УДК 338.2

РОЛЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЦИФРОВОЙ ЭКОНОМИКЕ

Иваев М.И.,
Поволжский государственный университет телекоммуникаций и информатики, Самара,
email: ivaevmarat@ya.ru, annamalina951@list.ru, avsafronova2002@mail.ru

Сафронова А.В.,
Поволжский государственный университет телекоммуникаций и информатики, Самара,
email: ivaevmarat@ya.ru, annamalina951@list.ru, avsafronova2002@mail.ru

Калемалькина А.А.,
Поволжский государственный университет телекоммуникаций и информатики, Самара,
email: ivaevmarat@ya.ru, annamalina951@list.ru, avsafronova2002@mail.ru

Аннотация. *Современное развитие экономики тесно связано с использованием интернета, спутниковой связи и передовых технологий обработки, хранения и передачи данных. Это подчеркивает важность защиты персональной информации и обеспечения информационной безопасности как для предприятий, так и для государства. Неавторизованный доступ к информационным ресурсам компаний, уничтожение данных, блокирование и копирование в личных целях могут принести серьезный ущерб как отдельным гражданам, так и всему обществу. В данной статье рассмотрим взаимосвязь между информационной безопасностью и экономической безопасностью, выявим современные вызовы и угрозы, с которыми сталкивается экономика в эпоху цифровой трансформации. Проанализируем статистические данные об экономических преступлениях, совершаемых с использованием цифровых технологий и определим возможные причины и факторы, способствующие ослаблению безопасности цифровой экономики. Также представим анализ статистических данных, в котором будут описаны количество и структура преступлений, связанных с нарушением информационной безопасности на территории страны. Особое внимание будет уделено борьбе с кибератаками на официальные веб-сайты государственных органов, разработке, использованию и распространению вредоносных компьютерных программ, а также пресечению мошенничества с использованием электронных платежных средств.*

Ключевые слова: информационная безопасность, цифровые технологии, кибербезопасность, цифровая экономика, экономическая безопасность, преступления, мошенничество, защита данных, угрозы, меры безопасности.

THE ROLE OF INFORMATION SECURITY IN THE DIGITAL ECONOMY

Ivaev M.I.,
Volga Region State University of Telecommunications and Informatics, Samara,
email: ivaevmarat@ya.ru, annamalina951@list.ru avsafronova2002@mail.ru

Safronova A.V.,
Volga Region State University of Telecommunications and Informatics, Samara,
email: ivaevmarat@ya.ru, annamalina951@list.ru avsafronova2002@mail.ru

Kalemalkina A.A.,
Volga Region State University of Telecommunications and Informatics, Samara,
email: ivaevmarat@ya.ru, annamalina951@list.ru avsafronova2002@mail.ru

Abstract. *Modern economic development is closely linked to the use of the Internet, satellite communications and advanced technologies for processing, storing and transmitting data. This highlights the importance of protecting personal information and ensuring information security for both businesses and the state. Unauthorized access to information resources of companies, data destruction, blocking and copying for personal purposes can cause serious damage to both individual citizens and the entire society. In this article, we will consider the relationship between information security and economic security, identify modern challenges and threats faced by the economy in the era of digital transformation. Let's analyze statistical data on economic crimes committed using digital technologies and identify possible causes and factors contributing to the weakening of the security of the digital economy. We will also present an analysis of statistical data, which will describe the number and structure of crimes related to information security violations in the country. Special attention will be paid to combating cyber-attacks on official websites of government agencies, the development, use and distribution of malicious computer programs, as well as the suppression of fraud using electronic means of payment.*

Keywords: information security, digital technologies, cybersecurity, digital economy, economic security, crimes, fraud, data protection, threats, security measures.

Основные положения

- Киберпреступность растет, нанося значительный ущерб мировой экономике.
- Доступ в интернет широко распространен как среди населения, так и среди организаций, что увеличивает количество потенциальных жертв киберпреступлений.
- Количество атак на критическую информационную инфраструктуру растет, что требует усиления мер по обеспечению информационной безопасности.

Введение

В современной цифровой экономике обеспечение безопасности становится все более сложной задачей из-за увеличения частоты и сложности кибератак, которые стимулируются использованием цифровых технологий. Органы, ответственные за экономическую и информационную безопасность, сталкиваются с вызовом выявления и снижения этих угроз, а также создания условий, способствующих улучшению информационной безопасности в цифровой среде.

Президент России Владимир Путин подчеркнул, что отсутствие цифровой экономики представляет угрозу для будущего страны. Он утверждает, что переход к новым технологиям необходим для развития российской экономики и общества в целом.

Цель исследования

Выявить проблемы и угрозы, которые сопровождают функционирование цифровой экономики и постоянную цифровую трансформацию. Эти вызовы и угрозы направлены на нарушение информационной и экономической безопасности России. Экономическая и информационная безопасность считаются компонентами национальной безопасности (рис. 1). Стратегические цели определяют необходимые цели устойчивого долгосрочного развития является одной из главных задач государства и требует принятия соответствующих мер.

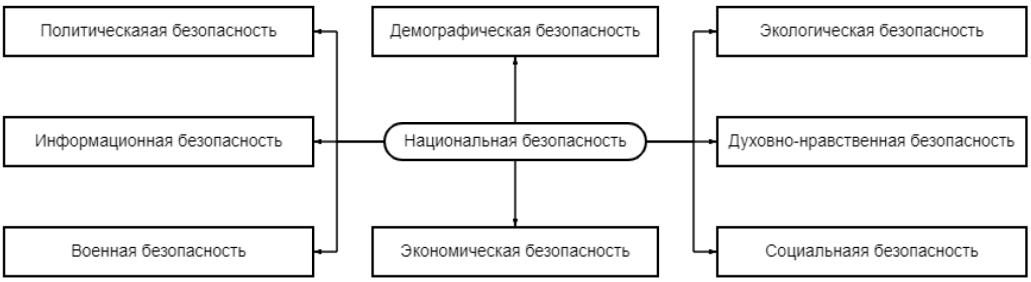

Рис. 1. *Структура национальной безопасности*

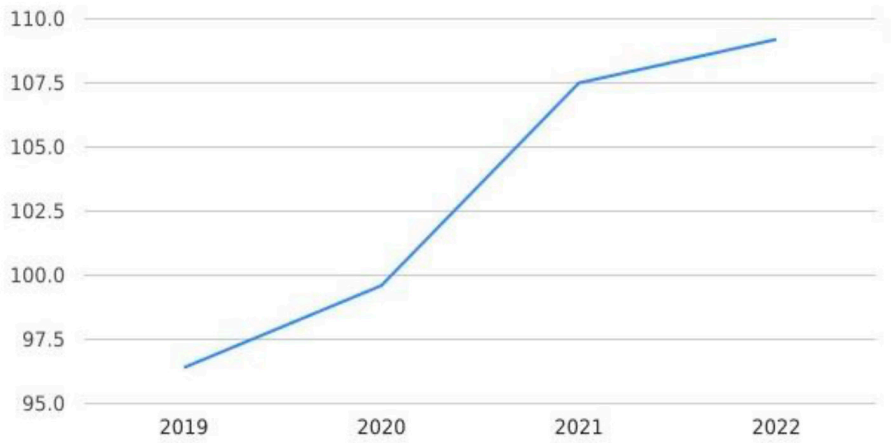

Рис. 2. *Число абонентов мобильного широкополосного доступа в Интернет на 100 человек населения*

Современная преступность все больше переходит в киберсреду. Киберпреступность выросла в 11 раз за последние 6 лет по данным Генпрокуратуры РФ. Ущерб мировой экономике от цифровых преступлений оценивается от 0,7 до 3 триллионов долларов и продолжает расти.

Методы исследования

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». К концу 2022 года примерно 109 из 100 человек в России имели доступ к мобильному интернету (рис. 2).

Фиксированный широкополосный доступ имеет 24 из 100 человек. Эта разница обусловлена размером необходимых вложений поставщиков в строительство телекоммуникационных сетей, число абонентов, имеющих как фиксированный, так и мобильный доступ в интернет, растет.

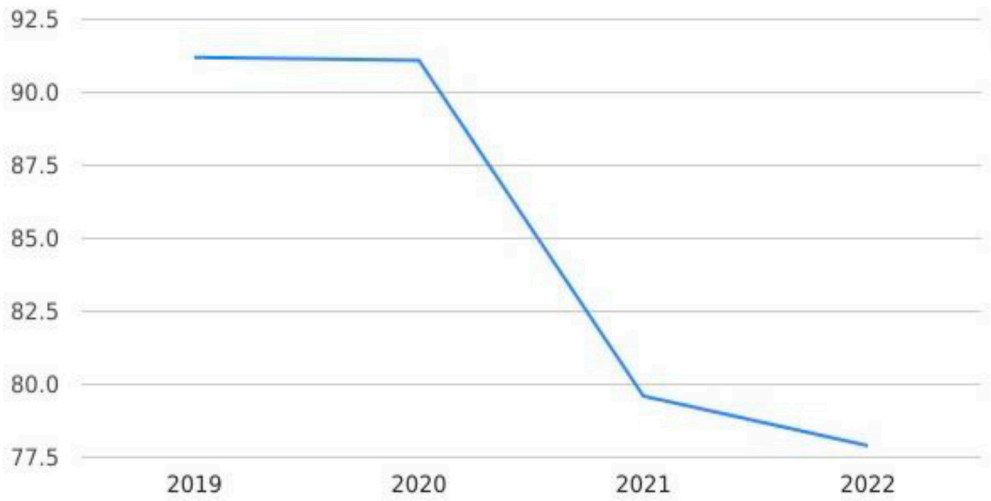

Рис. 3. *Доля организаций, использовавших Интернет, в общем числе обследованных организаций, %*

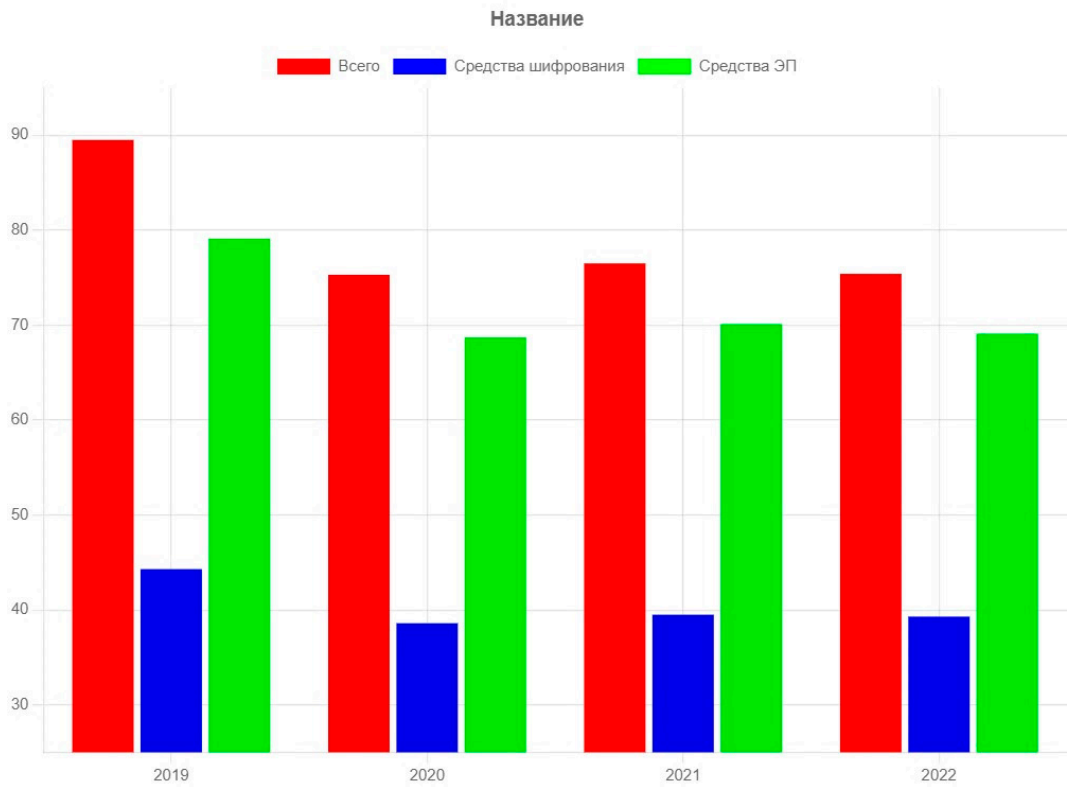

Рис. 4. *Доля организаций, использовавших средства защиты информации, передаваемой по глобальным сетям, %*

Среди организаций наблюдается значительный рост тех, кто внедряет интернет-технологии в свою деятельность. По данным на 2022 год, доля таких организаций составляет 89% (рис. 3).

Так как среди населения и организаций широко распространен доступ в интернет, то это повышает их вероятность стать жертвами киберпреступлений. Наша цель заключалась в изучении количества организаций, обеспечивающих защиту информации. К 2022 году доля таких организаций составляет 75,4% (рис. 4), что на 14,1% меньше, чем в 2019 году.

По данным Совета Безопасности РФ, в 2020 году зафиксировано около 1,4 миллиона атак на критическую информационную инфраструктуру. В 2021 году количество попыток проникновения в информационные системы властей выросло на 6,5% до 7,9 миллиона. Основной целью большинства атак является получение ограниченного доступа к информации и нарушение функционирования технических средств.

Интернет-мошенничество выделяется как основная проблема в киберпреступности. Интернет, хоть и важный источник информации, также служит средой для обмана. Для среднестатистического пользователя трудно оценить надежность сайтов, что делает его уязвимым перед мошенниками, использующими информационные технологии для обмана. Сложности в идентификации нарушителей делают их действия менее очевидными.

Надзорный орган имеет право блокировать и ограничивать доступ пользователей к нежелательному контенту с целью снижения распространения незаконного контента и обеспечения безопасности пользователей в сети. Эти действия ставят перед правоохранительными органами актуальную и сложную задачу борьбы с преступлениями в сфере информационных технологий.

Следует отметить, что пропорции преступлений примерно одинаковы, независимо от масштабов деятельности предприятия. Это потому, что киберпреступники выбирают объект преступления в зависимости от уровня безопасности информационных систем. Важнейшее правило защиты информационной системы предприятия состоит в том, что деньги, выделяемые на защиту информационной безопасности, не должны превышать затрат и потенциальной стоимости защищаемой информации. Структура киберпреступности в отношении экономических субъектов показана на рисунке 6.

Рис. 5. *Структура киберпреступлений, %*

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

Из этого можно сделать вывод, что доступность информации не всегда определяет ее ценность, и наоборот. С появлением новых технологий преступники улучшают свои методы действий, что делает их доступными для широкого круга людей, не знакомых с информационными технологиями. Это приводит к увеличению числа незаконных транзакций, особенно через интернет и мобильные устройства, включая интернет-банкинг. В 2019 году количество несанкционированных операций с платежными картами увеличилось на 44%, причинив ущерб в размере 1,38 млрд рублей. В 93% случаев такие операции происходят из-за использования электронных платежных средств без согласия клиента, из-за незаконных действий, утечки конфиденциальной информации и нарушения процесса аутентификации.

Социальная инженерия становится все более распространенной, что увеличивает риск несанкционированного доступа к личным данным граждан. Базы данных с телефонными номерами, именами и паспортными данными можно легко найти в интернете. Хотя в России действует закон о персональных данных, количество противоправных действий не уменьшается из-за сложности выявления преступлений и отсутствия прямого физического контакта между преступником и жертвой.

Результаты исследования и их обсуждение

Для улучшения информационной безопасности в цифровой экономике и обеспечения экономической безопасности страны, организации и частные лица могут принимать следующие меры:

1. Проведение обучения об информационной безопасности для населения о потенциальных угрозах в цифровой сфере, методах действий мошенников, способах предотвращения финансовых потерь, защите личных данных, которые являются объектом интереса злоумышленников.

2. Необходимо усовершенствовать законодательную базу в сфере информационной безопасности, определить возможные наказания за совершение преступлений против экономической и информационной безопасности граждан и государств.

3. Улучшение работы по блокировке сайтов, почтовых сообщений и колл-центров от мошеннических структур.

4. Налаживание взаимодействия с операторами мобильной связи и поставщиками телекоммуникаций, а также с телефонией и курьерами, улучшение взаимодействия с государственными учреждениями.

5. Составление «белого списка» банков и финансовых учреждений, уполномоченных запускать программы банкоматов. Программы за пределами этого списка не могут быть запущены в банкоматах, поэтому преступники не могут встраивать вредоносное ПО в операционные системы банкоматов.

Выводы

Важно понимать, что экономическая безопасность государства тесно связана с безопасностью экономических субъектов и отдельных личностей. Эти аспекты следует рассматривать в комплексе, так как безопасность экономической системы зависит от наиболее уязвимых звеньев. Эти уязвимые моменты могут быть представлены индивидуальными лицами, и пока они не защищены, угроза для общей безопасности страны будет сохраняться. С ростом информатизации экономических процессов возрастает потребность в дополнительных мерах безопасности.

Сегодня многие люди имеют доступ к смартфонам и компьютерам с возможностью подключения к Интернету. Каждый обладает своим собственным банковским счетом и карточкой, а также установленным мобильным приложением от банка. Это позволяет удобно и быстро управлять своими финансами, избегая походов в банк и экономя время, нервы и силы. Однако криминалитет также осознает преимущества данной ситуации и стремится обогатиться за счет других людей. Мошенники прибегают к различным способам взлома личных кабинетов пользователей мобильных приложений банков, получая доступ к деньгам и личным данным клиентов, чтобы реализовать свои коварные намерения.

В условиях быстро меняющегося цифрового мира, защита данных клиентов и счетов стала приоритетом для многих компаний и банков. Новые методы безопасности внедряются не только финансовыми учреждениями, но и другими участниками рынка, которые активно используют информационные технологии в своей работе.

Литература

1. Хочуева Ф.А., Шугунов Т.Л., Жуков А.З., Ингушев Ч.Х. Информационная безопасность сквозь призму цифровой экономики // Современные наукоемкие технологии. 2018. № 11 (1). С. 65-71.

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

3. Ярочкин В.И. Информационная безопасность М.: Гаудеамус, 2014. 802 с.

4. Гафнер В.В. Ростов н / Д.: Феникс, 2010. 324 с.

5. Жмуров Д.В., Протасевич А.А., Костромина А.С. // Эра милосердия. Пути развития преступности // Baikal Research Journal. 2019. № 2. [Электронный ресурс]. URL: http://brj-bguep.ru/reader/article.aspx?id=23010 (дата обращения: 10.03.2024).

6. Госпрограмма «Информационное общество (2011 – 2020 годы)» // RGRU Новости. [Электронный ресурс]. URL: https://rg.ru/documents/2010/11/16/infobschestvo-site-dok.html (дата обращения: 11.03.2024).

7. Лагутин П.Д. Киберпреступность как актуальная угроза обществу // Молодой ученый. 2018. № 42 (228). С. 108-109.

8. Булай Ю.Г. Профилактика и противодействие киберпреступности, а также международным киберугрозам // Академическая мысль. 2017. № 1. С. 31-35.