УДК 338:004.056.5
DOI:10.24412/2782-4845-2023-5-102-114

К ВОПРОСУ ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ РАЗВИТИЯ ЦИФРОВОЙ ЭКОНОМИКИ

А. В. Ровенская, Среднерусский институт управления – филиал ФГБОУ ВО «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации», г. Орёл, Россия
Е. Ю. Воробьёва, Среднерусский институт управления – филиал ФГБОУ ВО «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации», г. Орёл, Россия

Аннотация. *В настоящее время цифровая экономика проходит фазу активного развития, которое в свою очередь несет в себе не только потенциал и научное понимание, но и практическое применение. В этой связи в статье проводится анализ процесса развития цифровой экономики в системе обеспечения экономической безопасности. В работе отводится особое внимание изучению вопроса кибербезопасности как одного из сложных элементов системы информационно-экономической безопасности, являющегося ценным звеном в создании стабильного поля для развития экономики. Исследование позволило сделать вывод о том, что кибер-безопасность следует рассматривать в качестве важнейшего компонента системы экономической безопасности, а само киберпространство как некий объект, который оказывает влияние на риски и угрозы экономической безопасности в целом.*

Ключевые слова: *экономическая безопасность, информационная безопасность, цифровая экономика, процессы цифровизации, киберугрозы, кибербезопасность*

Для цитирования: Ровенская А. В., Воробьёва Е. Ю. К вопросу обеспечения экономической безопасности в условиях развития цифровой экономики // ЭФО: Экономика. Финансы. Общество. 2023. №1. (5) С.102-114. DOI:10.24412/2782-4845-2023-5-102-114

INTENSIVE DEVELOPMENT OF THE DIGITAL ECONOMY IN THE CONCEPT OF ECONOMIC SECURITY

A.V. Rovenskaya, Central Russian Institute of Management – Branch of the Russian Academy of National Economy and Public Administration under the President of the Russian Federation, Orel, Russia
E.Y. Vorobyeva, Central Russian Institute of Management - branch of the Russian Academy of National Economy and Public Administration under the President of the Russian Federation Russian Federation, Orel, Russia

Abstract. *At present the digital economy is undergoing intensive development, which in its turn possesses not only potential and scientific understanding, but also practical significancen. It is also worth emphasizing that the process of intensive development of the digital economy is necessary to assess socio-economic transformations in the system of*

economic security. That is why questions about cybersecurity have become more imperative now than ever. Since it is one of the most complex elements of the information and economic security system, it is a valuable link in creating a stable field for economic development. It turns out that in modern realities we should consider cyber security as the most important component of the economic security system, and cyberspace itself as an object that influences risks and threats to economic security.

Keywords: *economic security, information security, digital economy (digitalization), cyber threats, cybersecurity*

Введение

Начиная с 2022 года Российская Федерация вступила в период экономического спада или рецессию. При этом важно учесть, что по мнению экспертов, согласно прогнозам, данная фаза экономического спада продолжится. В настоящее время появляется всё больше и больше угроз, направленных на экономическую безопасность не только государства, но и находящихся в ней отдельно взятых организаций и учреждений. В этой связи нами были выделены три основные причины, которые в графическом виде представлены на рисунке 1.

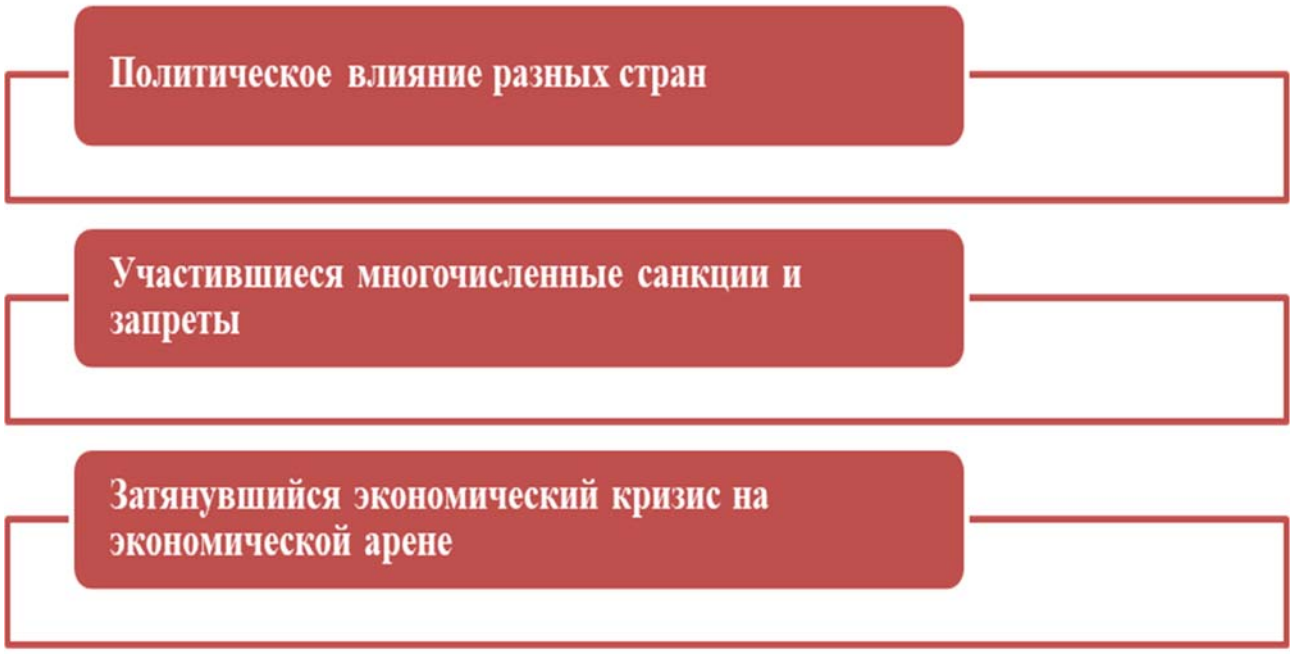

Рис. 1. **Причины появления угроз, направленных на экономическую безопасность не только государства, но и находящихся в ней отдельно взятых организаций и учреждений (2022–2023 гг.)***

****составлено авторами на основе данных [1]***

Практика показывает, что в экономической сфере общества произошло интенсивное развитие и трансформация процесса цифровизации, которые оказали большое влияние на ведение бизнеса, общество и саму мировую экономику в целом, и все это произошло за последние десятилетия. Сейчас можно констатировать, что имеется потребность в глобальном управлении

цифровой средой. Причиной этого можно считать следующее: несоблюдение равновесия между выгодами и рисками.

У общества есть понимание того, что цифровая экономика масштабна – у нее нет границ, так как благодаря своему стремительному развитию сфера цифровых технологий занимает значимое место не только в развитии науки, техники, но и в экономики. Естественно и то, что с увеличением роли отводимой цифровой экономике появляются и более сложные задачи: как управлять ею и соответственно, как ее регулировать. В современных реалиях залогом успеха любого вида хозяйственной деятельности является именно эффективное управление таким ресурсом цифровой экономики как информация, в конкурентной борьбе зачастую именно монопольное обладание данными оказывается решающим преимуществом.

Основная часть

В Указе Президента РФ от 9 мая 2017 г. № 203 "О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы", цифровая экономика определяется как приоритетное направление развития России. В рамках современного технологического уклада требуется дальнейшее повышение конкурентоспособности страны, так как именно интенсивное развитие цифровизации должно способствовать этому процессу. Важен и тот факт, что переход к цифровой экономике и ее стремительное развитие дают серьезные преимущества бизнесу, что выражается во многих аспектах, некоторые из которых были приведены в качестве примеров, а именно: внедрение различных цифровых технологий помогает ускорять получение необходимых услуг; позволяет быстро находить и сортировать всю необходимую информацию по ценам, продуктам, услугам, а также поставщикам. Не стоит забывать, что формирование цифровой экономики имеет не только положительные стороны, но и отрицательные, принимающие вид серьезных рисков и угроз экономической безопасности.

Акцентировать внимание стоит и на том, что основой формирования доверия в рамках новых условий взаимодействия являются именно современные цифровые технологии, которые уже стали одним из важных условий для социально-экономического развития.

Все экономические субъекты вне зависимости от формы собственности, отраслевой принадлежности имеют ряд проблем, связанных с обеспечением экономической безопасности, и сам процесс решения этих проблем является сложным. В экономических субъектах обеспечением экономической безопасности занимается персонал, менеджмент и собственники, при этом их функции в этих рамках закреплены в нормативных документах самой организаций. Средства передачи информации, как и места ее хранения, являются источниками рисков и угроз, которым в последнее время уделяется наибольшее внимание. В этой связи представляется целесообразным выделить инструменты экономической безопасности в условиях цифровой экономики, которые изображены на рисунке 2.

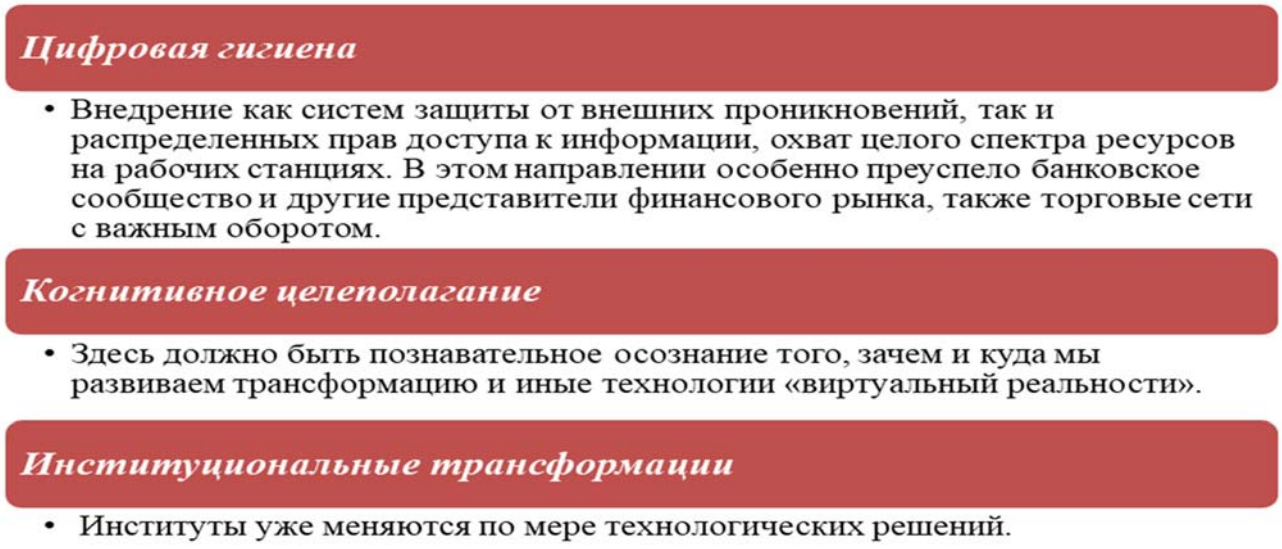

Рис. 2.* Инструменты экономической безопасности в условиях цифровой экономики

****составлено авторами на основе данных [1]***

Рассматривая экономическую безопасность в условиях интенсивного развития цифровой экономики, стоит обратить внимание и на период пандемии 2020 года, которая затронула все страны, включая Российскую Федерацию. Так, по данным Positive Technologies значение количества атак в начале 2020 года (1 кв.) превысило аналогичный показатель конца 2019 года (4 кв.) на 22,5%. Если рассматривать итоги 2022 года, то можно сказать, что количество атак увеличилось на 14,8% по сравнению с 2021 годом.

Для более наглядного примера нами был проведен анализ актуальных угроз информационной безопасности, основанный на экспертизе компании Positive Technologies, результатах расследований, а также на данных официальных источников. В качестве анализируемого периода был принят период 2021-2022 гг., сравнительный поквартальный анализ количества атак можно рассмотреть на рисунке 3.

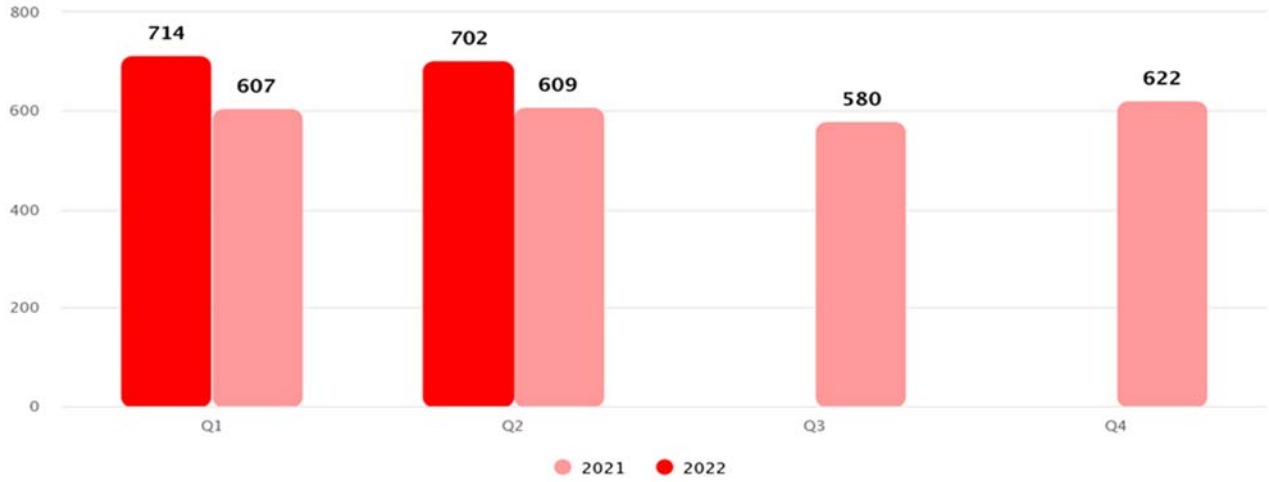

Рис. 3.* Количество атак в 2021 и 2022 годах (по кварталам)

****составлено авторами на основе данных [2]***

Стоит отметить, что чаще всего кибератакам подвергались государственные и научно-образовательные учреждения, организации промышленного сектора учреждения. Более подробно эта информация отображена на рисунке 4.

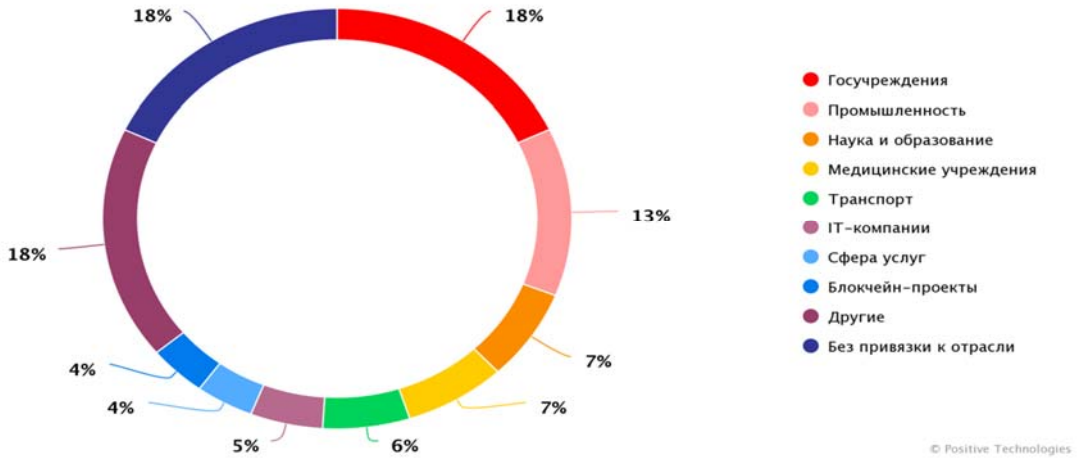

Рис. 4.* Категории жертв среди организаций

****составлено авторами на основе данных [3]***

Одним из важнейших элементов системы информационной безопасности (далее - ИБ) считаются именно «киберугрозы», но в современных реалиях этот поход должен быть изменен, ведь нам стоит учитывать и последствия, получаемые субъектами экономики от реализации таких угроз. Из этого следует, что в современных реалиях нам стоит рассматривать кибер-безопасность как важнейший компонент системы экономической безопасности, а само киберпространство как некий объект, который оказывает влияние на риски и угрозы экономической безопасности.

Далее. в процессе исследования нами были установлены основные причины так называемого «слива информации» из-за атак не только на «компьютерные» системы, но и на «реальные» (например, кардиостимуляторы, бытовые устройства и т.д.), а именно минусы устройств, используемых в повседневности. На рисунке 5 отображены итоговые статистические данные.

Рис. 5.* Минусы устройств, используемых в повседневности

****составлено авторами на основе данных [4]***

Есть множество вариантов характеристики «информационного права» с точки зрения кибернетического пространства, которые нашли отображение в рисунке 6.

Также стоит обратить внимание и на тот факт, что так называемые «кибератаки» имеют кардинальное отличие от злонамеренных действий «обычных» нарушителей. Это отличие проявляется в том, что «обычные» злоумышленники имеют ограниченный арсенал средств воздействия в сети Интернет (например, вирусы, трояны, уязвимости и эксплойты). Именно по этой причине они стремятся применить эти средства воздействия на как можно более широком классе систем, следовательно, их основной целью является именно охват «широкой аудитории». Если же рассматривать сами «киберугрозы», то можно увидеть обратную ситуацию, т.е. арсенал различных средств воздействия направлен уже на ограниченный набор целей. При этом сами субъекты «киберугроз» обладают значительным количеством ресурсов, которые направляются на поиск путей, способов и механизмов воздействия преимущественно на целевые системы.

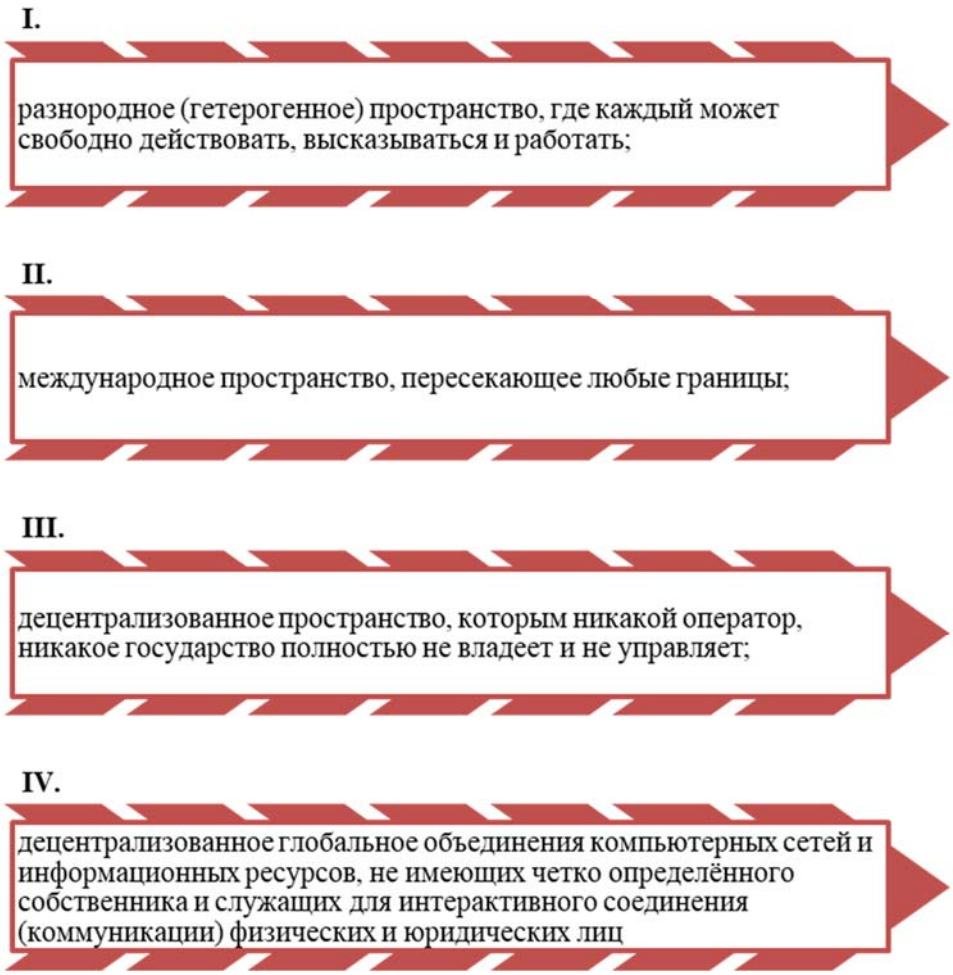

Рис. 6. **Характеристики «информационного права» с точки зрения кибернетического пространства***

****составлено авторами на основе данных [5]***

Получается, что определением «кибербезопасности» в секторе экономической безопасности является: «состояние киберпространства самой организации, благодаря которому появляется возможность достигнуть баланса как финансовых, так и иных ресурсов организации. При этом обеспечивается экономическая безопасность, благодаря которой сохраняется заданный уровень информации, работы информационных систем и компьютерной техники».

Со временем появляется большое количество различных инструментов и методов, позволяющих обеспечивать экономическую безопасность, но для их внедрения организациям необходимо понимание современных тенденций развития информационных технологий.

Так, в настоящее время в России продолжает функционировать Федеральный проект «Информационная безопасность» Национального проекта «Цифровая экономика». Одно из направлений его деятельности — создание в России сети опорных центров Национального киберполигона для подготовки высококвалифицированных кадров в сфере кибербезопасности.

Проанализировав основные тенденции появления новых угроз безопасности и механизмов их осуществления, на современном этапе развития информационных технологий были выявлены тенденции, отображенные на рисунке 7.

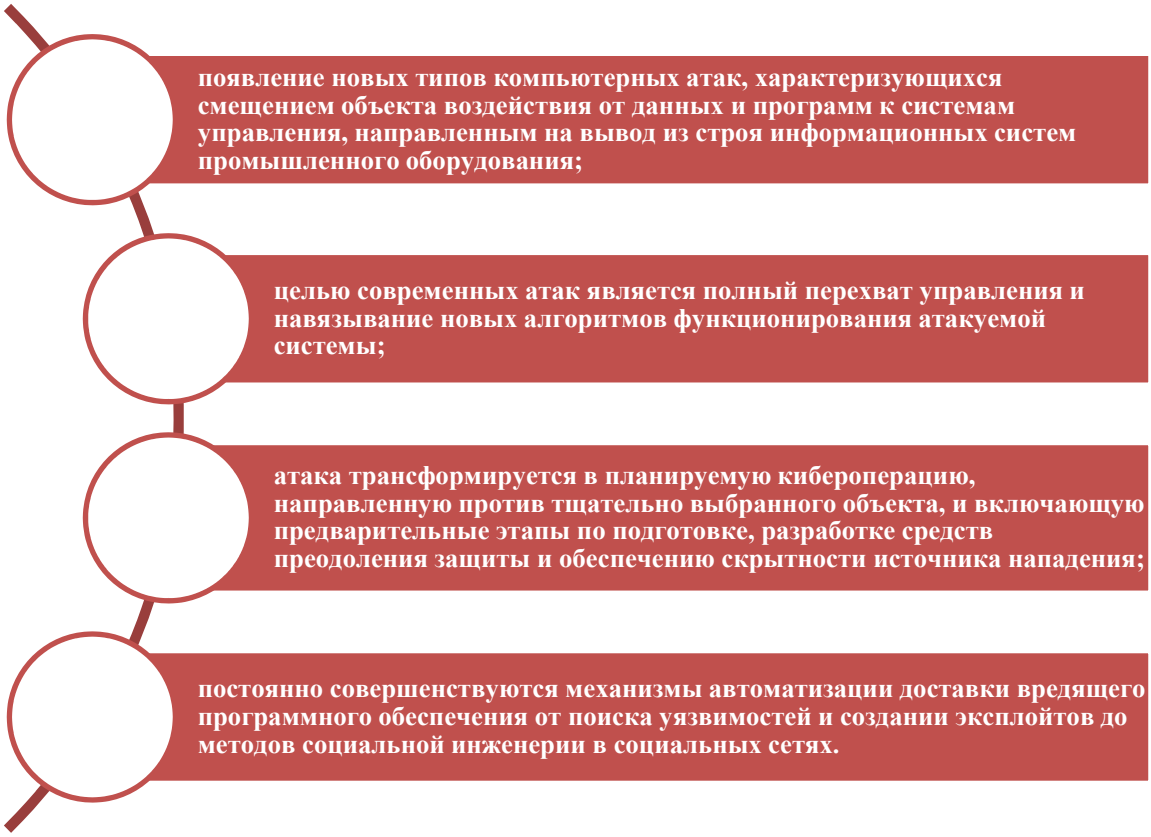

Рис. 7. **Тенденции появления новых угроз безопасности и механизмов их осуществления, на современном этапе развития информационных технологий***

****составлено авторами на основе данных [6]***

В настоящее время можно отметить, что не только производство различных средств нарушения безопасности, но и их доставка уже превратились в совершенно легальную IT-отрасль. В качестве примера можно привести наличие такого рода специфической услуги, как «hacking of service» (взлом сервиса). Зачастую она появляется в виде сети сайтов и различных программных средств типа «Black hole» (черная дыра).

Также стоит отметить, что нанесенный ущерб может быть достаточно весомым, особенно в условиях:

- прогрессирующего числа атак;
- создания различных механизмов, направленных на их автоматизацию;
- значительной зависимости информационной инфраструктуры и автоматизированных систем управления от электронных средств доступа и обмена информацией.

Все перечисленные условия усугубляются тем, что злоумышленники зачастую получают доступ к самой конфиденциальной информации.

Таким образом, проанализировав последствия атак на различные организации и частных лиц можно выделить основные типы, отображенные в рисунке 8.

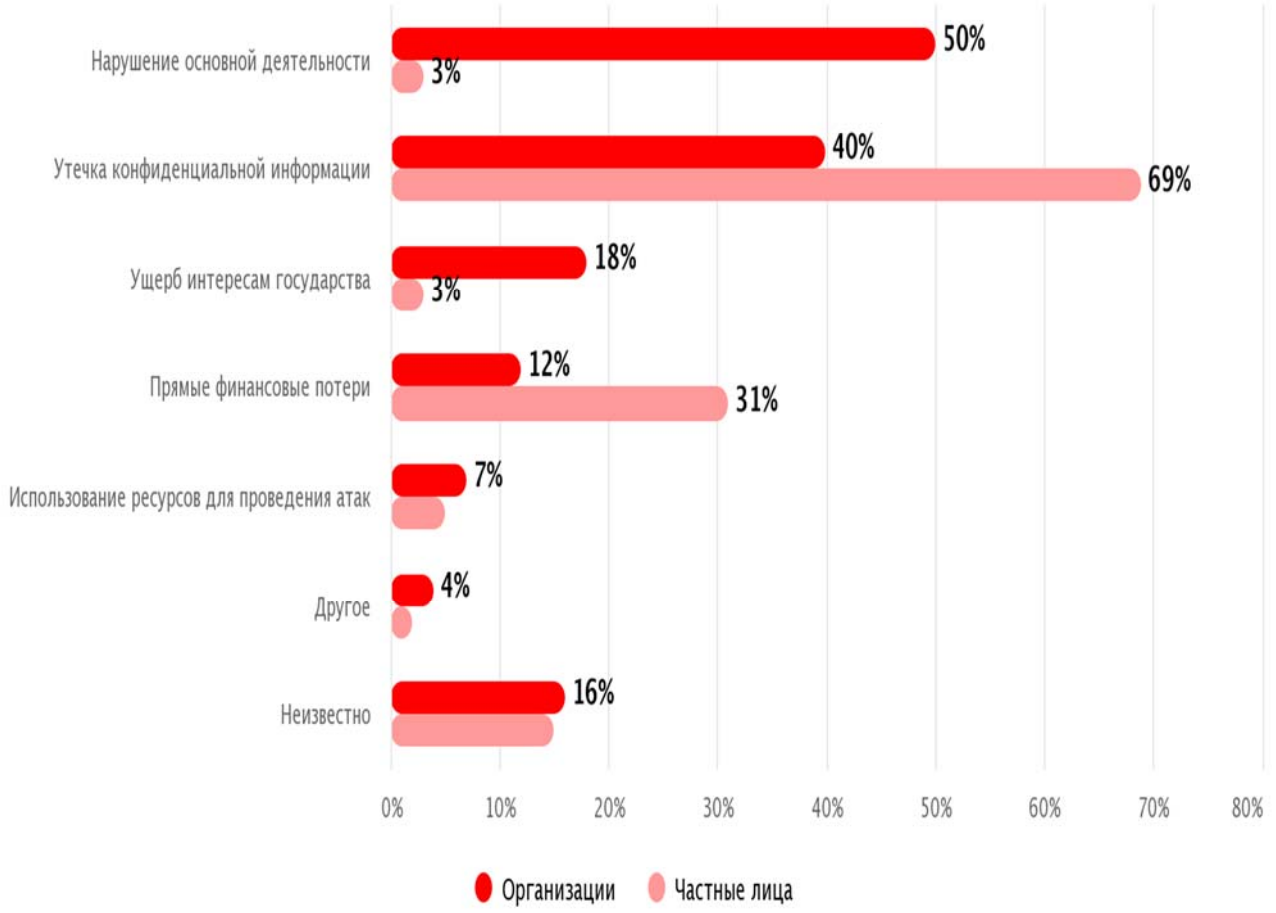

Рис. 8.* Последствия атак (доля атак)

****составлено авторами на основе данных [8]***

Также считаем важным выделить последствия атак на государственные учреждения, которые показаны на рисунке 9.

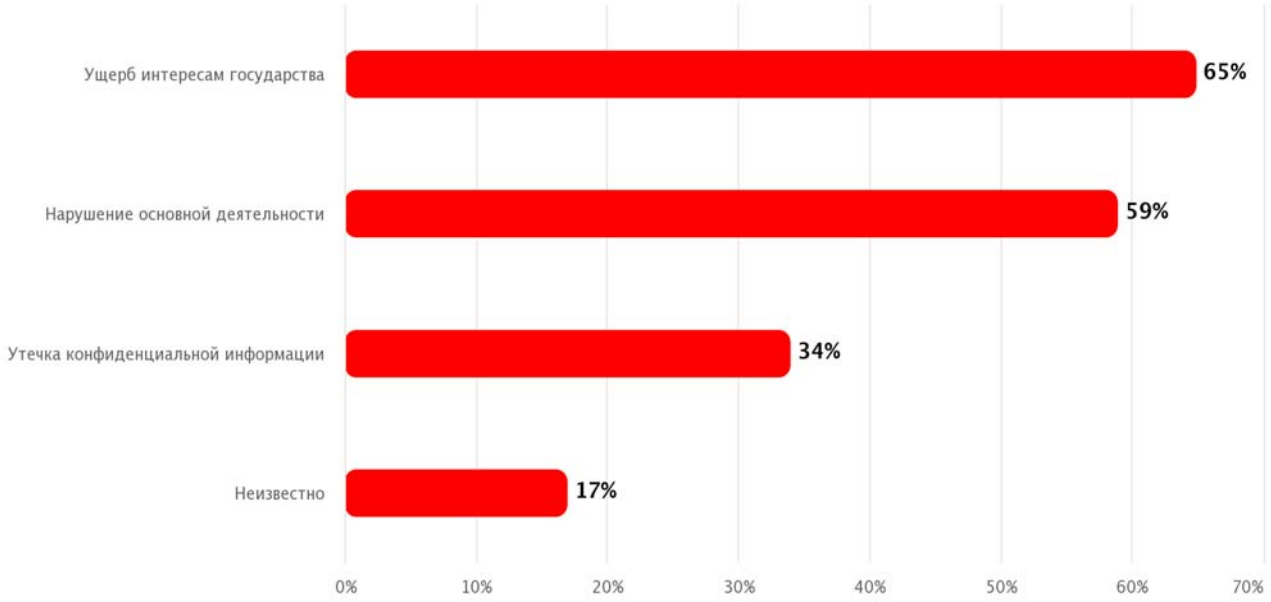

Рис. 9.* Последствия атак на государственные учреждения

****составлено авторами на основе данных [9]***

При рассмотрении «кибератак» направленных на государственные учреждения, можно заметить, что именно во II-м квартале 2022 года на них было направлено наибольшее количество «кибератак» среди различных организаций. Сравнивая количество атак за I-й и II-й кварталы 2022 года, можно сделать вывод, что их доля от общего числа атак возросла на 2 п.п.

При этом «кибератаки», которые были направленны именно на государственные учреждения, в 59% случаев имели серьезные последствия, которые нарушали основную деятельность учреждений, а это, в свою очередь, приводило к ущербу интересам самого государства (65%).

Статистика свидетельствует, что в России 2022 год стал рекордным с точки зрения распространения глобальных и локальных киберугроз. Информационная безопасность, потребность в которой возросла в разы в период пандемии, вновь дала о себе знать после ухода из страны зарубежных производителей программных обеспечений. Ландшафт киберугроз изменился. В широкой защите от киберпреступников нуждаются буквально все: как госучреждения, так и крупные промышленные корпорации, малый и средний бизнес, а также рядовые пользователи. При этом большое количество пользователе стало жертвами масштабных утечек данных. Всё это позволяет злоумышленникам совершенствовать схемы атак с использованием социальной инженерии, то есть злоумышленники смогут проводить свои атаки уже более точечно, так как они располагают детальной информацией о действиях жертвы.

Также статистика указывает на увеличение активности преступных действий в отношении частных лиц, клиентов онлайн-банков и других онлайн-

сервисов. Это происходит по причине того, что сейчас распространяется большое количество готовых комплектов для проведения массовых атак. Именно поэтому на текущий момент эксперты прогнозируют не только увеличение количества атак на пользователей социальных сетей и мессенджеров, н и рост числа атак на второй фактор аутентификации, применяемый пользователями именно для входа в различные сервисы.

В 2022 году было использовано много различных вредоносных арсеналов. Основную статистику по применяемым методам можно увидеть на рисунке 10.

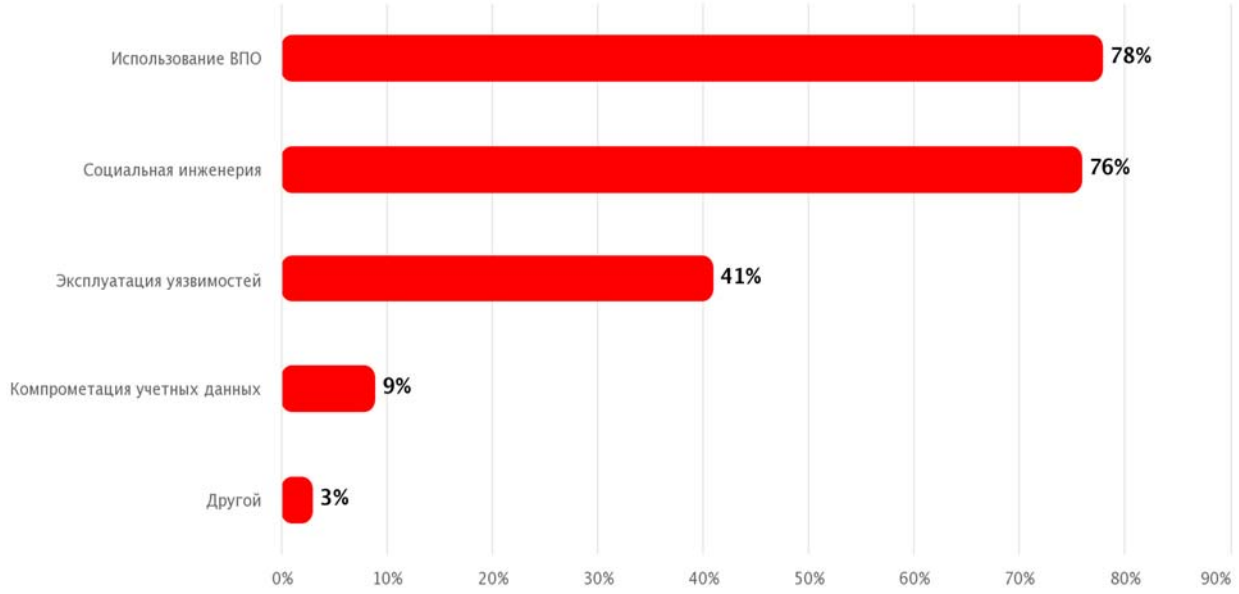

Рис. 10. **Виды вредоносных арсеналов, используемые в 2022 году***

****составлено авторами на основе данных [10]***

Злоумышленники, по наблюдениям экспертов, фокусируются на трех направлениях: медиа, государственные информационные системы и критическая информационная инфраструктура. Несмотря на то, что у рынка информационной экономической безопасности в России достаточно высокая степень зрелости, ему потребуется время для перенастройки. С одной стороны, рост числа цифровых атак продолжает оказывать давление и делает цифровое пространство уязвимым, с другой стороны — отечественные разработчики держат руку на пульсе и готовы предложить актуальные решения в области информационной безопасности. Эти процессы проходят на фоне введения дополнительных мер в сфере экономической безопасности на государственном уровне, которые предполагают появление ИБ-подразделения в каждой госструктуре, привлечение к работе организаций, имеющих лицензии на осуществление деятельности по технической защите конфиденциальной информации, переход на отечественное ПО.

Стоит обратить внимание и на то, то в современном мире узко специализированным проблемам остаётся все меньше места, из-за чего большое значение приобрело исследование междисциплинарных предметных областей, к

которым на данный момент можно отнести обеспечение экономической безопасности (ЭБ). Для достижения обеспечения ЭБ сейчас особое внимание уделяется именно проблемам, связанным с противодействием отрицательному влиянию «киберугроз», которые способны нанести ущерб экономической системе различного уровня управления. Кроме того, уже с 1 января 2025 года российские госструктуры должны осуществить полный переход на средства защиты информации отечественных разработчиков.

Заключение

Проведенное исследование позволило прийти к выводу, что вопросы «кибербезопасности» стали важным звеном в создании стабильного поля для развития экономики, а необходимость перехода госструктур и частного бизнеса на отечественное ПО очень актуальна.

Руководители госорганов и организаций должны нести личную ответственность за информационную безопасность в экономической деятельности, а также им необходимо создать новое или возложить обязанности на существующее структурное подразделение по обеспечению информационной безопасности, включая меры по обнаружению, предупреждению и ликвидации последствий кибератак и реагированию на киберинциденты.

Список использованных источников:

1. Актуальные киберугрозы [Электронный ресурс], 2022 URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q2/#id11 (Дата обращения: 04.02.2023)

2. Шалаев, И.А. Использование инновационных информационных технологий при модернизации и повышении эффективности налогового администрирования и налогового контроля в условиях развития цифровой трансформации экономики и своевременного применения технологий больших данных / И.А. Шалаев, О.И. Кожанчиков, О.И. Карпова, С.А. Ильминская //Вестник ОрелГИЭТ. 2021. № 4 (58). С. 92-104.

3. Рынок информационной безопасности: итоги года и прогнозы экспертов на 2023 год [Электронный ресурс], 2022 URL: https://www.anti-malware.ru/analytics/Technology_Analysis/AMLive-2022-results (Дата обращения: 07.01.2023)

4. Кобышева М.С., Володин А.А., Иванов М.В., Феофилова Т.Ю., Манасерян Т.М. Риски и угрозы экономической безопасности россии в условиях цифровой трансформации // Вестник Алтайской академии экономики и права. – 2021. – № 2. – С. 53-60; URL: https://vaael.ru/ru/article/view?id=1597 (дата обращения: 07.01.2023).

5. Информационная безопасность в условиях цифровой экономики [Электронный ресурс], 2022 URL: https://www.smart-soft.ru/blog/informatsionnaja_bezopasnost_v_uslovijah_tsifrovoj_ekonomiki/ (Дата обращения: 04.02.2023)

6. Коржова Д.К. Основные элементы адаптации в условиях цифровой трансформации экономики // Материалы XII Международной студенческой научной конференции «Студенческий научный форум» URL: https://scienceforum.ru/2020/article/2018018475 (дата обращения: 02.02.2023).

7. Как приспособиться к цифровой трансформации бизнесам не цифровой специфики [Электронный ресурс] // URL: https://russoft.org/news/kak-prisposobitsya-k-tsifrovoj-transformatsii-biznesam-ne-tsifrovoj-spetsifiki/(дата обращения 09.12.2019)

8. Субботина А.О., Сергеева И.А. Экономическая безопасность в условиях цифровой экономики / Экономическая безопасность общества, государства и личности: проблемы и направления обеспечения. Сборник статей по материалам VIII научно-практической конференции 11 марта 2021 г. / под общ. ред. С.В. Тактаровой, А.Ю. Сергеева. – Москва: Издательство «Перо», 2021 – С. 142-144

9. Уразгалиев, В. Ш. Экономическая безопасность : Учебник и практикум для вузов / В. Ш. Уразгалиев. -Москва : Юрайт, 2019. - 675 с.

10. Вечканов Г.С. «Экономическая безопасность: Учебник для вузов» // Режим доступа: URL: https://ru.b-ok.cc/book/2459923/aed0c9 (дата обращения 02.02.2023 г.)

11. Ерёмина Е.О. Теоретические аспекты экономической безопасности и угрозы ее обеспечения // Материалы XII Международной студенческой научной конференции «Студенческий научный форум» URL: https://scienceforum.ru/2020/article/2018018738 (дата обращения: 03.02.2023).

Сведения об авторах / Information about the author:

Ровенская Анастасия Васильевна – *студентка 1-го курса, Среднерусский институт управления – филиал ФГБОУ ВО «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации», факультет: Экономико-правовое обеспечение экономической безопасности субъектов хозяйственной деятельности, e-mail: r.a.v1608@yandex.ru /* ***Rovenskaya Anastasia Vasilyevna –*** *1st year student, Central Russian Institute of Management - branch of the Russian Academy of National Economy and Public Administration under the President of the Russian Federation, Faculty: Economic and legal support of economic security of economic entities, e-mail: r.a.v1608@yandex.ru*

Воробьёва Елена Юрьевна *– студентка 1-го курса, Среднерусский институт управления – филиал ФГБОУ ВО «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации», факультет: Экономико-правовое обеспечение экономической безопасности субъектов хозяйственной деятельности, e-mail: lena.vorobyova.03@mail.ru /* ***Vorobyeva Elena Yurievna*** *– 1st year student, Central Russian Institute of Management - branch of the Russian Academy of National Economy and Public Administration under the President of the Russian Federation, Faculty: Economic and legal support of economic security of economic entitiesф, e-mail: lena.vorobyova.03@mail.ru*

Сведения о вкладе каждого автора / Information about the contribution of each author

Ровенская А.В. *– проведение анализа основных показателей, обработка результатов исследований, визуализация, разработка теоретических предпосылок, доработка текста, формирование общих выводов и литературный анализ.*
Воробьева Е.Ю. *– формулирование основных направлений исследования, подготовка начального варианта статьи.*

Rivenskaya A.V. *- analysis of the main indicators, processing of research results, visualization, development of theoretical prerequisites, revision of the text, formation of general conclusions and literary analysis.*
Vorobyova E.Yu. *- formulation of the main directions of the research, preparation of the initial version of the paper.*

Дата поступления статьи: 10.03.2023
Принято решение о публикации: 28.03.2023

Авторы прочитали и одобрили окончательный вариант рукописи.

Конфликт интересов: авторы заявляют об отсутствии конфликта интересов.