УДК 338.246.87: 004.056

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: ОБЪЕКТЫ, ЭТАПЫ РАЗВИТИЯ, ФАКТОРЫ УСИЛЕНИЯ УГРОЗ В НАЧАЛЕ XXI ВЕКА

Наталья Валерьевна ВАСИЛЕНКО[1], д.э.н., профессор
Борис Геннадьевич ВАСИЛЕНКО[2], аспирант
[1]Кафедра экономики, управления и предпринимательства
Автономная некоммерческая организация высшего образования «Международный банковский институт имени Анатолия Собчака», Санкт-Петербург, Россия
Адрес для корреспонденции:
191023, Невский пр., 60. Санкт-Петербург, Россия
E-mail: nvasilenko@mail.ru
[2]Автономная некоммерческая организация высшего образования «Международный банковский институт имени Анатолия Собчака», Санкт-Петербург, Россия
Адрес для корреспонденции: 191023, Невский пр., 60. Санкт-Петербург, Россия
E-mail: dreaktor0@gmail.com

Аннотация

Актуальность исследования информационной безопасности определяется возрастанием роли информации и цифровых технологий в современной экономике и необходимостью защиты информационных объектов и критической инфраструктуры в условиях усиления геополитической напряженности. Цель исследования состояла в выявлении динамики характеристик объектов информационной безопасности, этапов развития информационной безопасности, а также факторов усиления угроз информационной безопасности в современный период. Для получения результатов исследования были применены общенаучные методы, а также исторический и сравнительный анализ. Разработана классификация объектов информационной безопасности и обоснована динамика их характеристик в цифровой среде. Выявлены этапы развития концепции экономической безопасности, отражающие их технологическую обусловленность. Усиление угроз информационной безопасности в начале XXI века связывается с действием таких факторов, как рост зависимости от цифровых технологий; возрастание сложности информационных систем; недостаток квалифицированных кадров; геополитические факторы; развитие киберпреступности. Направления дальнейших исследований авторы видят в развитии подходов к информационной безопасности, учитывающей цифровизацию бизнес-процессов предприятий и организаций.

Ключевые слова

Информационная безопасность, информация, информационные ресурсы, информационные системы, кибербезопасность.

UDC 338.246.87: 004.056

INFORMATION SECURITY: OBJECTS, DEVELOPMENT STAGES, FACTORS OF INCREASING THREATS AT THE BEGINNING OF THE XXI CENTURY

Natalia Valeryevna VASILENKO[1], Doctor of Economics, Professor
Boris Gennadievich VASILENKO[2], graduate student
[1]Department of Economics, Management and Entrepreneurship,
Autonomous Nonprofit Organization of Higher Education «International Banking Institute named after Anatoliy Sobchak», St. Petersburg, Russia
Address for correspondence: 191023, Russia, St. Petersburg, Nevsky pr. 60
E-mail: nvasilenko@mail.ru
[2]Autonomous Nonprofit Organization of Higher Education «International Banking Institute named after Anatoliy Sobchak», St. Petersburg, Russia
Address for correspondence: 191023, Russia, St. Petersburg, Nevsky pr. 60
E-mail: dreaktor0@gmail.com

Abstract

The relevance of information security research is determined by the increasing role of information and digital technologies in the modern economy and the need to protect information facilities and critical infrastructure in the context of increasing geopolitical tensions. The purpose of the study was to identify the dynamics of the characteristics of objects and stages of the development of information security, as well as factors of increasing threats to information security in the modern period. General scientific methods, as well as historical and comparative analysis were used to obtain the results of the study. The classification of information security objects has been developed and the dynamics of their characteristics in the digital environment has been substantiated. The stages of the development of the concept of economic security are revealed, reflecting their technological conditionality. The strengthening of threats to information security at the beginning of the XXI century is associated with the action of such factors as the growing dependence on digital technologies; the increasing complexity of information systems; the lack of qualified personnel; geopolitical factors; the development of cybercrime. The authors see the directions of further research in the development of approaches to information security, taking into account the digitalization of business processes of enterprises and organizations.

Keywords

Information security, information, information resources, information systems, cybersecurity.

Введение

Информация представляет собой важнейший ресурс любой экономической системы, без которого невозможно обеспечение ее развития. В последние десятилетия отмечается лавинообразное накопление данных, объем которых в 2022 году приблизился к уровню 97 зеттабайт и, как ожидается, удвоится к 2025

году [1]. При этом, по сведениям FSG, 90 % данных в глобальной среде имеют репликационную и распределенную природу, то есть представляют собой результат копирования и хранения корпоративных данных в нескольких местах. В результате репликации только в 2019 году, под воздействием пандемии Коронавируса-19, было сгенерировано 13,6 зеттабайт данных и в этом же году число утечек этих данных возросло на 400 % [2].

Усиление конкурентной борьбы между компаниями в глобальной цифровой среде привело к необходимости защиты различных форм и видов информации, начиная от государственных секретов и заканчивая корпоративными и личными данными. Исследования компании Positive Technologies показали, что общее число киберинцидентов в 2022 году возросло на 20,8 % по сравнению с предыдущим годом, при этом из тех атак, которые оказались успешными, 67 % имели целенаправленный характер [3]. При росте на 56 % атак на веб-ресурсы организаций в 53 % случаев это приводило к нарушению организационной деятельности.

Геополитическая напряженность последних десятилетий также способствует росту угроз в области информационной безопасности. Так, в 2022 году, по данным того же исследования [3], в результате атак нанесен ущерб государственным учреждениям (17 % от общего числа пострадавших), медицинским организациям и промышленным предприятиям (по 9 % в каждом секторе), сфере науки и образования (7 %), а также ИТ-компаниям (6 %) с последующим взломом ИТ-инфраструктуры их клиентов. В 47 % случаев кибератаки привели к утечке конфиденциальной информации организаций, в 64 % случаев – частных лиц. 12 % атак нанесли ущерб интересам государства. Приведенные данные свидетельствуют о необходимости привлечения внимания к вопросам информационной безопасности практически в каждой сфере экономической жизни.

Обзор научной литературы в рассматриваемой области показал, что О.Н. Коломыц, М.С. Геворкова и А.С. Павлова связывают актуальность развития информационной безопасности с увеличением объема корпоративных данных [4]. H. Shaikha H., A. Mazen, K. Sherah K. и T. Ramayah подчеркивают существенное влияние информационной безопасности на эффективность экономической деятельности и необходимость повышения готовности организаций к обеспечению кибербезопасности [5]. К.О. Полыхань понятие «информационная безопасность» рассматривает в контексте развития информационного общества [6], А.Ю. Румянцева и Y. Shen – с позиций информационного и цифрового суверенитетов [7; 8]. Л.Н. Мамаева

сопоставляет информационную безопасность с такими понятиями, как «компьютерная безопасность» [9], В.К. Спильниченко – «экономическая безопасность предприятия» [10]. А.З. Жуков, Ч.Х. Ингушев, А.А. Битов трактуют информационную безопасность как составляющую национальной безопасности [11], а Е.П. Гусева противопоставляет информационную безопасность понятию «информационная прозрачность» [12].

К настоящему времени в научных работах проведен исторический анализ концептуальных и практических подходов к защите информации в России [13], предложены классификации угроз информационной безопасности [14], информационных рисков и методов их анализа [15], методов обеспечения информационной безопасности [4]. Обоснованы актуальность проблемы защиты персональных данных [16], управления рисками кибербезопасности [17], а также необходимость формирования особого типа мышления в области информационной безопасности [18]. Выявлены основные направления реализации угроз информационной безопасности в условиях санкций [10].

Вместе с тем изменение внешней среды экономической деятельности ведет к появлению новых вызовов и угроз, которые в текущей ситуации связаны прежде всего с распространением цифровых технологий, меняющих задачи и методы обеспечения информационной безопасности. Кроме того, усиление геополитической напряженности и введение санкций против Российской Федерации значительно повлияло на угрозы в области информационной безопасности, что может ослабить экономический потенциал страны, отдельных отраслей и предприятий, снизить уровень жизни и защищенности российских граждан. Все это требует исследования динамических свойств основных параметров информационной безопасности, что и определило цель исследования.

Цель исследования состояла в выявлении динамики характеристик объектов информационной безопасности, этапов развития информационной безопасности, а также факторов усиления угроз информационной безопасности в современный период.

Материалы и методы

Методологическую основу исследования составили общенаучные методы, а также исторический и сравнительный анализ. Для типологизации объектов информационной безопасности применялись анализ и систематизация форм информации, циркулирующей в экономике [20]. Сравнительный анализ объектов информационной безопасности с точки зрения их формы и основного назначения использован для обоснования динамики характеристик этих

объектов в цифровой среде. Выявление этапов развития концепции экономической безопасности реализовано на основе исторического анализа развития методов защиты информации и информационных технологий [9; 10]. Определение факторов, усиливающих угрозы информационной безопасности в начале XXI века, выполнено с применением методов индукции и дедукции внешних и внутренних детерминант функционирования экономических систем в исследуемом периоде, а также обобщения и синтеза подходов к управлению угрозами информационной безопасности, существующими в научной литературе [13–18].

Материалами для получения результатов послужили научные работы российских и зарубежных авторов, посвященные изучению различных аспектов информационной безопасности, а также статистические материалы базы данных Statista и материалы аналитических исследований ИТ-компаний [1–3].

Под информационной безопасностью понималась теория и практика предотвращения несанкционированного доступа, раскрытия, искажения, изменения, использования или уничтожения информации. [19]. Проблема информационной безопасности заключалась в угрозах и рисках, связанных с использованием информации в качестве важнейшего экономического ресурса.

Результаты

Типологизация и эволюция объектов информационной безопасности в цифровой среде

Информация как знание технологии возделывания сельскохозяйственных культур, возведения построек и секреты различных ремесел во все времена имела существенное значение. По мере развития научно-технического прогресса ценность информации возрастала и ее роль в экономике непрерывно расширялась. Эти процессы продолжаются и в наши дни.

Исследование показало, что все формы информации, циркулирующей в экономике, можно разделить на три группы в зависимости от роли информации в экономическом процессе (таблица 1).

Таблица 1 – Формы информации, циркулирующей в экономике

№ п\п	Форма	Назначение	Пример
1. Роль информации как ресурса			
1	Данные: факты, цифры, статистика	Анализ и принятие решений	Финансовая отчетность компаний, статистика рынка, демографические данные

2	Большие данные	Выявление тенденций, разработка стратегий	Наборы трансакционных данных о бизнес-процессах и поведении потребителей
3	Знания, в том числе экспертные	Разработка продуктов и услуг, обучение персонала	Проектная и технологическая документация, программы обучения
4	Интеллектуальная собственность	Продажа в виде лицензии или организация бизнеса	Авторские права, патенты, товарные знаки и т.п.
2. Роль информации как результата			
1	Управленческие решения различных уровней	Обеспечение результативного управления экономическими системами	Стратегии, политики, планы, прогнозы корпоративного и регионального развития
2	Программное обеспечение	Обработка, хранение и передача информации	Текстовые и графические редакторы, интернет-браузеры и т.п.
3	Информационные продукты в традиционной форме	Удовлетворение деловых, образовательных и др. потребностей	Книги, журналы, буклеты, аналитические отчеты и др.
4	Цифровой контент	Онлайн-торговля	Музыка, фильмы, электронные книги и т.п.
3. Роль информации, формирующей рынок			
1	Рынок интеллектуальной собственности	Трансфер и диффузия инноваций	Покупка и продажа лицензий на изобретения, авторские произведения и т.д.
2	Рынок информационных продуктов	Купля-продажа информационных товаров в традиционной и цифровой форме	Рынки художественной литературы, учебной литературы, научно-популярной литературы и т.п.
3	Рынок информационных услуг	Предоставление деловых и личных услуг в традиционной и цифровой форме	Рынки консалтинговых и образовательных услуг в различных областях, включая бизнес, финансы, медицину и многое другое.
4	Рынок услуг в сфере медиа и развлечений	Предоставление доступа к контенту, такому как фильмы, музыка, видеоигры, новости и т.п.	Рынки услуг СМИ, кинотеатров, музыкальных, игровых сервисов и т.п.
5	Рынок данных, включая большие данные и статистики	Купля-продажа наборов данных для их последующей аналитики	Различные виды статистических отчетов и рыночных исследований

6	Рынок коммуникационных услуг	Обеспечение передачи информации между абонентами	Рынки услуг интернет-провайдеров, мобильных операторов и телекоммуникационных компаний
7	Рынок информационных технологий и программного обеспечения	Обеспечение обработки, хранения и передачи информации	Рынки компьютерного оборудования, рынки программных продуктов, включая услуги сопровождения
8	Рынок инфраструктурных услуг в сфере хранения данных	Обеспечение хранения информации различных пользователей	Рынки облачных услуг, рынки услуг центров обработки данных (ЦОДов)
9	Рынок в сфере информационной безопасности и кибербезопасности	Обеспечение защиты информации и данных	Рынки аппаратных средств защиты, рынки программных средств защиты

Источник: составлено авторами с использованием материалов [20].

В конце XX – начале XXI вв. информация во всех своих формах стала критическим ресурсом для различных отраслей и экономики в целом, а ее эффективное использование и защита – ключевыми аспектами успешной экономической деятельности. Отсюда все обозначенные в таблице 1 формы информации представляют собой объекты информационной безопасности. При этом следует отметить две тенденции в изменении характеристик таких объектов:

- постепенный переход носителя информации из материальной в цифровую форму, облегчающий тиражирование и создающий дополнительные угрозы в области регулирования доступа и целостности;

- возрастающий объем, прежде всего за счет трансакционных наборов данных, повышающий требования к обработке и хранению информации.

Как показывают данные таблицы 1, в контексте информационной безопасности можно выделить два вида информационных рынков:

- опосредованные цифровыми технологиями частично, предлагающие продукты и услуги как в традиционной, так и в цифровой форме в зависимости от предпочтений потребителя (№№ 1–5);

- сформировавшиеся под потребности, связанные с различными действиями с данными и информацией (№№ 6–9).

На рынках первой группы в современных условиях внимание фокусируется прежде всего на обеспечении конфиденциальности данных. Рынки, отнесенные ко второй группе, также связаны с предоставлением услуг по защите данных и информации от несанкционированного доступа, а также нарушения целостности.

Основные этапы развития концепции информационной безопасности и их технологическая обусловленность

Концепция информационной безопасности и ее развитие прошли несколько этапов, отражающих изменения в технологиях и понимании угроз. Обобщение существующих подходов позволило выделить пять этапов.

Первый этап – докомпьютерный (до 1960-х годов). На первом этапе большинство данных обрабатывалось и хранилось на бумаге или в механических устройствах, а основное внимание уделялось физической их безопасности. Для защиты от пожаров и наводнений применялись сейфы, пожарные системы и системы для обнаружения соответствующих угроз. Для предотвращения физических краж документов или оборудования, на котором хранились данные, использовали охрану, видеонаблюдение, контроль доступа к документам и помещениям, а также машины для уничтожения бумаг и документов до нечитаемого уровня. Для передачи или перевозки важных бумажных документов или магнитных носителей данных применяли шифрование данных и защищенные транспортные средства.

С развитием компьютеров и цифровых технологий многие из этих мер были адаптированы и интегрированы в современные информационные системы для обеспечения безопасности данных. Следует отметить, что до наших дней физическая безопасность информации и данных не потеряла своей актуальности.

Второй этап – компьютерной обработки данных (1960–1970-е годы). На втором этапе автоматизация обработки данных предполагала применение аппаратных средств и соответствующих физических сред, где хранилась информация, которой и требовалась защита.

Для решения этой задачи в этот период было разработано несколько важных методов управления доступом, определяющих, кто и как может получать доступ к данным и ресурсам информационных систем. Среди наиболее распространенных методов управления доступом можно выделить:

- матрицу управления доступом (Access Control Matrix), в которой строки представляли субъектов информационной безопасности (пользователей или процессы), столбцы – объекты информационной безопасности (ресурсы или

файлы), а содержание ячейки указывало, какой доступ (чтение, запись и т. д.) разрешен или запрещен для данного субъекта к данному объекту;

- дискреционное управление доступом (Discretionary Access Control, DAC), позволяющее владельцам информационных ресурсов на пользовательском уровне устанавливать правила доступа, например, к чтению какой-либо записи или удалению какого-либо файла;

- мандатное управление доступом (Mandatory Access Control, MAC), основанное на классификации объектов и субъектов информационной безопасности для их распределения по уровням секретности;

- ролевое управление доступом (Role-Based Access Control, RBAC), при котором доступ предоставляется на основе назначаемых субъектам информационной безопасности ролей, предполагающих определенные права доступа;

- управление доступом через базы данных (Database Access Control, DBMS), определяющее на системном уровне, какие пользователи или приложения к каким данным имеют доступ в базе данных.

Рассмотренные методы управления доступом стали важными шагами в обеспечении конфиденциальности данных и безопасности информационных систем. Эти методы послужили основой для развития современных подходов и технологий управления доступом, которые активно используются в организациях для защиты информации в настоящее время.

В 1970-х годах была разработана тройственная модель информационной безопасности, также известная как концепция «Конфиденциальность – целостность – доступность» (Confidentiality – Integrity – Availability, CIA), которая служит основой для определения целей и принципов обеспечения безопасности информации и в наши дни. Конфиденциальность информации означает, что только авторизованные пользователи имеют право доступа к этой информации, что предотвращает несанкционированный доступ к данным. Для обеспечения конфиденциальности используются методы шифрования, управления доступом и другие меры. Целостность информации гарантирует, что данные не изменяются несанкционированным образом. Целостность информации обеспечивается посредством контрольных сумм, хэшированием и другими методами. Доступность информации подразумевает, что информация доступна для авторизованных пользователей тогда, когда им это необходимо. Для обеспечения доступности информации используются меры по обеспечению надежности систем и сетей, резервированию и восстановлению данных.

Конфиденциальность, целостность и доступность, образуя основу мер безопасности информации, помогают выявить соответствующие угрозы и риски.

Концепция CIA со временем дополнялась другими аспектами информационной безопасности, такими как аутентификация, авторизация, аудит и невозможность отказа в обслуживании (DDoS), что позволило обеспечить более высокий уровень информационной безопасности.

В этот период происходило активное развитие теории, методик и средств обеспечения безопасности компьютерной и информационных систем, среди которых можно назвать:

- алгоритмы шифрования данных, например, Data Encrytion Standard (DES);

- антивирусные программы, например, первую антивирусную программу Creeper, разработанную Реймондом Томлинсоном для удаления сетевых «червей» с компьютеров;

- межсетевые экраны (брандмауэры) и средства мониторинга сетевого трафика для выявления несанкционированных действий и др.

Эти и другие достижения в области безопасности компьютеров и информационных систем стали отправной точкой для дальнейшего развития технологий и методов обеспечения безопасности в современных цифровых средах.

Третий этап – стандартизация в сфере информационной безопасности (1980–2000-е годы). На третьем этапе стандарты и нормативы в области информационной безопасности стали важным направлением по обеспечению безопасности информации, помогая организациям в разработке структурированных и систематических подходов к обеспечению конфиденциальности, целостности и доступности данных.

Наиболее известными и широко применяемыми стандартами являются:

- «ISO/IEC 27001: Управление информационной безопасностью», устанавливающий требования к системе управления информационной безопасностью в организации, описывающий процесс управления рисками, внедрение мер по обеспечению безопасности и др. аспекты;

- «ISO/IEC 27002: Практические рекомендации по управлению информационной безопасностью», представляющий рекомендации по конкретным мерам информационной безопасности в соответствии с требованиями ISO/IEC 27001;

- «PCI DSS (Стандарт безопасности данных индустрии платежных карт»), разработанный для обеспечения безопасности данных платежных карт и

требующий, чтобы организации, принимающие платежи кредитными картами, соблюдали определенные меры безопасности, и др.

Эти стандарты играют важную роль в обеспечении безопасности информации и данных как на уровне организации, так и на глобальном уровне. Они также способствуют созданию общих рамок и распространению лучших практик в области информационной безопасности.

В России в указанный период также наблюдается активный процесс стандартизации в сфере информационной безопасности. Технические требования к информационным системам и средствам защиты информации содержатся, например, в ГОСТ Р 34.10. «Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защиты информации. Процессы формирования и проверки электронной цифровой подписи» (2001). Требования к обработке и защите информации установлены в Федеральном законе «О персональных данных» (2006), Федеральном законе «Об информации, информационных технологиях и о защите информации» (2006) и др. Национальной версией ISO/IEC 27001 является ГОСТ Р ИСО/МЭК 27001 «Информационная технология. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования» (2006). В настоящее время действуют обновленные версии указанных документов.

Четвертый этап – развитие интернета и рост киберугроз (2000–2010-е годы). На четвертом этапе концепции информационной безопасности включают в себя не только технические меры, но и обучение сотрудников в сфере кибербезопасности и кибергигиены, в том числе при помощи специализированных компаний по кибербезопасности.

В соответствии с подходами к информационной безопасности рассматриваются периода организации:

- проводят оценку рисков, чтобы определить уязвимости и угрозы, а также разработать стратегии по их снижению;

- разрабатывают политики и процедуры в области информационной безопасности, которые включают в себя правила доступа, шифрование данных и другие меры защиты;

- устанавливают системы мониторинга, которые следят за активностью в сети и на компьютерных устройствах для выявления аномалий и потенциальных инцидентов;

- регулярно обновляют программное обеспечение и устраняют уязвимости с помощью специальных программ и обновлений;

- соблюдают требования законодательства и стандартов в области информационной безопасности, таких как GDPR в Европе или HIPAA в США, в том числе при работе с конфиденциальными личными данными.

В рассматриваемый период формируется комплексный подход к кибербезопасности, который включает в себя технические, организационные и образовательные аспекты. Соблюдение всех указанных ранее мер позволяет организациям эффективно защищать свои данные и информацию от киберугроз.

Пятый этап – распространение сквозных технологий цифровой экономики (2010-е годы – настоящее время). На пятом этапе с появлением облачных вычислений, интернета вещей (IoT), искусственного интеллекта и других технологических инноваций область информационной безопасности становится все более широкой и сложной. Концепция информационной безопасности этого этапа включает в себя не только технические меры, обучение персонала, но и управление рисками, соблюдение нормативов и многие другие аспекты.

Это связано с тем, что новые технологии могут быть использованы как для усиления информационной безопасности, так и для развития киберпреступности. Так, с развитием технологий обработки больших данных и искусственного интеллекта (ИИ), возникли не только новые средства для обнаружения и предотвращения угроз, но и новые методы для проведения кибератак (таблица 2).

Таблица 2 – Применение искусственного интеллекта (ИИ) и машинного обучения (МО) в контексте информационной безопасности (ИБ)

№ п/п	Задача в области ИБ	Способ решения задачи при помощи МО и ИИ
Повышение уровня информационной безопасности		
1	Обнаружение вторжений	Анализ трафика и выявление аномальных или вредоносных активностей системами интранет-детекторов и системами предотвращения трансакций
2	Обнаружение мошенничества	Анализ финансовых данных и транзакций с целью выявления несанкционированных транзакций
3	Получение сведений от кибер разведки	Автоматический анализ данных из социальных сетей, а также новостных статей и сообщений с целью выявления потенциальных угроз и трендов
4	Мониторинг угроз ИБ	Анализ больших объектов данных с целью определения состояния потенциальных и новых угроз, что помогает быстрее реагировать на новые виды атак

5	Реакция при реализации угроз ИБ	Автоматическая реакция на киберинциденты, например, блокировка доступа к уязвимым системам или изоляция скомпроментированных устройст
Снижение уровня информационной безопасности		
1	Повышение эффективности кибератак	Автоматизация атак, таких как фишинг-кампании, атаки на веб-приложения и генерация вредоносных программ, например, при помощи ботов
2	Ослабление защитных свойств системы ИБ	Создание атакующих алгоритмов, которые адаптируются к защите и изменяют свое поведение, чтобы избегать обнаружения

Источник: составлено авторами с использованием материалов [20].

Кроме того, с развитием квантовых компьютеров возникли новые угрозы для криптографии, а значит и информационной безопасности в целом. Все это подчеркивает необходимость постоянного совершенствования систем безопасности и мониторинга новых технологических разработок для эффективного обнаружения и противодействия угрозам в современном мире.

Усиление угроз информационной безопасности в начале XXI века

Исследование этапов развития информационной безопасности и подходов к ее обеспечению подтверждает, что в силу непрерывного изменения угроз информационная безопасность является чрезвычайно динамичной областью. Можно выделить несколько факторов, которые усиливают проблему информационной безопасности в последние десятилетия:

- рост зависимости от технологий, прежде всего цифровых;
- возрастание сложности информационных систем;
- недостаток квалифицированных кадров;
- геополитические факторы;
- развитие киберпреступности.

Действие первых трех факторов обусловлено научно-техническим прогрессом и информационным развитием, имеющими следствием изменение структуры спроса на рабочую силу, и следует ожидать, что их влияние в ближайшем периоде будет только усиливаться. Остановимся на этих факторах более подробно.

С появлением новых технологий, таких, как интернет вещей (IoT), облачные вычисления, искусственный интеллект и мобильные устройства, компании и организации становятся все более зависимыми от цифровых ресурсов и данных. Цифровизация бизнес-процессов означает, что все больше бизнес-операций выполняется с использованием цифровых технологий и

хранится в электронной форме на удаленных сервисах. Это создает большой объем ценной информации, которая становится объектом киберугроз. Развитие онлайн-торговли и электронных платежей означает, что финансовые транзакции и личные данные клиентов становятся доступными для киберпреступников, что может привести к серьезным финансовым потерям, а также потере доверия к компаниям со стороны клиентов.

Рост числа устройств IoT приводит к усложнению компьютерных сетей и информационных систем, что делает их более уязвимыми. Кибератаки на IoT-устройства могут иметь серьезные последствия, включая нарушение работы критической инфраструктуры. Применение мобильных устройств расширяет возможности доступа к корпоративным данным и онлайн-сервисам, но в то же время повышает их уязвимость для киберугроз. Обработки и анализ больших данных и использованием искусственного интеллекта могут использоваться как для обнаружения угроз, так и для их нейтрализации, что представлено в таблице 2.

Современные информационные ресурсы и системы, состоящие из множества компонентов, включая серверы, сети, базы данных, приложения и другие элементы, становятся все более сложными и взаимосвязанными, что затрудняет мониторинг и обнаружение угроз.

Новые точки уязвимости в сложных информационно-компьютерных системах могут возникать:

- при интеграции в корпоративные информационные системы сторонних решений и сервисов, особенно если сторонние поставщики не обеспечивают должный уровень безопасности;

- в условиях охвата больших территорий и наличия множества точек доступа;

- при настройке ролей и прав доступа для большого количества неоднородных пользователей, включая сотрудников организации, клиентов и представителей других заинтересованных сторон;

- в ситуации неоднородности среды при использовании различных платформ, операционных систем и технологий, а также различных версий программного обеспечения, что создает сложности в управлении едиными политиками безопасности и может оставить уязвимости незамеченными;

- в условиях реализации внутренних угроз со стороны персонала, возникающих из-за его недостаточной квалификации и внимательности.

Указанные уязвимости могут быть использованы киберпреступниками для кибератак. При этом угрозы могут исходить из любой точки мира и причинить ущерб экономической деятельности в любой стране.

Для борьбы с угрозами информационной безопасности в условиях усиления зависимости от технологий и роста сложности информационных систем организации должны принимать комплексные меры, включая улучшение киберзащиты, обучение сотрудников, мониторинг угроз и разработку планов реагирования на инциденты. Это важно для обеспечения устойчивости экономической деятельности и защиты ценной информации.

Особенно актуальной задачей становится обучение сотрудников, так как существующий в настоящее время дефицит квалифицированных специалистов по информационной безопасности приводит к недостаточности ресурсов для борьбы с угрозами.

Для решения проблемы недостатка квалифицированных кадров в области информационной безопасности организации могут предпринимать следующие меры:

- инвестиции в обучение и повышение квалификации имеющихся сотрудников;

- сотрудничество с учебными заведениями и институтами для подготовки будущих специалистов по информационной безопасности;

- сотрудничество с внешними поставщиками услуг по безопасности, если внутренние ресурсы ограничены.

Любое государство для защиты своих национальных интересов организует работу разведывательных служб, деятельность которых имеет информационную основу и связана с такими методами, как шпионаж и проч. Однако в периоды геополитической напряженности усилить проблемы информационной безопасности могут:

- кибершпионаж для сбора разведывательной информации о других странах, корпорациях и гражданах, что может привести к утечке чувствительных данных и нарушению конфиденциальности информации;

- информационные войны, в которых государства могут использовать информационные ресурсы и социальные сети для распространения дезинформации с целью воздействия на общественное мнение и дестабилизации политической ситуации в других странах;

- киберконфликты и кибервойны, которые возникают при переносе политических конфликтов между странами в киберпространство, где

государства могут проводить кибератаки на критическую информационную инфраструктуру друг друга;

- кибератаки, сопровождающие политические санкции и контрсанкции, а также совершаемые состороны неформальных групп и хактивистов, действующих по политическим мотивам.

Политические и геополитические факторы могут создавать дополнительные вызовы, что подчеркивает важность международного сотрудничества и разработки стратегий управления рисками в условиях геополитической нестабильности.

Киберпреступники не всегда имеют политические мотивы для своей деятельности, гораздо чаще их противоправные действия совершаются с целью личной наживы. Киберпреступления связаны с использованием компьютерных систем, информационных технологий и интернета. Преступления такого рода предполагают осуществление несанкционированного доступа, модификацию, уничтожение, кражу или финансовые махинации, а также другие виды атак, направленных на компьютерные сети, электронные устройства и данные.

Примерами киберпреступлений являются:

- создание и распространение компьютерных вирусов, шпионских программ и других видов вредоносного программного обеспечения с целью заражения индивидуальных или корпоративных компьютеров и уклонения от обнаружения;

- атаки на финансовые институты, банки, платежные онлайн-системы и криптовалютные биржи с целью кражи денег;

- обман пользователей при помощи представления киберпреступников в качестве легитимных организаций или лиц с целью получения конфиденциальной информации, такой как пароли и данные банковских счетов (фишинг);

- мошенничество с кредитными картами, продажа фальшивых товаров или услуг и др.;

- размещение ложной информации, а также атаки на государственные и общественные ресурсы с целью создания паники или дискредитации (кибертерроризм);

- шифрование данных пользователя с последующим требованием выкупа для их разблокировки;

- незаконный сбор разведывательной информации, в том числе конфиденциальной информации, такой как медицинские записи, бизнес-данные,

объекты интеллектуальной собственности, государственные секреты (кибершпионаж).

Киберпреступники могут использовать методы социальной инженерии для манипуляции сотрудниками и получения доступа к системам.

Международный характер киберпреступности усложняет процесс выявления и привлечения к ответственности злоумышленников. Кроме того, киберпреступники быстро адаптируются к новым методам защиты и постоянно совершенствуют свои атаки.

В целом киберпреступность представляет серьезную угрозу для организаций, государств и частных лиц, и борьба с ней требует множества мер и технических и организационных решений, включая кибербезопасность, обучение персонала и законодательные меры.

Выводы

В результате проведенного исследования объекты информационной безопасности, к которым авторы отнесли все формы информации, циркулирующей в экономике, были разделены на три группы в зависимости от роли информации в экономическом процессе. Анализ форм и назначения объектов информационной безопасности в рамках ресурсной и результативной ролей информации позволил выявить две тенденции, определяющие динамику характеристик объектов информационной безопасности: изменение формы носителя, создающее дополнительные угрозы в области регулирования доступа и целостности, а также возрастающий объем информации за счет трансакционных наборов данных, повышающий требования к их обработке и хранению.

В рамках третьей роли информации (формирующей рынки) такие рынки были разделены в контексте проводимого исследования на два вида: осуществляющие обеспечение конфиденциальности данных (интеллектуальной собственности, информационных продуктов и услуг и т.д.) и фокусирующиеся на защите данных и информации от несанкционированного доступа и нарушения целостности (коммуникационных услуг, информационных технологий и программного обеспечения, инфраструктурных услуг в сфере хранения данных, а также в сфере информационной и кибербезопасности).

Определены пять этапов развития концепции экономической безопасности, отражающих технологическую обусловленность появления новых вызовов и угроз, связанную с развитием компьютерного оборудования, коммуникационных и информационных систем, а также автоматизацией методов шифровая информации.

Выявлены факторы, стимулирующие возникновение и реализацию угроз информационной безопасности в начале XXI века. К таким факторам отнесены: рост зависимости от цифровых технологий; возрастание сложности информационных систем; недостаток квалифицированных кадров; геополитические факторы; развитие киберпреступности.

Показано, что влияние первых трех факторы, обусловленных технологическим и инновационным развитием, будет только усиливаться, и предложен ряд мер противодействия соответствующим угрозам.

Заключение

Проведенное исследование подтверждает высокую динамичность информационной безопасности на уровне ее объектов, угроз и способы обеспечения. Существенное влияние информационной безопасности на экономическую деятельность на всех уровнях современной экономики, технологическая обусловленность усложнения систем информационной безопасности, а также усиление геополитической напряженности, стимулирующее информационные войны и кибератаки на критическую инфраструктуру требуют непрерывного совершенствования и развития теории и практики информационной безопасности.

Современная информационная безопасность, являясь непрерывным процессом, предполагает постоянный мониторинг и адаптацию к новым угрозам и вызовам, что может быть реализовано только с помощью интегрированного подхода, включающего технологические, организационные и человеческие аспекты. Серьезнейшей проблемой в области информационной безопасности в настоящее время является недостаток кадров. Исследование позволило подтвердить, что решение этой проблемы требует совместных усилий со стороны государства, организаций и общества, а также международное сотрудничество.

Направление дальнейших исследований авторы видят в развития теоретических и практических подходов к обнаружению и выработке мер по нейтрализации вызовов и угроз, связанных с цифровизацией бизнес-процессов предприятий и организаций.

Список источников

1. Positive Technologies. Актуальные киберугрозы: итоги 2022 года. Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022/ (дата обращения: 22.10.2023).
2. Statista. Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2020, with forecasts from 2021 to 2025. Available

at: https://www.statista.com/statistics/871513/worldwide-data-created/ (дата обращения: 22.10.2023).
3. FSG. Big Data Statistics 2023: How Much Data is in The World?. Available at: https://firstsiteguide.com/big-data-stats/ (дата обращения: 22.10.2023).
4. **Коломыц О.Н., Геворкова М.С., Павлова А.С.** Методы управления информационной безопасностью предприятия // Инновационная экономика: перспективы развития и совершенствования. – 2020. – № – 6 (48). – С. 44–50. doi: 10.47581/2020/10.23.PS85/IE/5.48.007.
5. **Shaikha H., Mazen A., Sherah K., Ramayah T.** Evaluating the cyber security readiness of organizations and its influence on performance // Journal of Information Security and Applications. – 2021. – Vol. 58. –№102726. doi: 10.1016/j.jisa.2020.102726.
6. **Полыхань К.О.** Проблемы и особенности состояния информационной безопасности в соответствии с доктриной информационной безопасности Российской Федерации // Устойчивое развитие науки и образования. – 2019. – № 5. – С. 154–160.
7. **Василенко Н.В., Румянцева А.Ю.** Формирование информационного суверенитета государства в условиях цифровизации экономики: технологическая и ценностная составляющие // Экономика и управление. – 2022. – Т. 28. – № 10. – С. 1051–1063. http://doi.org/10.35854/1998-1627-2022-10-1051-1063.
8. **Shen Y.** Cyber Sovereignty and the Governance of Global Cyberspace // Chinese Political Science Review. – 2016. – Vol. 1. – P. 81–93.
9. **Мамаева Л.Н.** Характерные проблемы информационной безопасности в современной экономике // Информационная безопасность регионов. – 2016. – № 1 (22). – С. 21–24.
10. **Спильниченко В.К.** Влияние сферы информационных технологий на экономическую безопасность государства и личности в новых реалиях // Наука и искусство управления / Вестник Института экономики, управления и права Российского государственного гуманитарного университета. – 2022. – № 3. – С. 53–68. Doi: 10.28995/2782-2222-2022-3-53-68.
11. **Жуков А.З., Ингушев Ч.Х., Битов А.А.** Информационная безопасность как элемент национальной безопасности Российской Федерации // Проблемы экономики и юридической практики. – 2021. – Т. 17. – № 1. – С. 278–283.
12. **Гусева Е.П.** Менеджмент: аспекты информационной безопасности, прозрачности и доверия к информации // Экономика, статистика и информатика. – 2012. – №5. – С. 173.
13. **Никулин В.В.** Исторические аспекты развития информационной безопасности в системе национальной безопасности Российской Федерации // Вестник образовательного консорциума Среднерусский

университет. Информационные технологии. – 2022. – № 2 (20). – С. 18–22.
14. **Николаева М.О.** Информационная безопасность: современная картина проблемы информационной безопасности и защиты информации // Мониторинг. Образование. Безопасность. – 2023. – Т. 1. – № 1. – С. 51–57.
15. **Шайкинов А.Ж., Курманбекова А.К., Юсупова А.Ю.** Анализ рисков информационной безопасности // Современные проблемы механики. – 2020. – № 39 (1). – С. 56–62.
16. **Saglam R.B., Nurse J.R.C., Hodges D.** Personal information: Perceptions, types and evolution // Journal of Information Security and Applications. – 2022. – Vol. 66. – №103163. Doi: 10.1016/j.jisa.2022.103163.
17. **Parkin S., Kuhn K., Shaikh S.A.** Executive decision-makers: a scenario-based approach to assessing organizational cyber-risk perception // Journal of Cybersecurity. – 2023. – Vol. 9. – N. 1. – tyad018, doi: 10.1093/cybsec/tyad018.
18. **Schoenmakers K., Greene D., Stutterheim S., Lin H., Palmer M.J.** The security mindset: characteristics, development, and consequences // Journal of Cybersecurity. – 2023. – Vol. 9. – N. 1. – tyad010. Doi: 10.1093/cybsec/tyad010.
19. **Селезнев Е.А., Горбунова О.А.** Сущность информационной безопасности и ее место в обеспечении экономической безопасности предприятия // Вестник Самарского муниципального института управления. – 2022. – № 1. – С. 36–44.
20. Цифровая трансформация экономических систем: проблемы и перспективы (ЭКОПРОМ-2022) : сборник трудов Всероссийской научно-практической конференции с зарубежным участием, 11–12 ноября 2022 г. / Под ред. д-ра экон. наук, проф. Д. Г. Родионова, д-ра экон. наук, проф. А. В. Бабкина. – СПб. : ПОЛИТЕХ-ПРЕСС, 2022. – 819 с.

References

1. Positive Technologies. Current cyber threats: the results of 2022. Available at: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022/ (accessed: 22.10.2023).
2. Statista. Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2020, with forecasts from 2021 to 2025. Available at: https://www.statista.com/statistics/871513/worldwide-data-created/ (accessed: 22.10.2023).
3. FSG. Big Data Statistics 2023: How Much Data is in The World? Available at: https://firstsiteguide.com/big-data-stats/ (accessed:22.10.2023).
4. **Kolomyc O.N., Gevorkova M.S., Pavlova A.S.** Metody upravleniya informacionnoj bezopasnost'yu predpriyatiya // Innovacionnaya ekonomika:

perspektivy razvitiya i sovershenstvovaniya. – 2020. – № – 6 (48). – S. 44–50. Doi: 10.47581/2020/10.23.PS85/IE/5.48.007.

5. **Shaikha H., Mazen A., Sherah K., Ramayah T.** Evaluating the cyber security readiness of organizations and its influence on performance // Journal of Information Security and Applications. – 2021. – Vol. 58. –№102726. Doi: 10.1016/j.jisa.2020.102726.
6. **Polyhan' K.O.** Problemy i osobennosti sostoyaniya informacionnoj bezopasnosti v sootvetstvii s doktrinoj informacionnoj bezopasnosti Rossijskoj Federacii // Ustojchivoe razvitie nauki i obrazovaniya. – 2019. – № 5. – S. 154–160.
7. **Vasilenko N.V., Rumyanceva A.YU.** Formirovanie informacionnogo suvereniteta gosudarstva v usloviyah cifrovizacii ekonomiki: tekhnologicheskaya i cennostnaya sostavlyayushchie // Ekonomika i upravlenie. – 2022. – T. 28. – № 10. – S. 1051–1063. http://doi.org/10.35854/1998-1627-2022-10-1051-1063.
8. **Shen Y.** Cyber Sovereignty and the Governance of Global Cyberspace // Chinese Political Science Review. – 2016. – Vol. 1. – P. 81–93.
9. **Mamaeva L.N.** Harakternye problemy informacionnoj bezopasnosti v sovremennoj ekonomike // Informacionnaya bezopasnost' regionov. – 2016. – № 1 (22). – S. 21–24.
10. **Spil'nichenko V.K.** Vliyanie sfery informacionnyh tekhnologij na ekonomicheskuyu bezopasnost' gosudarstva i lichnosti v novyh realiyah // Nauka i iskusstvo upravleniya / Vestnik Instituta ekonomiki, upravleniya i prava Rossijskogo gosudarstvennogo gumanitarnogo universiteta. – 2022. – № 3. – S. 53–68. Doi: 10.28995/2782-2222-2022-3-53-68.
11. **ZHukov A.Z., Ingushev CH.H., Bitov A.A**. Informacionnaya bezopasnost' kak element nacional'noj bezopasnosti Rossijskoj Federacii // Problemy ekonomiki i yuridicheskoj praktiki. – 2021. – T. 17. – № 1. – S. 278–283.
12. **Guseva E.P.** Menedzhment: aspekty informacionnoj bezopasnosti, prozrachnosti i doveriya k informacii // Ekonomika, statistika i informatika. – 2012. – №5. – S. 173.
13. **Nikulin V.V.** Istoricheskie aspekty razvitiya informacionnoj bezopasnosti v sisteme nacional'noj bezopasnosti Rossijskoj Federacii // Vestnik obrazovatel'nogo konsorciuma Srednerusskij universitet. Informacionnye tekhnologii. – 2022. – № 2 (20). – S. 18–22.
14. **Nikolaeva M.O.** Informacionnaya bezopasnost': sovremennaya kartina problemy informacionnoj bezopasnosti i zashchity informacii // Monitoring. Obrazovanie. Bezopasnost'. – 2023. – T. 1. – № 1. – S. 51–57.
15. **SHajkinov A.ZH., Kurmanbekova A.K., YUsupova A.YU**. Analiz riskov informacionnoj bezopasnosti // Sovremennye problemy mekhaniki. – 2020. – № 39 (1). – S. 56–62.

16. **Saglam R.B., Nurse J.R.C., Hodges D.** Personal information: Perceptions, types and evolution // Journal of Information Security and Applications. – 2022. – Vol. 66. – №103163. Doi: 10.1016/j.jisa.2022.103163.
17. **Parkin S., Kuhn K., Shaikh S.A.** Executive decision-makers: a scenario-based approach to assessing organizational cyber-risk perception // Journal of Cybersecurity. – 2023. – Vol. 9. – N. 1. – tyad018, doi: 10.1093/cybsec/tyad018.
18. **Schoenmakers K., Greene D., Stutterheim S., Lin H., Palmer M.J.** The security mindset: characteristics, development, and consequences // Journal of Cybersecurity. – 2023. – Vol. 9. – N. 1. – tyad010. Doi: 10.1093/cybsec/tyad010.
19. **Seleznev E.A.,** Gorbunova O.A. Sushchnost' informacionnoj bezopasnosti i ee mesto v obespechenii ekonomicheskoj bezopasnosti predpriyatiya // Vestnik Samarskogo municipal'nogo instituta upravleniya. – 2022. – № 1. – S. 36–44.
20. Digital transformation of economic systems: problems and prospects (ECOPROM-2022): proceedings of the All-Russian Scientific and Practical Conference with foreign participation, November 11-12, 2022 / Edited by Dr. D. G. Rodionov, Dr. D. G. Rodionov, Dr. A. V. Babkin. – St. Petersburg : POLYTECH-PRESS, 2022. – 819 p.