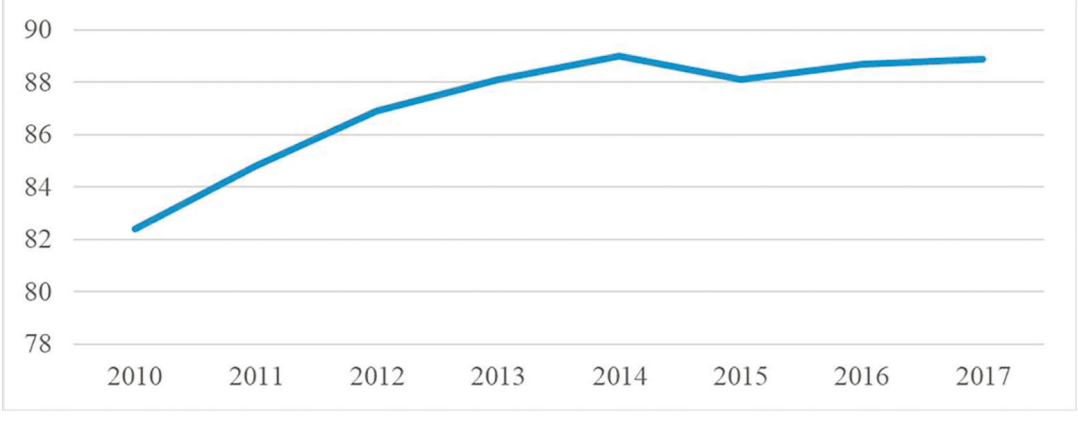

Рис. 3. Доля организаций, использовавших Интернет, в общем числе обследованных организаций, %

Источник: Федеральная служба государственной статистики : офиц. сайт. М., 2019. URL: https://www.gks.ru/folder/14477 (дата обращения: 14.11.2019).

Рис. 4. Доля организаций, использовавших средства защиты информации, передаваемой по глобальным сетям, %

Источник: Федеральная служба государственной статистики : офиц. сайт. М., 2019. URL: https://www.gks.ru/folder/14477 (дата обращения: 14.11.2019).

мационные системы органов государственной власти[3]. Цель большинства атак — получение информации ограниченного доступа и нарушение функционирования технических средств [6].

Структура киберпреступлений по данным прокуратуры представлена на рис. 5. Наиболее значимый удельный вес в количестве преступлений в сфере информационных технологий занимает интернет-мошенничество [7].

В эпоху развития информационных технологий интернет является неким проводником в мир безграничной информации и зачастую простому пользователю затруднительно оценить степень достоверности информации, которую ему преподносят различные сайты и ресурсы. С другой стороны, мошенники, использующие возможности информационных технологий, имеют все возможности для обмана своих потенциальных жертв. Если в реальной жизни им зачастую приходиться коммуницировать со своими жертвами, то в сети Интернет их личность остается в тени, тем самым создавая иллюзию невозможности идентификации преступника [8].

Также немаловажным следует признать и тот факт, что для совершения обмана в виртуальной реальности не обязательно обладать особыми навыками, и без них можно создавать сайты-однодневки с целью своего обогащения.

Нелегальный контент, наоборот, имеет наименьшую долю в структуре киберпреступлений по причине того, что в России у людей сформировано особое отношение к такого рода контенту. Нелегальным он считается только по закону, но в подсознании людей информация воспринимается как вполне легальная и пользоваться ею можно на безвозмездных началах по отношению к правообладателю.

С нелегальным контентом борется служба по надзору в сфере связи, информационных технологий и массовых коммуникаций, у данного органа есть

[3] Статистика и аналитика // Министерство внутренних дел РФ. М., 2019. URL: https://www.Deljatel-nost/statistics (дата обращения: 17.11.2019).

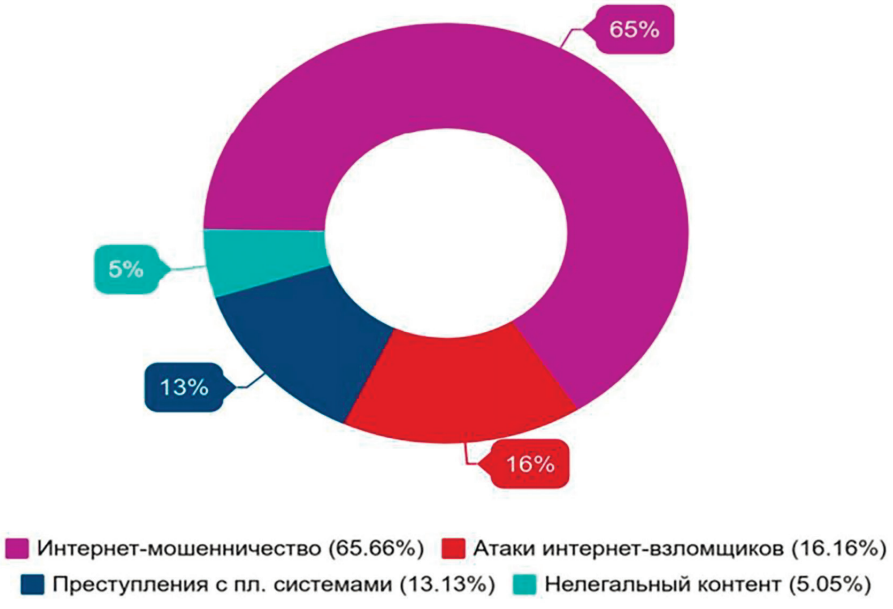

Рис. 5. Структура киберпреступлений, %

Источник: Портал правовой статистики / Генеральная прокуратуры РФ. М., 2019. URL: http://crimestat.ru/ (дата обращения: 15.11.2019).

полномочия блокировать и ограничивать доступ пользователей к нежелательному контенту.

Примечательно, что доли преступлений примерно одинаковы независимо от масштаба предприятия [9]. Это связано с тем, что киберпреступники выбирают себе объект преступления в зависимости от степени защищенности информационных систем[4]. Самое главное правило защиты информационной системы предприятия заключается в следующем: деньги, выделяемые на защиту информационной безопасности не должны превышать стоимость и потенциальную ценность защищаемой информации. Другими словами, микропредприятие не будет защищать свою информацию настолько же эффективно (пропорционально затратам), насколько это делают крупные корпорации [там же].

Структура киберпреступлений против хозяйствующих субъектов представлена на рис. 6.

Отсюда можно сделать вывод: более доступная информация является менее ценной и наоборот. Можно провести параллель с реальной жизнью: одни преступники крадут кошельки в метро, другие — используют различные схемы для максимизации своего дохода. И те, и другие находят себе жертву по своему «уму».

Так, согласно отчету центра мониторинга и реагирования, на компьютерные атаки в кредитно-финансовой сфере (Департамент информационной безопасности Банка России), в 2018 г. более 97 % хищений со счетов физических лиц и 39 % хищений со счетов юридических лиц было совершено с использованием приемов социальной инженерии. Это приемы, с помочью которых преступник злонамеренно вводит в заблуждение свою жертву с помощью обмана или злоупотребления довери-

[4] Ландшафт угроз для систем промышленной автоматизации. Первое полугодие 2018 / АО Лаборатория Касперского. URL: https://ics-cert.kaspersky.ru/reports/2018/09/06/threat-landscape-for-industrial-automation-systems-h1-2018/ (дата обращения: 17.11.2019).

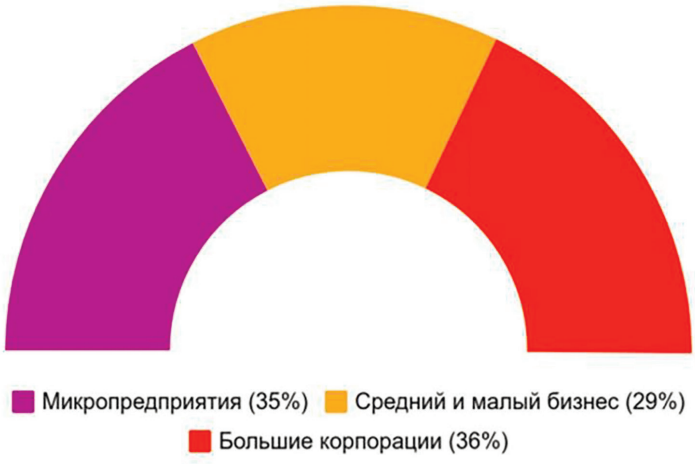

Рис. 6. Статистика по предприятиям, пострадавшим от кибератак, %

Источник: Ландшафт угроз для систем промышленной автоматизации. Первое полугодие 2018 / АО Лаборатория Касперского. URL: https://ics-cert.kaspersky.ru/reports/2018/09/06/threat-landscape-for-industrial-automation-systems-h1-2018/ (дата обращения: 17.11.2019).

ем[5]. Отличительная черта этого вида мошенничества — направленность на конкретные группы граждан: конечной целью злоумышленников является перевод средств жертв на собственные счета, при этом средства достижения этой цели варьируются.

По данным МВД РФ, самыми популярными нарушениями в сфере информационных технологий являются нарушения по следующим статьям [10]: 272 УК РФ «Неправомерный доступ к компьютерной информации» (рис. 7), 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ» (рис. 8), 159.3 УК РФ «Мошенничество с использованием электронных средств платежа» (рис. 9)[6].

Неправомерный доступ к компьютерной информации наказывается уголовной ответственностью в случаях, когда это действие повлекло:

1) нарушение целостности (уничтожение или модификация информации);

– нарушение конфиденциальности (копирование информации);

– нарушение доступности (блокирование информации) [11].

Согласно данным статистики МВД за период с 2012 по 2018 гг. заметен нисходящий тренд расследований преступлений. Число зарегистрированных преступлений год от года варьируется, но остается на достаточно высоком уровне.

На рис. 8 представлена статистика преступлений по ст. 273 УК РФ, с 2015 по 2018 гг. количество расследованных дел по отношению к зарегистрированным составляет около 50 %.

Вредоносное программное обеспечение (далее —ПО) по-прежнему остается одним из основных инструментов компьютерных преступников. Пользователь чаще всего добровольно скачивает «пиратские» видеоигры, компьютерные программы,

[5] Отчет центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Департамента информационной безопасности Банка России 1.09.2017 — 31.08.2018 // Банк России : офиц. сайт. М., 2019. URL: https://www.cbr.ru/Content/Document/File/50959/survey_0917_0818.pdf (дата обращения: 14.11.2019).

[6] Статистика и аналитика // Министерство внутренних дел Российской Федерации. М., 2019. URL: https://www.Deljatel-nost/statistics (дата обращения: 17.11.2019).

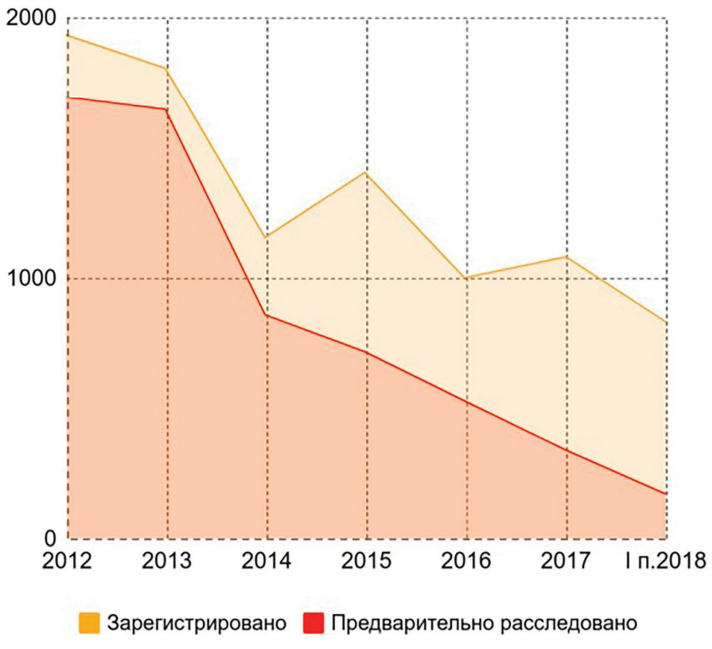

Рис. 7. Неправомерный доступ к компьютерной информации (ст. 272 УК РФ)
Источник: Статистика и аналитика // Министерство внутренних дел Российской Федерации. М., 2019. URL: https://www.Deljatel-nost/statistics (дата обращения: 17.11.2019).

которые распространяются в сети Интернет бесплатно. Киберпреступник «взламывает» лицензионные платные программы, игры с целью встроить в них свое вредоносное ПО, при этом, пользователь ничего не подозревает. По такой схеме работает ПО, которое незаконно использует чужие вычислительные системы без ведома владельцев компьютеров. Расширение сферы безналичных расчетов повлекло за собой возникновение своеобразной криминальной индустрии, необходимой для совершения несанкционированных операций по переводу денежных средств, в том числе с использованием платежных карт (рис. 9). Криминальные технологии постоянно совершенствуются, становясь доступными широкому кругу лиц, которые могут не обладать широкими познаниями в области информационных технологий [12].

Повышение доступности мошеннических схем и инструментов для их реализации ожидаемо влечет за собой рост числа незаконных транзакций. Так, в 2016 г. количество несанкционированных операций с использованием платежных карт выросло на 13,8 % (с 260 тыс. до 296 тыс.), а объем ущерба составил 1,08 млрд (1,15 млрд) р.[7] В подавляющем большинстве, несанкционированные операции производятся «посредством сети Интернет и мобильных устройств, в том числе интернет-банкинга». Чаще всего (в 93 % случаев) такие операции означают использование электронных средств платежа (ЭСП) без согласия клиента вследствие противоправных действий, потери, нарушения конфиденциальности аутентификационной информации.

[7] Отчет центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Департамента информационной безопасности Банка России 1.09.2017 — 31.08.2018 // Банк России : офиц. сайт. М., 2019. URL: https://www.cbr.ru/Content/Document/File/50959/survey_0917_0818.pdf (дата обращения: 14.11.2019).

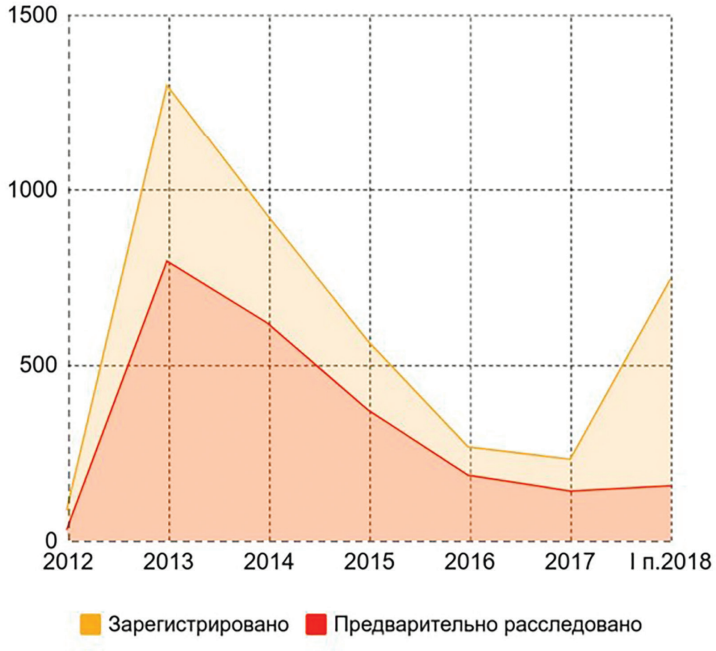

Рис. 8. Создание, использование и распространение вредоносных компьютерных программ

Источник: Статистика и аналитика // Министерство внутренних дел Российской Федерации. М., 2019. URL: https://www.Deljatel-nost/statistics (дата обращения: 17.11.2019).

Обеспечение экономической и информационной безопасности в условиях цифровой трансформации связано с рядом проблем. Быстро и активно развивающиеся информационные технологии, которые активно используются мошенниками и злоумышленниками, заставляют государство и хозяйствующих субъектов совершенствовать системы защиты и противодействия возможным угрозам и повышать уровень информационной безопасности в целом. Однако, на сегодняшний день, это происходит медленно, и нарушители все чаще находят все более новые и изощренные способы совершения своих преступлений, которые труднее обнаружить и выявить. Исходя из этого, разработка возможных мер противодействия таким угрозам и повышения информационной безопасности становится все сложнее [13].

Экономическую безопасность государства нельзя обособлять от экономической безопасности хозяйствующего субъекта и отдельной личности, их обязательно нужно рассматривать в совокупности. Это связано с тем, что состояние защищенности экономической системы в целом определяется по самому слабо защищенному звену. Таким звеном в экономической безопасности государства является отдельный человек, и пока его безопасность будет на низком уровне, всегда будут иметь место вызовы и угрозы безопасности страны в целом.

Растущая информатизация экономических процессов требует повышения уровня ее безопасности. В настоящее время практически у каждого человека есть компьютер, смартфон, имеющий выход в интернет. У каждого есть счет в банке, банковская карта и, чаще всего, есть мобильное приложение этого банка — это удобно, быстро и главное — без больших потерь времени, нервов и

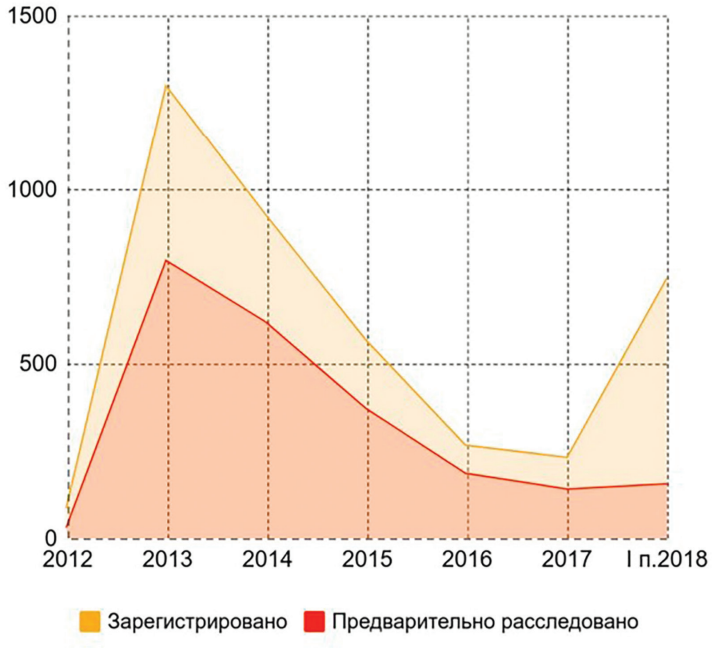

Рис. 9. Мошенничество с использованием электронных средств платежа
Источник: Статистика и аналитика // Министерство внутренних дел Российской Федерации. М., 2019. URL: https://www.Deljatel-nost/statistics (дата обращения : 17.11.2019).

сил на походы непосредственно в банк. Это понимают и мошенники, желающие обогатиться за чужой счет преступным путем. Они различными путями «взламывают» личные кабинеты пользователей мобильных приложений банков, получают несанкционированный доступ к денежным средствам, персональным данным клиентов банков и реализуют свои злоумышленные цели. Но многие банки, крупные компании все чаще вводят новые способы защиты и повышения безопасности личных данных и электронных счетов своих клиентов. Это касается не только банков, но и других экономических субъектов рынка, которые, так или иначе, работают с информационными и компьютерными технологиями в процессе своей экономической деятельности.

Распространение социальной инженерии способствует возможностям преступника получить несанкционированный доступ к персональным данным граждан и использовать их в своих корыстных целях. На сегодняшний день не составляет труда приобрести базы данных с номерами телефонов, ФИО, паспортными данными граждан на различных интернет-сайтах, телеграм-каналах. Несмотря на то, что в Российской Федерации есть закон «О персональных данных», нарушение которого предусматривает уголовную и административную ответственность, количество совершаемых противозаконных деяний не снижается. Нарушители эффективно маскируются — этому способствует отсутствие прямого физического контакта нарушителя и потенциальной жертвы.

В целях повышения информационной безопасности в условиях цифровой экономики, а, следовательно, и экономической безопасности страны, организации и человека в частности, можно предложить следующие меры:

1. Эффективное выполнение задач и мероприятий, предусмотренных стратегией развития информационного общества в РФ на 2017–2030 гг. и доктриной информационной безопасности РФ.

2. Повышение информированности населения о возможных угрозах в сфере цифровых технологий, о способах и видах мошенничества, в результате которых люди могут потерять свои деньги, о том, как избежать этого мошенничества, как повысить безопасность своих сбережений и персональных данных, которые являются целью злоумышленников.

3. Совершенствование нормативно-правовой базы в сфере обеспечения информационной безопасности, возможное ужесточение наказаний за совершение преступлений против экономической и информационной безопасности людей и страны. Также очень важно разработать новые правовые нормы в отношении определенных случаев мошенничества, не охваченных существующими законами.

4. В современных условиях цифровой экономики каждая организация должна регулярно оценивать уровень своей информационной безопасности, осуществлять постоянный и всесторонний анализ возможных угроз и последствий от их реализации. Важными для организации должны быть вопросы о том, созданы ли условия для внедрения современных цифровых технологий по защите информации, эффективно ли осуществляется менеджмент в сфере обеспечения информационной безопасности, насколько рационально распределены финансовые ресурсы между кадровым обеспечением организации и цифровыми технологиями, направленными на защиту данных и т.п.

5. Усиление работы по блокировке сайтов, рассылок и call-центров мошеннических структур.

6. Построение взаимодействия с операторами не только мобильной связи и телеком-провайдерами, но и ip-телефонии и мессенджеров, а также повышение взаимодействия с профильными государственными органами [6].

7. Составление банками и финансовыми организациями «белого списка» разрешенных к запуску программ на банкоматах. Программы не из этого списка не смогут быть запущены на банкоматах, следовательно, преступники не смогут внедрять вредоносное ПО в операционные системы банкоматов.

Список использованной литературы

1. Ярочкин В.И. Информационная безопасность / В.И. Ярочкин. — Москва : Гаудеамус, 2014. — 802 с.

2. Коротков Э.М. Управление экономической безопасностью общества / Э.М. Коротков, А.А. Беляев // Менеджмент в России и за рубежом. — 2001. — № 6. — С. 9–25.

3. Гафнер В.В. Информационная безопасность : учеб. пособие / В.В. Гафнер. — Ростов-на-Дону : Феникс, 2010. — 324 с.

4. Жмуров Д.В. Эра милосердия. Пути развития преступности / Д.В. Жмуров, А.А. Протасевич, А.С. Костромина. — DOI 10.17150/2411-6262.2019.10(2) // Baikal Research Journal. — 2019. — Т. 10, № 2. — URL: http://brj-bguep.ru/reader/article.aspx?id=23010.

5. Блокчейн в цифровой криминологии: постановка проблемы / А.П. Суходолов, Е.А. Антонян, М.В. Рукинов [и др.]. — DOI 10.17150/2500-4255.2019.13(4).555-563 // Всероссийский криминологический журнал. — 2019. — Т. 13, № 4. — С. 555–563.

6. Булай Ю.Г. Профилактика и противодействие киберпреступности, а также международным киберугрозам / Ю.Г. Булай, Р.И. Булай // Академическая мысль. — 2017. — № 1. — С. 31–35.

7. Лагутин П.Д. Киберпреступность как актуальная угроза обществу / П.Д. Лагутин, Т.А. Миханова // Молодой ученый. — 2018. — № 42 (228). — С. 108–109.

8. Карпова Д.Н. Киберпреступность: глобальная проблема и ее решение / Д.Н. Карпова // Власть. — 2014. — № 8. — С. 46–50.

9. Котова Н.Н. Информационное обеспечение экономической безопасности бизнеса / Н.Н. Котова, В.В. Борчанинов // Вестник Южно-Уральского государственного университета. Серия: Экономика и менеджмент. — 2017. — Т. 11, № 1. — С. 20–27.

10. Овтин В.В. Особенности неправомерного доступа к компьютерной информации по статье 272 УК РФ: ответственность и наказание / В.В. Овтин, В.В. Гудырев // Студенческий. — 2018. — № 8-4 (28). — С. 69–72.

11. Ларина Л.Ю. Уголовная ответственность за неправомерное воздействие на критическую информационную инфраструктуру России / Л.Ю. Ларина // Актуальные вопросы борьбы с преступлениями. — 2017. — № 3. — С. 22–25.

12. Гольтяпина И.Ю. Система информационного законодательства: вопросы теории / И.Ю. Гольтяпина // Проблемы права. — 2014. — № 3 (46). — С. 95–99.

13. Никонов А.И. Системы защиты информации и их место в политике безопасности / А.И. Никонов, Н.О. Павлов // Вестник НГИЭИ. — 2016. — № 8 (63). — С. 48–54.

References

1. Yarochkin V.I. *Informatsionnaya bezopasnost'* [Information Security]. Moscow, Gaudeamus Publ., 2014. 802 p.

2. Korotkov E.M., Belyaev A.A. Managing the Company's Economic Security. *Menedzhment v Rossii i za rubezhom = Management in Russia and Abroad,* 2001, no. 6, pp. 9–25. (In Russian).

3. Gafner V.V. *Informatsionnaya bezopasnost'* [Information Security]. Rostov-on-Don, Feniks Publ., 2010. 324 p.

4. Zhmurov D.V., Protasevich A.A., Kostromina A.S. The Era of Mercy. Ways of Criminality Development. *Baikal Research Journal*, 2019, vol. 10, no. 2. DOI: 10.17150/2411-6262.2019.10(2).18. Available at: http://brj-bguep.ru/reader/article.aspx?id=23010. (In Russian).

5. Sukhodolov A.P., Antonyan E.A., Rukinov M.V., Shamrin M.Yu., Spasennikova M.G. Blockchain in Digital Criminology: Problem Statement. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2019, vol. 13, no. 4, pp. 555–563. DOI: 10.17150/2500-4255.2019.13(4).555-563. (In Russian).

6. Bulai Yu.G., Bulai R.I. Cybercrime as Well as International Cyber Threats and Their Solution. *Akademicheskaya mysl' = Academic Thought,* 2017, no. 1, pp. 31–35. (In Russian).

7. Lagutin P.D., Mikhanova T.A. Cybercrime as an Actual Threat to Society. *Molodoi uchenyi = Young Scientist,* 2018, no. 42 (228), pp. 108–109. (In Russian).

8. Karpova D.N. Cybercrime: a Global Challenge and its Solution. *Vlast' = Power,* 2014, no. 8, pp. 46–50. (In Russian).

9. Kotova N.N., Borchaninov V.V. The Information Support for the Economic Security of Business. *Vestnik Yuzhno-Ural'skogo gosudarstvennogo universiteta. Seriya: Ekonomika i menedzhment = Bulletin of South Ural State University. Series: Economics and Management,* 2017, vol. 11, no. 1, pp. 20–27. (In Russian).

10. Ovtin V.V., Gudyrev V.V. Features of Illegal Access to Computer Information Under Article 272 of the Criminal Code of the Russian Federation: Responsibility and Punishment. *Studencheskii = Student,* 2018, no. 8-4 (28), pp. 69–72. (In Russian).

11. Larina L.Yu. Criminal Liability for Unlawful Interference Critical Information Infrastructure the Russian Federation. *Aktual'nye voprosy bor'by s prestupleniyami = Actual Issues of Fight Against Crimes*, 2017, no. 3, pp. 22–25. (In Russian).

12. Goltyapina I.Yu. SyStem of InformatIon LegISLatIon: Issues of Theory. *Problemy prava = Issues of Law,* 2014, no. 3 (46), pp. 95–99. (In Russian).

13. Nikonov A.I., Pavlov N.O. Systems of Information Security and their Place in the Security Policy. *Vestnik NGIEI = Bulletin NGIEI,* 2016, no. 8 (63), pp. 48–54. (In Russian).

Информация об авторах

Бушуев Алексей Леонидович — студент, Байкальский государственный университет, Российская Федерация, г. Иркутск, e-mail: a.l.98bushuev@mail.ru.

Деревцова Ирина Валерьевна — кандидат экономических наук, доцент, кафедра мировой экономики и экономической безопасности, Байкальский государственный университет, Российская Федерация, г. Иркутск, e-mail: derevczovai@mail.ru.

Мальцева Юлия Алексеевна — студент, Байкальский государственный университет, Российская Федерация, г. Иркутск, e-mail: maltseva.iuliya@gmail.com.

Терентьева Виктория Дмитриевна — студент, Байкальский государственный университет, Российская Федерация, г. Иркутск, e-mail: tervik@bk.ru.

Authors

Aleksey L. Bushuyev — Undergraduate Student, Baikal State University, Irkutsk, Russian Federation, e-mail: a.l.98bushuev@mail.ru.

Irina V. Derevtsova — PhD in Economics, Associate Professor, Chair of World Economy and Economic Security, Baikal State University, Irkutsk, Russian Federation, e-mail: derevczovai@mail.ru.

Yulia A. Maltseva — Undergraduate Student, Baikal State University, Irkutsk, Russian Federation, e-mail: maltseva.iuliya@gmail.com.

Viktoriya D. Terentyeva — Undergraduate Student, Baikal State University, Irkutsk, Russian Federation, e-mail: tervik@bk.ru.

Для цитирования

Роль информационной безопасности в условиях цифровой экономики / А.Л. Бушуев, И.В. Деревцова, Ю.А. Мальцева, В.Д. Терентьева. — DOI: 10.17150/2411-6262.20.11(1).6 // Baikal Research Journal. — 2020. — Т. 11, № 1.

For Citation

Bushuyev A.L., Derevtsova I.V., Maltseva Yu.A., Terentyeva V.D. Role of Information Security in Terms of Digital Economy. *Baikal Research Journal*, 2020, vol. 11, no. 1. DOI: 10.17150/2411-6262.20.11(1).6. (In Russian).