УДК 338

Иванова Татьяна Александровна

Российская академия народного хозяйства и государственной службы при Президенте РФ, г. Санкт-Петербург

t.ivanova04@mail.ru

АНАЛИЗ УГРОЗ БЕЗОПАСНОСТИ ЦИФРОВОЙ ЭКОНОМИКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация: Цель статьи – выявить основные угрозы и вызовы цифровой экономики Российской Федерации. В частности, будет исследована безопасность цифровой экономики Российской Федерации и существующие угрозы, а именно: мошенничество, киберпреступность, нехватка IT-специалистов, недостаточные темпы развития и проблемы, связанные с государственным регулированием Цифровой экономики Российской Федерации.

Ключевые слова: цифровая экономика, цифровизация, угрозы, риски, киберпреступность, мошенничество.

Ivanova T.A.

Russian Presidential Academy of National Economy and Public Administration

North-West Institute of Management

ANALYSIS OF SECURITY THREATS TO THE DIGITAL ECONOMY OF THE RUSSIAN FEDERATION

Abstract: The purpose of the article is to identify the main threats and challenges of the digital economy of the Russian Federation. In particular, the security of the digital economy of the Russian Federation and existing threats will be investigated, namely: fraud, cybercrime, lack of IT specialists, insufficient development rates and problems related to state regulation of the Digital economy of the Russian Federation.

Keywords: digital economy, digitalization, threats, risks, cybercrime, fraud.

Цифровизация экономики предполагает рост новых угроз и рисков, связанных с программным обеспечением, интеллектуальной собственностью, утечкой данных и прочими вопросами информационной безопасности в

киберсреде.

1) Самой значимой проблемой в сфере цифровой экономики является новый вид мошенничества – киберпреступность.

Число атак увеличивается с каждым годом. Путем создания вирусов, различными мошенническими действиями, звонками, спамом, взломами, киберпреступники завладевают информацией и конфиденциальными данными.

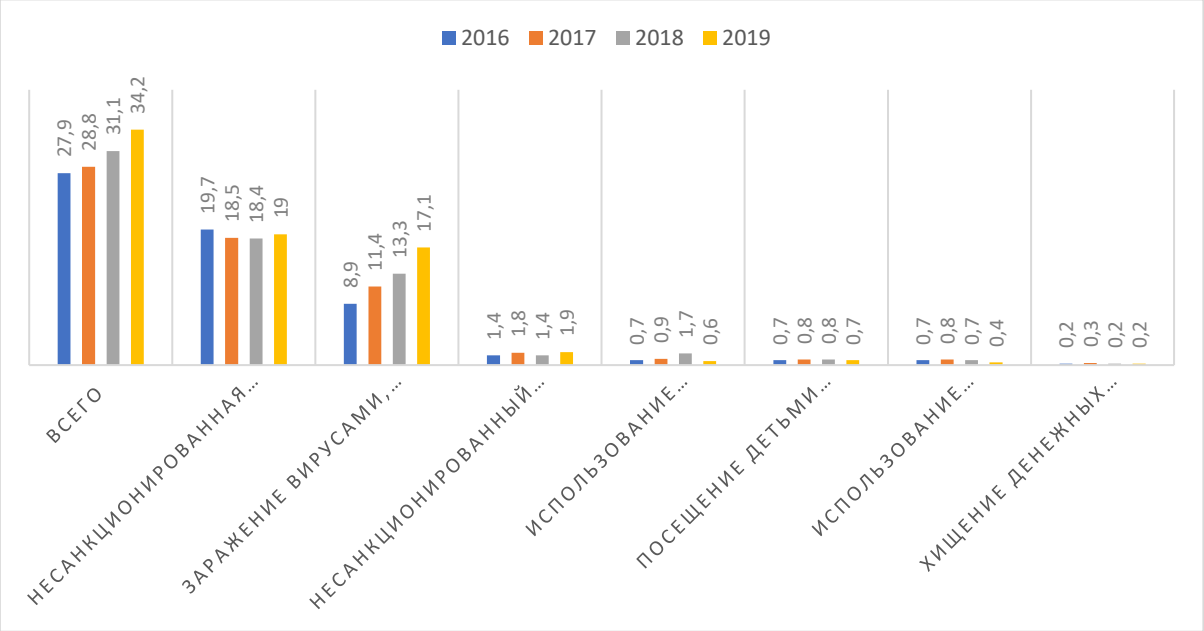

Рис. 1 – столкновение населения с угрозами информационной безопасности при использовании интернета [3]

Субъектами данной угрозы являются вирусы-шифровальщики, например, cryptolocker, проникающие не только в личные компьютеры, но и в сети стратегических объектов, космодромов, АЭС, аэропортов, нефтепроводов, оборонных предприятий, крупных заводов, способные вызвать техногенные катастрофы. Потери и ущерб от таких проникновений исчисляются сотнями миллионов долларов. Объектами угроз являются личность, организации, общество и государство, а предметом является цифровая среда экономики. Основным мотивом кибератак выступают получение данных и финансовая выгода. [1]

По данным Росстата в России, киберпреступность выросла в 30 раз за

последние 3 года. В 2019 году было зафиксировано более 1600 атак, что превышает показатели прошлого года на 19%. Под основной удар попадают Государственные учреждения (241 атака), промышленность (125), финансовые отрасли (92), а также, медицинские учреждения (93). [2] Самыми распространенными угрозами в России являются несанкционированная рассылка (49, 25% от общего числа угроз) и заражение вирусами через интернет, ведущих к потере и удалению информации с устройства (22,25 % от общего числа угроз). На третьем месте идет несанкционированный доступ к компьютеру (3,5 %), далее – использование электронной почты (1,75 %). На последнем месте стоит хищение денежных средств и персональных данных (0,75 %). [4]

В список самых распространённых киберугроз входят:

– утечка конфиденциальной информации пользователей сети Интернет и смартфонов;

– использование организациями бесплатных неоригинальных ПО и антивирусных программ. «Пиратские» версии обладают низким уровнем защищенности системы, низкой производительностью, а также, могут содержать вредоносные программы (вирусы) и использовать ПК как часть бот-сети для рассылки спама, подбора паролей или DDoS-атаки.

В 2019 году число заражений вредоносным ПО выросло на 38% по сравнению с 2018 годом. В 41% случаев заражения вредоносным ПО сочетались с методами социальной инженерии; [4]

– хищение мошенниками денежных средств у клиентов банков, кражи электронных кошельков и паролей, взломы личных и бизнес аккаунтов, путем звонков из банков или созданием поддельных платежных систем, терминалов.

По данным ЦБ РФ мошенники воздействуют на клиентов банков обманным путем, побуждая их к самостоятельному проведению переводов.

– создание фальшивых доменов известных фирм и брендов;

– атаки на публичные размещения акций компаний в блокчейн-пространстве, кража активов и ликвидация платформ. В атаках на юридические

лица злоумышленников больше всего интересуют персональные данные.

По данным Group-IB, за последние три года количество киберинцидентов в России увеличилось на 72 %, а ущерб от них возрос на 200 %; [5]

– распространение вируссодержащих сайтов или программ, путем реклам на сайтах или спам-сообщений по почте или СМС.

В феврале 2020 года специалистами центра расследования киберинцидентов JSOC CERT был обнаружен рост незаметных кибератак на банки и энергетику РФ, которые похожи на поведение хакерской группировки Silence. [6]

Все вышеперечисленные угрозы относятся к области киберпреступности и вызывают недоверие у людей к цифровой среде.

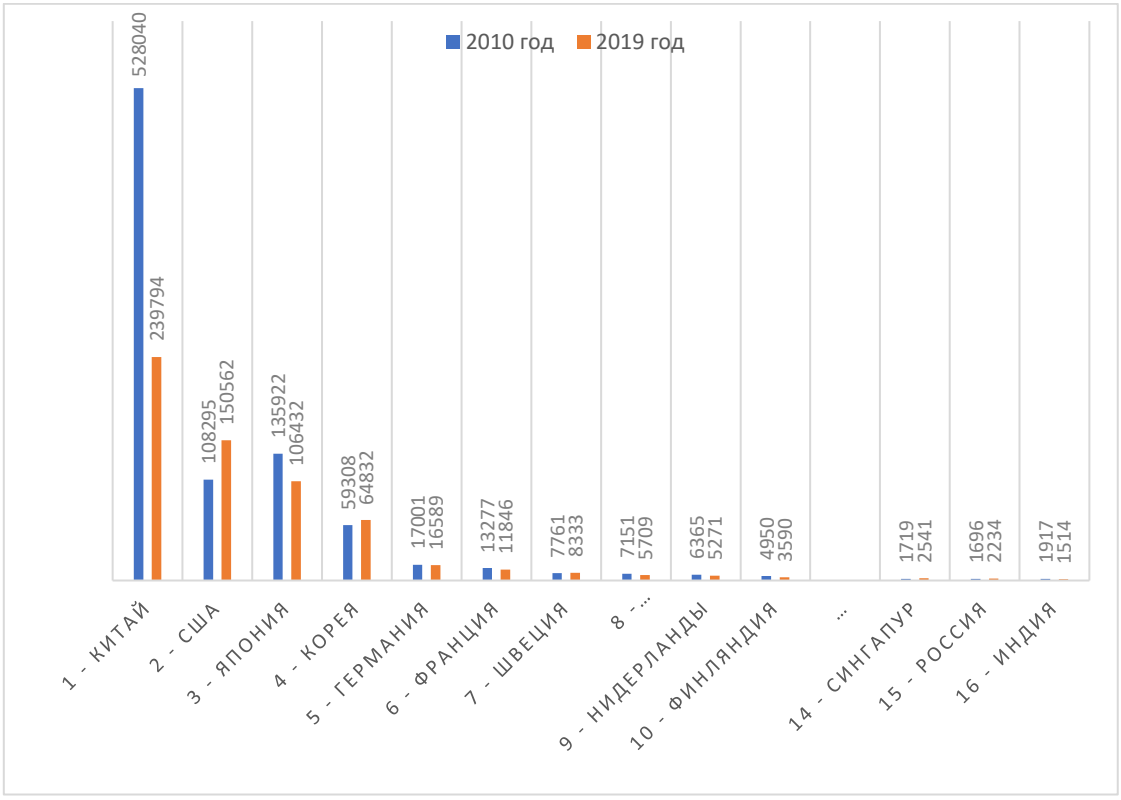

Рис. 2 – Патентные заявки на изобретения в области ИКТ по стране заявителя, 2020 г. [8]

2) Еще одной угрозой для цифровой экономики России является недостаточная подготовка IT-специалистов. По прогнозам ФРИИ (Фонд развития интернет-инициатив), к 2027 году российская экономика будет

нуждаться примерно в 1,5 млн IT-специалистах. Фонд развития интернет инициатив подсчитал, что к 2028 году, в России будет не хватать примерно 2 миллиона IT-профессионалов. [7]

Во избежание нехватки рабочей силы, необходимо повысить выпуск IT-специалистов на 40 тысяч в год и каждые полгода обеспечивать прохождение курсов повышения квалификации.

3) Недостаточные темпы развития так же следует отнести к угрозам цифровой экономики.

Россия занимает 15 место в мире по патентам на изобретения. По сравнению с лидирующим Китаем (239 794 ед.), у России - 2 234 (в 107 раз меньше). Также, стоит отметить, что по сравнению с 2010 годом, количество возросло всего на 515, что является незначительным показателем.

Сейчас по уровню цифровизации сильнее всего от стран ЕС отстают важнейшие для России отрасли – добывающая, обрабатывающая промышленность и транспорт.

Российское законодательство часто сталкивается с такой проблемой, что при отставании нормативного законодательства от развития цифровой экономики и новых технологий, и сервисов, случается диссонанс, когда компании, занимающиеся разработками новых технологий, тестируя свои объекты, рискуют нарушить действующие законы. Но для устранения данной проблемы в России на данный период времени вводится правовой механизм «регулятивные песочницы», суть которого заключается в том, что разработчики получают разрешение на безопасное тестирование своих программ.

4) Последней проблемой выступает недостаточная поддержка государством отечественных компаний, многие российские компании зависят от зарубежных разработок.

Правительство проводит такую политику, риск которой заключается в заполнении российского цифрового рынка иностранными товарами и услугами. А с данной ситуацией Россия уже не раз сталкивалась.

То есть государству важно поддерживать отечественное производство и

облегчать законы, а также делать некоторые льготы.

Рекомендации, направленные на нейтрализацию угроз и рисков цифровой экономики Российской Федерации:

1) В рамках первой угрозы необходимо:

– покупать и использовать только лицензионные ПО, программы, приложения, антивирусные программы Security Kaspersky, DrWeb, Nod32 и специализированные сервисы анти-DDoS.

– установить спам и фишинг-фильтры, сетевые экраны и Брандмауэры

– усилить системы аутентификации и паролей:

– следует ограничить привилегированный доступ к информации

– повысить компьютерную грамотность у населения,

– тщательно подходить к выбору интернет-магазина, избегать поддельные фирмы;

– соответствовать стандарту PCI DSS «стандарт безопасности индустрии платёжных карт».

2) В рамках второй угрозы, необходимо повысить компетенции IT-специалистов в области информационной безопасности, а увеличить число кадров. Сделать это не так просто, так как это требует в общем развития инфраструктуры образования, подготовки новых преподавателей, стимулирования поступающих на высшее образование и повышения квалификации уже имеющихся специалистов.

3) В рамках 3 угрозы следует проработать, систему стимулирования на создание и развитие бизнеса, ориентированного на поднятие цифровой экономики (сниженные кредитные ставки, гарантии по банковским кредитам, субсидирование, пониженные процентные ставки по налогам и страхованию);

4) И в рамках последней проблемы, необходимо:

– законодательное ограничение на приобретение зарубежных ПО российскими государственными организациями;

– оказание государственной поддержки (например, компенсации за

патентование) таких крупных компаний на рынке цифровой экономики, как Security Kaspersky, Abbey, Yandex и других;

– дополнительное финансирование программ кибербразведки платформы Cyber Threat Intelligence, таких как Group-IB, PT Cybersecurity Intelligence и R-Vision;

– запуск новых продуктов и программ страхования от киберугроз.

Также, решением проблемы является выполнение программы цифровой экономики. В 2017 году Российское правительство своим распоряжением от 28 июля 2017 г. № 1632-р запустило программу «Цифровая экономика 2024». Программа распланирована на 13 лет вперед в целях реализации стратегии развития цифровой экономики РФ. В основе программы лежит повышение благосостояния и качества жизни народа. Данную цель планируется достичь к 2030 году путем повышения цифровой грамотности населения, повышения доступности и качества предоставляемых товаров и услуг, производимых цифровой экономикой, а также, повышения качества и упрощения предоставляемых государством услуг. [9]

Для реализации программы необходимо не только государственное вмешательство, также необходимо взаимодействие бизнеса и науки. Программа направлена на обеспечение безопасности как внутри страны, так и за ее пределами, на защиту платежных систем от кибер-атак, на развитие антивирусных сервисов и дополнительное финансирование программ кибербразведки платформы Cyber Threat Intelligence, таких как Group-IB, PT Cybersecurity Intelligence и R-Vision по поиску киберпреступников и уничтожению преступного бизнеса.

К сожалению, все вышеперечисленные меры нельзя выполнить быстро и только за счёт субсидирования. Помимо государственных ресурсов, требуется такие ресурсы как СМИ, временный ресурс и человеческий фактор. Также, важно отметить, что меры должны осуществляться в совокупности, их должны соблюдать все коммерческие и государственные организации.

Итак, проведя анализ угроз и безопасности Российской цифровой

экономики, можно сделать вывод о том, что с каждым годом темпы развития растут в данной области, что очень важно для безопасности, но к сожалению, растет уязвимость цифровой экономики и увеличивается число кибер-преступлений.

Помимо государственных ресурсов, требуются такие ресурсы как СМИ, временный ресурс и человеческий фактор.

Недостаточное внимание к цифровой экономике может послужить причиной значительного экономического отставания. Устранение угроз и рисков цифровой экономики, обеспечение безопасности информационной среды стало сегодня основой конкурентоспособности человека, бизнеса и государства.

Список литературы

1. Экономическая безопасность: Учебник и практикум / Кузнецова Е.И. — М.: Издательство Юрайт, 2018.

2. Россия – расчеты Института статистических исследований и экономики знаний НИУ ВШЭ по данным Росстата; зарубежные страны – ОЭСР, Евростат. URL: https://issek.hse.ru/ . (Дата обращения 15.12.2020).

3. ИНДИКАТОРЫ ЦИФРОВОЙ ЭКОНОМИКИ: 2019 Статистический сборник Редактор М. Ю. Соколова Художник П. А. Шелегеда Компьютерный макет О. Г. Егин, В. Г. Паршина, В. В. Пучков.

4. Портал «Positive technologies» URL: https://www.ptsecurity.com/ru-ru/. (Дата обращения: 15.12.2020).

5. IB-Group - источник стратегических данных о развитии киберугроз на глобальном уровне. URL: https://www.group-ib.ru/resources/threat-research/2019-report.html. (Дата обращения: 15.12.2020).

6. SOLAR JSOC - Центр информационной безопасности. URL: https://rt-solar.ru/products/jsoc/services / (Дата обращения: 15.12.2020).

7. Фонд развития интернет – инициатив URL: https://www.iidf.ru/. (Дата обращения: 15.12.2020).

8. Министерство цифрового развития, связи и массовых коммуникаций

Российской Федерации URL: https://digital.gov.ru/ru/. (Дата обращения: 15.12.2020).

9. Программа «Цифровая экономика Российской Федерации» 28.07.2017. URL: http://government.ru/rugovclassifi er/ 614/events. (Дата обращения: 15.12.2020).

10. World Bank (2018). Russia Digital Economy Report: Competing in the Digital Age: Policy Implications for the Russian Federation. The World Bank, 2018.

11. URL: https://www.worldbank.org/en/country/russia/publication/competing-in-digital-age. (Дата обращения: 15.12.2020).

12. Беляков К. С. Цифровая экономика России: проблемы и перспективы // Информационное общество: состояние, проблемы, перспективы: Материалы V ежегодной Всероссийской научно-практической интернет-конференции. М.: Изд-во РЭУ им. Г.В. Плеханова, 2018. С. 61–67.