УДК 004.056

ЭКОНОМИЧЕСКАЯ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В УСЛОВИЯХ ЦИФРОВОЙ ЭКОНОМИКИ

Коды JEL: O14, L86, K32

Мамонтова С. В., *кандидат экономических наук, доцент кафедры экономики, управления и аудита, Юго-Западный государственный университет, г. Курск, Россия*
E-mail: efv05@mail.ru
SPIN-код: 6009-8715

Поступила в редакцию 25.11.2022. Принята к публикации 02.12.2022

Аннотация
Предмет. *Экономическая и информационная безопасность в условиях цифрой трансформации.*
Тема. *Институционально-инструментальное обеспечение мероприятий по предотвращению финансово-экономических преступлений, поиск механизмов обеспечения экономической и информационной безопасности.*
Цели. *Оценка динамики экономической и информационной безопасности в условиях цифровой трансформации экономической системы с целью предотвращения финансовых коррупционных проявлений и киберпреступности.*
Методология. *Анализ трудов ведущих специалистов и практиков, занимающихся разработкой и обеспечением информационной безопасности в сфере деятельности, ориентированной на цифровизацию различных систем. Использовались методы: сравнений, диалектический, статистико-экономический, логический.*
Результаты. *Проведённое исследование показало слабую защиту информации о персональных данных, низкий уровень компетенций сотрудников и корпоративной культуры, и их ответственности перед клиентами, результатом которых является рост киберпреступлений, фишинга, финансово-экономических преступлений. Предложены основные рекомендации защиты информации, от кибератак и других неправомочных действий.*
Область применения. *Сфера экономической и информационной безопасности.*
Выводы. *Важность темы исследования обусловлена изменениями, происходящими в сфере экономики на микро и макроуровне и, как следствие, непосредственно влияющими на деятельность компаний в условиях глобализации экономики и возрастающей конкуренции. Появляются новые виды вредоносного программного обеспечения, растет число атак с использованием шпионских программ, активизируются хакерские группировки. Возрастают действия фишинговых рассылок клиентам банков и усиливаются атаки, эксплуатирующие уязвимость программного обеспечения. Программы-шпионы позволяют получать удаленный доступ к информационным системам организаций. Таким образом, необходимо ориентироваться не только на повышение технического и информационного обеспечения, цифровых компетенций работников и руководителей, но и на совершенствование законодательной базы, интегрируя данный процесс.*

Ключевые слова: *экономическая безопасность, цифровая экономика, информационная безопасность, киберугрозы, кибератаки, коррупционные проявления, киберпреступность, финансово–экономические преступления.*

UDC 004.056

ECONOMIC AND INFORMATION SECURITY IN THE DIGITAL ECONOMY

JEL Codes: O14, L86, K32

Mamontova S. V., *Candidate of Economic Sciences, Associate Professor of the Department of Economics, Management and Audit, Southwest State University, Kursk, Russia*
E-mail:efv05@mail.ru
SPIN-код: 6009-8715

Annotation
Subject. *Economic and information security in the context of digital transformation.*
Topic. *Institutional and instrumental support of measures to prevent financial and economic crimes, search for mechanisms to ensure economic and information security.*
Purpose. *Assessment of the dynamics of economic and information security in the context of the digital transformation of the economic system in order to prevent financial corruption and cybercrime.*
Methodology. *Analysis of the works of leading specialists and practitioners in this field of activity engaged in the development and provision of information security oriented to digitalization of various systems. The methods used were: comparative, dialectical, statistical-economic, logical.*
Results. *The conducted research shows weak protection of information about personal data, a low level of competence of employees and individuals, a low level of corporate culture and responsibility to customers, the result of the above is an increase in cybercrimes, phishing, financial and economic crimes. The main recommendations for the protection of information, cyber-attacks and other unauthorized actions are proposed.*
Application area. *The sphere of economic and information security.*
Conclusions. *The importance of the research topic is due to the changes taking place in the field of economics at the micro and macro levels, and as a result directly affecting the activities of companies in the context of economic globalization and increasing competition. New types of malicious software are emerging, the number of attacks using spyware is growing, and hacker groups are becoming more active. Phishing mailings to bank customers and attacks exploiting software vulnerabilities are increasing. Spyware allows you to gain remote access to information systems of organizations. Thus, it is necessary to focus on not only improving technical and information support, digital competencies of employees and managers, but also improving the legislative framework by integrating this process.*
Keywords: *economic security, digital economy, information security, cyber threats, cyberattacks, corruption manifestations, cybercrime, financial and economic crimes.*

DOI: 10.22394/1997-4469-2022-59-4-145-153

Введение

Актуальность и цель исследования связанна с обострением коррупционных проявлений в сфере экономической и информационной безопасности, которые являются одними из ключевых факторов сдерживания экономического роста страны, бизнеса и развития здоровой конкуренции.

Представляя, угрозу национальной безопасности каждого государства, требуются разработки конкретных шагов в области минимизации последствий, рассматриваемой проблемы.

На состоявшемся 16 июня 2021 года в Женеве саммите, одним из основных вопросов в повестке дня стал вопрос, информационной безопасности, вопросы борьбы с киберпреступностью, а также вопросы экономического сотрудничества в данной сфере деятельности на международном и национальных уровнях.

Особую значимость заявленная тема исследования приобретает в условиях цифрой трансформации, когда происходит усиление различного рода информационных атак. Так в 2022 году рост кибератак и киберпреступлений в России на автоматизированные системы управления взлетело на 80 %, увеличилась динамика финансово-экономических преступлений. Сложившаяся ситуация требует институционально-инструментального обеспечения мероприятий по предотвращению финансово-экономических преступлений; поиска механизмов обеспечения экономической и информационной безопасности.

Происходящие сегодня процессы динамично развивающихся национальных экономик и глобализации мирового пространства напрямую связаны с экономической безопасностью страны.

Само понятие «Экономическая безопасность страны» отражает способность соответ-

ствующих политических, правовых и экономических институтов государства защищать интересы своих субъектов в рамках национальных хозяйственных традиций и ценностей. Экономическая безопасность служит гарантом защиты субъектов экономики и социальной защищенности каждого человека [1].

Обеспечивая гарантии независимости любого государства, условия стабильности и эффективной жизнедеятельности общества, достижения успеха. Это связано с тем, что одним из основных и фундаментальных направлений современного государства является экономическое. Так как экономика представляет собой одну из жизненно важных сторон деятельности общества, государства и личности, следовательно, понятие национальной безопасности будет пустым словом без оценки жизнеспособности экономики, её прочности при возможных внешних и внутренних угрозах. Исходя, из этого, обеспечение экономической и информационной безопасности государства считается не только актуальным, но первостепенным вопросом на сегодняшний день.

Экономическая и информационная безопасность в условиях цифрой экономики

Экономическую безопасность следует рассматривать, как основную качественную характеристику экономической системы, которая определяет её способность поддерживать положительные условия жизнедеятельности населения, устойчивое обеспечение ресурсами развития народного хозяйства, а также последовательную реализацию национально–государственных проектов.

Сегодня как никогда все государства, в том числе и Россия, перейдя на цифровой этап развития, используя IT-технологии, программные продукты столкнулись с совершенно новыми мошенническими схемами в области экономической безопасности. Соответственно на всех уровнях государственной политики, в системе стратегического управления одним из важнейших направлений устойчивого развития экономики является обеспечение экономической безопасности. Так в соответствии с Указом Президента Российской Федерации от 13 мая 2017 г. № 208 была утверждена «Стратегии обеспечения экономической безопасности Российской Федерации на период до 2030 года». В России первый закон по обеспечению экономической безопасности был принят еще в 1996 году. Следует отметить, что ключевая роль экономической безопасности также отведена в Стратегии национальной безопасности Российской Федерации до 2030 года [2].

Реализация стратегии проходит два этапа: на первом этапе осуществляется разработка и реализация мер организационного, нормативно-правового и методического характера в целях обеспечения экономической безопасности, совершенствование механизмов мониторинга и оценки её состояния; второй этап — выполнение мер по нейтрализации вызовов и угроз экономической безопасности [3].

В Российской Федерации выделяются три основных уровня безопасности, а именно безопасность личности, общества и государства. По направлениям на внешнюю и внутреннюю безопасность, государственную, военную, экономическую, продовольственную, экологическую безопасность и так далее. Её нельзя рассматривать односторонне, так как затрагивается способность власти создавать механизмы защиты и реализации национальных интересов развития отечественной экономики, поддержания социально-политической стабильности общества [4, с. 12].

Насколько подвержена экономика влиянию внешних факторов на её устойчивость, стабильность и положительное функционирование общественного воспроизводства, подрывающий достигнутый уровень жизни населения и тем самым вызывающий повышенную общественную напряженность в социуме, а также угрозу самому существованию государства» [5, с. 32].

Таким образом, экономическую безопасность следует рассматривать как качественную характеристику экономической системы, определяющую ее способность поддерживать нормальные условия жизнедеятельности населения, устойчиво формировать продовольственную безопасность, обеспечивать инновационное развитие производительных сил, а также системно и последовательно реализовывать национально–государственные интересы. В дополнение можно сказать, что экономическую безопасность следует рассматривать на основе интеграции экономической и юридической систем, способных быстро реагировать и действенно противостоять неправомерному воздействию на государственном, региональном, международном уровнях и каждого индивида в отдельности.

Преступления в экономической сфере являются частью корыстной преступности, которая напрямую воздействует на экономические отношения в обществе.

Эти преступления посягают на собственность и другие экономические интересы государства, отдельных групп граждан, то есть потребителей, партнеров, конкурентов, а также на порядок управления экономической деятельностью в целях извлечения наживы, зачастую в рамках и под прикрытием законной экономической деятельности [6, с. 69].

Сегодня, когда трансформируется вся система национальной экономики ситуация с экономическими и информационными преступлениями в современном обществе становится острее, а вопросы безопасности и защиты от угроз актуальнее.

Эксперты по безопасности информационных технологий на основе аналитических данных предполагают, что число успешных попыток свершить преступление в экономической и информационной отрасли в дальнейшем будут увеличиваться. Цели и мотивы киберпреступлений, представлены на рисунке 1.

Экономические и информационные преступления направлены финансовое мошенничество, их доля составляет 41,0 % и соответственно 42,0 % для получения различных данных, в том числе и персональных, которые в дальнейшем могут использоваться злоумышленниками, как средство получения прибыли, за счёт вымогательства или шантажа, с чем сегодня сталкивается общество.

Так от деятельности злоумышленников в прошедшем году пострадали различные отрасли и сферы экономики, представленные на рисунке 2.

В большей степени атакуемыми и пострадавшими отраслями стали госучреждения, промышленность, медицина, сфера образования и финансовая отрасль. На их долю приходится наибольшее число преступлений.

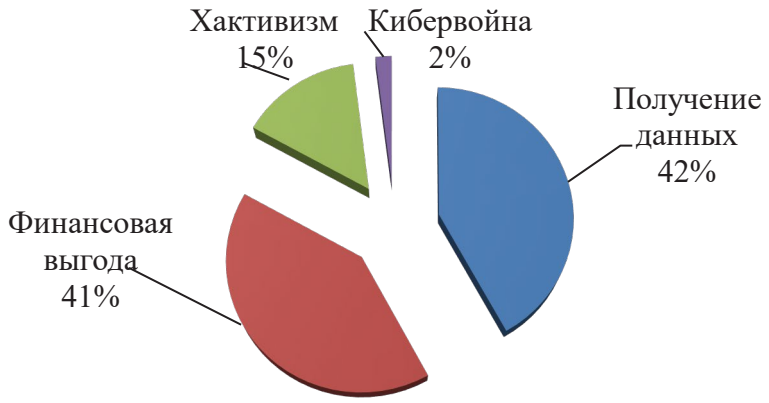

Рис. 1. Целевая и мотивационная составляющая интернет-преступлений

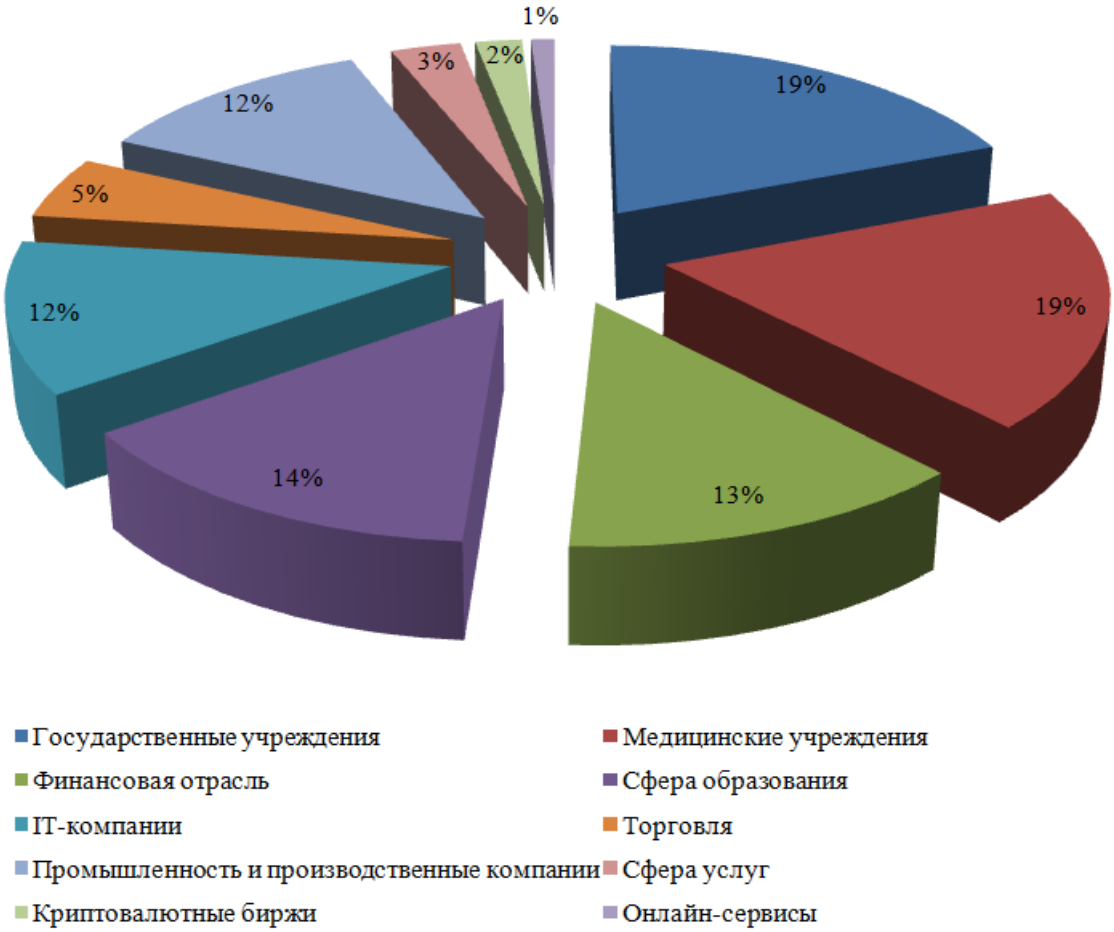

Рис. 2. Распределение сфер экономической деятельности, наиболее пострадавших от киберпреступлений

В результате проведенного опроса среди руководителей компаний разных стран, который показал, что за последние годы, столкнулись с экономическими преступлениями 66 % респондентов.

Однако уровень экономической преступности в России остается выше, чем средний общемировой результат. Кроме этого, уровень экономической преступности в РФ выше на 30 пунктов по сравнению со странами «большой семерки развивающихся стран» и на 26 пунктов со странами Восточной Европы (рисунок 3) [7].

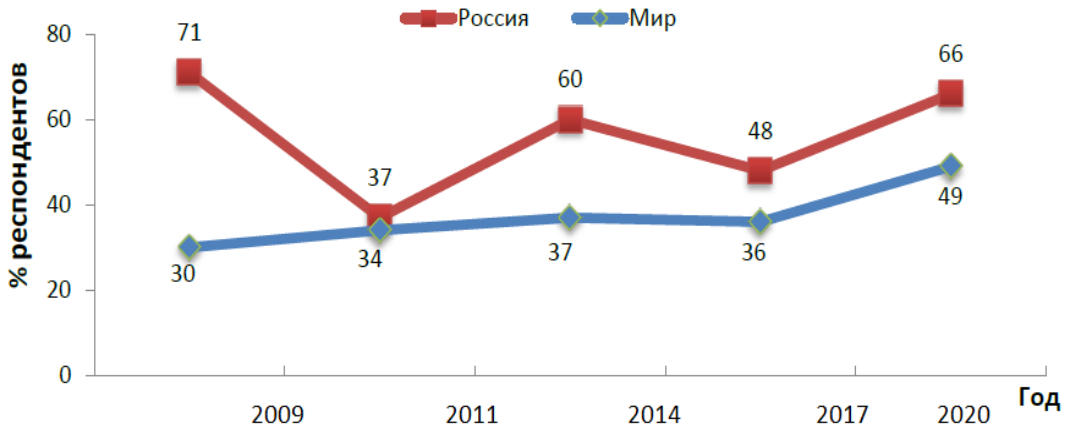

Рис. 3. Уровень экономической преступности, %

Размер ущерба является одним из ключевых вопросов, возникающих в случае совершения экономического преступления (рисунок 4). Так 41 % российских компаний сообщили о том, что они стали жертвами экономических преступлений, вследствие которых они понесли прямые финансовые потери в размере менее 100 тыс. долларов США, что ниже мировых показателей (45 %).

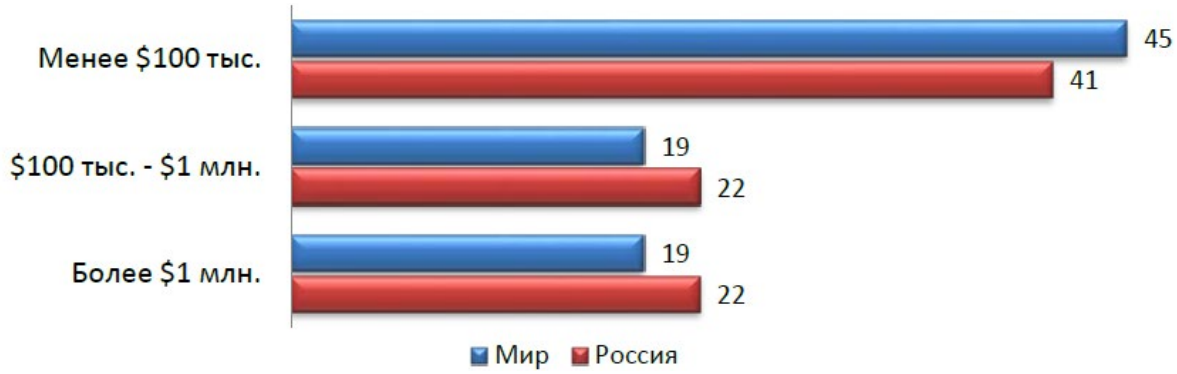

Рис. 4. Финансовые убытки, понесенные в результате экономических преступлений [7]

В то же время 22 % респондентов из России в результате преступлений в сфере экономики понесли потери более 1 млн долларов США, в то время как по всему миру такой же ущерб составил 19 %. Это свидетельствует о том, что ущерб от преступлений по-прежнему велик.

На сегодняшний день существует два основных вида угроз, которым могут подвергаться пользователи сети: технические и социальная инженерия. Техническая инженерия представляет из себя, как правило, работу различных вредоносных программ, а социальная инженерия — это в первую очередь фишинг — атаки, попрошайничество; фиктивные интернет-магазины; фиктивная работа на дому; фиктивные платежные системы; мошенничество в социальных сетях и электронной почте, и другие [8, с. 98].

Увеличивается число кибератак на корпоративные сети так, компания CPR (Check Point Research) проводя исследования, зафиксировала их рост на 50 % в неделю по сравнению с 2020 годом. Исследователи отметили, что пик атак был в декабре 2021 года (925 нападений на организацию в неделю) — можно предположить, что это произошло из-за эксплуатации Log4J (рисунок 5).

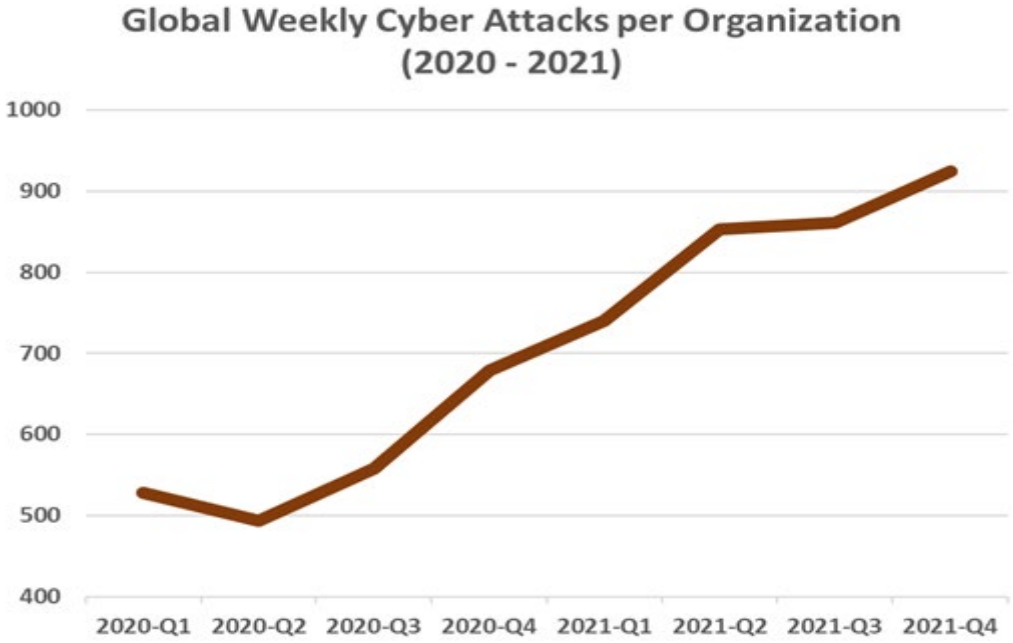

Рис. 5. Глобальный еженедельник кибератак на организации [9]

Самыми желанными для хакеров были организации Африки, Азиатско-Тихоокеанского региона и Латинской Америки, ну а самый высокий процент кибератак в 2021 году по сравнению с 2020 годом наблюдается в Европе. А самым атакуемым в мире является сектор образования и исследований.

Так рост атак на долю организации в сфере образования и исследований в 2021 году составил 75 %; организации из государственной и оборонной сферы на 47 %; организации из сферы коммуникаций на 51 %; ИТ сервис-провайдеры на 67 %; организации из сферы здравоохранения на 71 %.

Наиболее вероятная причина роста фишинговых атак связана с введением ограничительных мер в условиях пандемии COVID-19, именно в этот период стали активно использовать дистанционный способ оплаты товаров и услуг в интернет магазинах. Злоумышленники приспособили свои цели и инструменты к изменениям, вызванным пандемией, таким как переход на удаленную работу и рост популярности онлайн-шопинга.

Ежегодные исследования, проводимые лабораторией Касперского, выявили компании, отдельных пользователей, не стали исключением и финансовые учреждения, которые были подвержены киберугрозам. Киберпреступники продолжили активно использовать инструменты и методы, освоенные в начале пандемии. Остались актуальными риски, связанные с режимами удаленной и гибридной работы, а экономические проблемы, вызванные пандемией, еще больше усугубили ситуацию. Бедность и безработица привели к усилению вредоносной активности против банков и их клиентов. Кроме вредоносных вирусных программ, преступники разработали фишинговые, это веб-страницы, имитирующие сайты известных организаций, и электронные письма, рассылаемые от их имени — с помощью которых мошенники выманивают у потенциальных жертв конфиденциальную информацию. В результате были получены следующие данные: в 2021 году от фишинговых атак пострадали 8,2 % пользователей;

— доля мошеннических операций в сфере электронной коммерции и инцидентов, связанных с онлайн-банкингом составила 17,6 % и 11,1 % соответственно;

— жертвы PayPal, которые пытались перейти по ссылке на страницу, имитирующую сайт этой платежной системы, составили 37,8 % от всех фишинговых атак;

— система Visa, которая долгое время лидировала в этой категории, осталась на четвертом месте, её доля составили 9,4 % от общего числа.

Динамика вредоносного ПО для персональных компьютеров следующая:

— пользователи ПК, атакованные банковскими троянцами, сократилось на 35 % — с 625 364 человек в 2020 году до 405 985 в 2021 году;

— самым распространенным банковским зловредом остается Zbot (20,5 %), за ним идут SpyEye (12,2 %), который в последнее время значительно укрепил свои позиции, и CliptoShuffler (10,2 %);

— доля угроз, затрагивающих корпоративных пользователей, выросла почти на два процентных пункта — до 37,8 %. При этом количество атак на сектор банковского обслуживания физических лиц осталось прежним — 62,2 %.

Вредоносное ПО мобильных устройств имеет следующую тенденцию: число пользователей устройств на базе Android, пострадавших от банковского вредоносного ПО, сократилось на 50 % — с 294 158 человек в 2020 году до 147 316 в 2021 году [10].

Хотелось бы отметить, что программы — шпионы позволяют получать удаленный доступ к информационным системам организаций. Это дает основания прогнозировать отложенный эффект в виде роста хищений и в дальнейшем, это касается и владельцев криптовалют, т. к. на сегодня они являются приманкой для мошенников.

Рассмотрев данные полученной информации, возникает вопрос, как защититься от нападок и угроз кибермошенников.

В целях противодействия преступлениям совершаемым в интернет–пространстве в нашей стране, актуальны следующие меры с точки зрения закона и порядка:

1. Необходимо организовать подразделения по борьбе с киберпреступностью, включающие в себя следственные и оперативные группы, функционирующие круглосуточно, согласно рекомендациям Европейской конвенции о киберпреступности (обеспечивается специализация борьбы, непосредственность и непрерывность процесса раскрытия и расследования преступлений).

Введение в следственные подразделения органов уголовного преследования групп, специализирующихся на противодействии киберпреступлениям, обеспечит квалифицированное расследование преступлений данной категории.

2. Необходимо пересмотреть и ввести особую систему подбора кадров в правоохранительных и специальных органах, а также экспертных подразделениях (оперативные сотрудники с техническим образованием). Полагаем возможным использовать положительный опыт зарубежных стран, привлекающих на должности оперативных работников и специалистов лиц, имеющих, как правило, техническое образование, с прохождением курсов юридической подготовки. На первоначальном этапе такое требование возможно установить к оперативным работникам.

3. Методическое обеспечение расследования. Активное использование методов имитации преступной деятельности и внедрения сотрудников правоохранительных органов, а также инициирование создания единой правовой платформы на территории стран постсоветского пространства, содержащей опыт расследования киберпреступлений, сведения о преступниках, блокированных сайтах и т. д.

4. Надлежащее международное правовое сотрудничество.

Кроме того, механизм обеспечения экономической и информационной безопасности должен быть органично встроен в систему управления предприятием и способствовать достижению его основных целей. Данный механизм представляет собой систему средств и методов воздействия на процесс разработки управленческих решений, направленных на минимизацию негативного воздействия угроз экономической безопасности и обеспечения конкурентного развития предприятия [11, с. 188].

Механизм обеспечения экономической безопасности предприятий традиционно включает четыре подсистемы:

1) подсистема инструментов обеспечения экономической безопасности, включающая методики оценки рисков и идентификации угроз, методы прогнозирования уровня экономической безопасности;

2) подсистема показателей и индикаторов уровня экономической безопасности, включающая пороговые значения и периодичность оценки рисков;

3) подсистема регулирования уровня экономической безопасности предприятия, включающая методы распределения ресурсов, стимулы и санкции, использование резервов;

4) обеспечивающая подсистема, включающая кадровую, нормативно–правовую, информационную и управленческую системы.

В условиях цифровизации предприятий самым значительным трансформациям подвергается обеспечивающая подсистема. Первостепенная задача состоит в определении уровня цифровизации системы экономической безопасности предприятия, глубины проникновения цифровых технологий в деятельность по управлению рисками, что служит основой для определения перечня рисков и угроз экономической безопасности и характера их проявления.

Практики, занимающиеся программным обеспечением, в нашем исследовании взята «Лаборатория Касперского», где специалисты дают следующие рекомендации:

Устанавливайте приложения только из надежных источников.

Прежде чем предоставить приложению запрошенные права и разрешения, убедитесь, что они ему действительно необходимы.

Никогда не переходите по ссылкам и не открывайте документы, прикрепленные к сообщениям, которых вы не ждали и которые выглядят подозрительно.

Установите надежное защитное решение, например Kaspersky Security Cloud, которое обезопасит вас и вашу цифровую инфраструктуру от широкого спектра финансовых киберугроз.

Обеспечить защиту бизнеса от финансовых вредоносных программ необходимо соблюдение следующих правил:

Проводите тренинги по кибербезопасности — особенно для сотрудников, ответственных за финансовый учет — чтобы научить их отличать фишинговые страницы.

Повышайте цифровую грамотность персонала.

Установите политику «запрет по умолчанию» для критически важных пользователей — например, для финансовых подразделений –— чтобы они могли посещать только легитимные веб-сайты.

Устанавливайте последние обновления и исправления для всего используемого ПО [10].

Заключение

Таким образом, рассматриваемая проблема требует скорейшей разработки программ обеспечивающих защиту и снижение негативной динамики информационной и экономической безопасности, тормозящей не только национальную экономику, но мировые экономические системы. Механизмы обеспечения экономической безопасности должны быть направлены не только на повышение технического и информационного обеспечения, уровня цифровых компетенций работников и руководителей, но и совершенствования законодательной базы.

Информация о конфликте интересов

Мы, авторы данной статьи, со всей ответственностью заявляем о частичном и полном отсутствии фактического или потенциального конфликта интересов с какой бы то ни было третьей стороной, который может возникнуть вследствие публикации данной статьи.

ЛИТЕРАТУРА

1. *Стрижкова Д. А.* Фишинговые атаки и методы борьбы с ними [Электронный ресурс] / Д. А. Стрижкова. — Режим доступа: http://web.snauka.ru

2. О стратегии национальной безопасности Российской Федерации : указ Президента Российской Федерации от 31 декабря 2015 г. № 683 [Электронный ресурс]. — Режим доступа: https://base.garant.ru/71296054/

3. Стратегия экономической безопасности до 2030 года: цели и задачи в сфере IT [Электронный ресурс]. — Режим доступа: https://d-russia.ru/strateqiya-ekonomicheskoj-bezopasnosti-do-2030-qoda-tseli-izadachi-v-svere-it.html?ysclid=laxzwiyzd862529903

4. *Сенчагов В. К.* Особенности обеспечения экономической безопасности в зарубежных странах / В. К. Сенчагов // Социально-экономические явления и процессы. — 2015. — № 11. — 12 с.

5. *Глазьев С. В.* Социально-экономическое развитие России / С. В. Глазьев, А. Г. Аганбегян. — Москва : Академия народного хозяйства при Правительстве РФ, 2005. — 32 с.

6. *Емельянова О. В.* Процессы диссипации в экономике России и их оценка / О. В. Емельянова // Научный альманах Центрального Черноземья. — 2014. — № 2. — С. 67—70.

7. Информационная безопасность. Опыт ведущих стран Азии [Электронный ресурс]. — Режим доступа: https://ictnews.uz/27/12/2017/infosec–asia/

8. *Новиков В. В.* Формирование механизма обеспечения экономической безопасности / В. В. Новиков // Экономическая безопасность личности, общества, государства. — 2017. — № 3. — С. 98—103.

9. Число кибератак в России и в мире [Электронный ресурс]. — Режим доступа: https://www.tadviser.ru/index.php/ %D0 %A1 %D1 %82 %D0 %B0 %D1 %82 %D1 %8C %D1 %8F: %D0 %A7 %D0 %B8 %D1 %81 %D0 %BB %D0 %BE_ %D0 %BA %D0 %B8 %D0 %B1 %D0 %B5 %D1 %80 %D0 %B0 %D1 %82 %D0 %B0 %D0 %BA_ %D0 %B2_ %D0 %A0 %D0 %BE %D1 %81 %D1 %81 %D0 %B8 %D0 %B8_ %D0 %B8_ %D0 %B2_ %D0 %BC %D0 %B8 %D1 %80 %D0 %B5

10. Финансовые киберугрозы в 2021 году [Электронный ресурс]. — Режим доступа: https://securelist.ru/financial-cyberthreats-in-2021/104553/

11. *Манахова И. В.* Развитие механизма обеспечения экономической безопасности предприятий при внедрении цифровых технологий / И. В. Манахова, Е. В. Левченко, А. В. Быстров, А, Р, Есина // Вестник РЭУ им. Г. В. Плеханова. — 2019. — № 6 (108). — С. 183—190.

LITERATURE

1. *Strizhkova D. A.* Phishing attacks and methods of dealing with them [Electronic resource] / D. A. Strizhkov. — Access mode: http://web.snauka.ru

2. On the national security strategy of the Russian Federation : Decree of the President of the Russian Federation of December 31, 2015 No. 683 [Electronic resource]. — Access mode: https://base.garant.ru/71296054/

3. Strategy of economic security until 2030: goals and objectives in the field of IT [Electronic resource]. — Access mode: https://d-russia.ru/strateqiya-ekonomicheskoj-bezopasnosti-do-2030-qoda-tseli-izadachi-v-svere-it.html?ysclid=laxzwiyzd862529903

4. *Senchagov V. K.* Features of ensuring economic security in foreign countries / V. K. Senchagov // Socio-economic phenomena and processes. — 2015. — No. 11. — 12 p.

5. *Glazyev S. V.* Socio-economic development of Russia / S. V. Glazyev, A. G. Aganbegyan. — Moscow : Academy of National Economy under the Government of the Russian Federation, 2005. — 32 p.

6. *Emelyanova O. V.* Dissipation processes in the Russian economy and their assessment / O. V. Emelyanova // Scientific Almanac of the Central Chernozem Region. — 2014. — No. 2. — P. 67—70.

7. Information security. The experience of the leading Asian countries [Electronic resource]. — Access mode: https://ictnews.uz/27/12/2017/infosec–asia/

8. *Novikov V. V.* Formation of the mechanism for ensuring economic security / V. V. Novikov // Economic security of the individual, society, state. — 2017. — No. 3. — P. 98—103.

9. The number of cyber attacks in Russia and in the world [Electronic resource]. — Access mode: https://www.tadviser.ru/index.php

10. Financial cyber threats in 2021 [Electronic resource]. — Access mode: https://securelist.ru/financial-cyberthreats-in-2021/104553/

11. *Manakhova I. V.* Development of the mechanism for ensuring the economic security of enterprises in the implementation of digital technologies / I. V. Manakhova, E. V. Levchenko, A. V. Bystrov, A, R, Esina // Vestnik REU im. G. V. Plekhanov. — 2019. — No. 6 (108). — S. 183—190.