ISBN 978-5-901722-96-1

УДК 004.056

ВЛИЯНИЕ ЦИФРОВИЗАЦИИ НА РИСКИ В СФЕРЕ ИНФОРМАЦИОННОЙ И ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

Антонова Елизавета Алексеевна[1], студент
e-mail: elizavetaantonova26@yandex.ru
Лыкова Елизавета Алексеевна[2], магистрант
e-mail: lisalikova@bk.ru
Лыкова Елена Сергеевна[1], к.э.н., доцент кафедры экономики и менеджмента
e-mail: likova_elena@bk.ru

[1] Волжский государственный университет водного транспорта, Нижний Новгород, Россия
[2] Московский энергетический институт, Москва, Россия

Аннотация. Цифровые технологии проникают во все сферы: бизнес, госуправление, финансы, образование, социальные отношения. Они делают процессы эффективнее и быстрее, но также создают угрозы — поэтому подходы к безопасности нужно пересматривать. Традиционные методы защиты, основанные на контроле периметра корпоративных сетей, утрачивают эффективность, поэтому требуется переход к моделям «нулевого доверия» (Zero Trust), где доступ к ресурсам предоставляется только после непрерывной верификации идентичности и контекста безопасности каждого запроса.

Ключевые слова: цифровизация, киберугрозы, информационная безопасность, Zero Trust («нулевое доверие»), уязвимости.

THE IMPACT OF DIGITALIZATION ON RISKS IN THE FIELD OF INFORMATION AND ECONOMIC SECURITY

Elizaveta A. Antonova[1], Student
e-mail: elizavetaantonova26@yandex.ru
Elizaveta A. Lykova[2], Master's Degree student
e-mail: lisalikova@bk.ru
Elena S. Lykova[1], Candidate of Economic Sciences, Associate Professor at the Department of Economics and Management
e-mail: likova_elena@bk.ru

[1] Volga State University of Water Transport, Nizhny Novgorod, Russia
[2] Moscow Power Engineering Institute, Moscow, Russia

Abstract. Digital technologies are penetrating all spheres: business, public administration, finance, education, and social relations. They make processes more efficient and faster, but also create threats — which is why security approaches need to be reconsidered. Traditional methods of protection based on controlling the perimeter of corporate networks are losing effectiveness, so a transition to

«zero trust» (Zero Trust) models is required, where access to resources is granted only after continuous verification of the identity and security context of each request.

Keywords: digitalization, cyber threats, information security, Zero Trust, vulnerabilities.

Цифровая трансформация охватывает сегодня все сферы жизни: бизнес, государственное управление, финансы, образование и социальные отношения. Внедрение цифровых технологий повышает эффективность, ускоряет процессы и открывает новые возможности, однако одновременно порождает ранее неизвестные угрозы. Кибератаки, утечки данных, автоматизированное мошенничество и сбои цифровой инфраструктуры становятся не просто техническими проблемами, а факторами, напрямую влияющими на экономическую стабильность предприятий и государства. Привычные методы защиты, основанные на контроле периметра корпоративных сетей, утрачивают эффективность. В этих условиях требуется пересмотр подходов к оценке рисков и построению систем информационной и экономической безопасности.

1. Цифровизация как драйвер трансформации среды безопасности

Под цифровизацией понимается внедрение цифровых технологий в различные виды деятельности — от производства и логистики до банковского обслуживания и здравоохранения. Её влияние на безопасность имеет двойственную природу.

Позитивные изменения:

— Повышение ситуационной осведомлённости. Системы видеонаблюдения с элементами искусственного интеллекта, датчики и средства автоматического контроля позволяют фиксировать инциденты в реальном времени и собирать данные, необходимые для прогнозирования развития событий.

— Интеграция служб безопасности. Цифровые платформы объединяют разрозненные подразделения и ведомства, сокращая время обмена информацией с часов до секунд и обеспечивая синхронность действий при инцидентах.

— Автоматизация рутинных процессов. Управление доступом, регистрация событий, создание резервных копий — всё это снижает нагрузку на персонал и сокращает число ошибок, связанных с человеческим фактором.

Негативные последствия и вызовы:

— Усложнение киберугроз. Злоумышленники активно используют облачные сервисы, интернет вещей (IoT) и технологии искусственного интеллекта. Программы-вымогатели (Ransomware) превратились в полноценную индустрию с моделью «атака как услуга» (RaaS).

— Появление новых уязвимостей. Широкое распространение «умных» устройств, развёртывание сетей 5G, переход на квантовые вычисления создают риски, которые невозможно устранить с помощью классических межсетевых экранов и антивирусов.

— Человеческий фактор остаётся критическим. Социальная инженерия, фишинг и подкуп сотрудников остаются одними из самых действенных инструментов атакующих. Любое цифровое нововведение бесполезно, если работник раскрывает пароль по телефону «техподдержки».

2. Почему традиционные подходы к защите перестают быть эффективными

Долгое время безопасность строилась на концепции «защищённого периметра»: внешняя граница корпоративной сети тщательно контролировалась, а всё, что находилось внутри, считалось доверенным. Однако такая модель перестала отвечать современным требованиям по нескольким причинам.

Размывание границ. Облачные сервисы, удалённая работа, мобильные устройства и цифровые экосистемы партнёров стирают чёткую границу между «внутренним» и «внешним». Теперь данные и приложения могут находиться где угодно, и контролировать каждое подключение традиционными средствами невозможно.

Рост сложности и скорости атак. Современные кибератаки часто бывают многоэтапными и используют методы, которые не выявляются сигнатурными антивирусами. Злоумышленники действуют в автоматическом режиме, сканируя уязвимости и адаптируясь к защите.

Объём данных. Для выявления инцидента необходимо анализировать терабайты логов и событий. Человек физически не способен обработать такой массив, а старые системы мониторинга не имеют встроенных механизмов машинного обучения.

В ответ на эти вызовы мировое сообщество переходит к моделям «нулевого доверия» (Zero Trust), где ни одно устройство или пользователь не считается доверенным по умолчанию, а доступ к ресурсам предоставляется только после непрерывной верификации идентичности и контекста безопасности каждого запроса.

3. Новые виды рисков, порождённые цифровизацией

Цифровая трансформация порождает риски, выходящие далеко за рамки традиционной информационной безопасности. Их можно классифицировать следующим образом.

Киберугрозы прямого экономического действия. Это атаки с целью хищения денег (компрометация систем ДБО), вымогательство (шифровальщики), кража платёжных данных клиентов, а также DDoS-атаки, нарушающие работу интернет-магазинов и сервисов.

Цифровое неравенство. Разрыв в доступе к технологиям между разными регионами и социальными группами создаёт зоны уязвимости: часть населения оказывается исключённой из цифровых услуг, что порождает социальную напряжённость и дополнительные риски для государства.

Риски, связанные с искусственным интеллектом. Алгоритмическая предвзятость, некачественные данные обучения, а также использование ИИ для создания дипфейков и автоматизированного фишинга. Особую опасность представляет принятие значимых решений (о кредитах, трудоустройстве, медицинской помощи) на основе «чёрных ящиков» без прозрачной логики.

Институциональные и правовые риски. Законодательство зачастую отстаёт от технологий. Высокая зависимость от импортного ПО и оборудования создаёт угрозу цифрового суверенитета. Нерегулируемый оборот персональных данных и отсутствие чётких норм ответственности за киберинциденты затрудняют борьбу с преступлениями.

Социальные и этические риски. Цифровизация социальной поддержки может привести к дискриминации граждан, не владеющих технологиями. Массовый сбор данных формирует риски «цифрового рабства», когда поведение людей управляется алгоритмами без их осознанного согласия.

Риски инфраструктурной зависимости. Выход из строя центров обработки данных, сбой в работе облачного провайдера или отключение электричества могут парализовать экономику региона. Чем сильнее общество зависит от цифровых систем, тем выше ущерб от их отказа.

4. Синергия информационной и экономической безопасности

Информационная безопасность (ИБ) и экономическая безопасность (ЭБ) традиционно рассматривались как разные области. Однако цифровизация сделала их неразрывно связанными. Любой серьёзный инцидент в ИБ неминуемо влечёт экономические последствия:

— утечка коммерческой тайны приводит к потере конкурентных преимуществ и снижению выручки;

— остановка производства из-за вирусной атаки оборачивается штрафами по контрактам и упущенной прибылью;

— разглашение персональных данных влечёт крупные штрафы регуляторов и репутационный ущерб, который напрямую влияет на капитализацию.

В свою очередь, экономические проблемы (нехватка средств на обновление ПО, сокращение штата ИТ-специалистов) ослабляют защиту информационных активов. Поэтому современная система управления рисками должна быть единой, объединяющей технические, финансовые и организационные аспекты. Руководители служб безопасности должны мыслить не в категориях «защищённости сети», а в терминах «предотвращённого ущерба» и «стоимости простоя».

5. Комплекс мер по минимизации рисков в условиях цифровизации

Эффективное противодействие рискам требует сочетания технических, организационных, правовых и образовательных инструментов.

5.1. Технические меры

— Современные межсетевые экраны нового поколения (NGFW) с функцией глубокого анализа трафика.

— EDR-системы (Endpoint Detection and Response), которые выявляют аномалии на конечных устройствах с помощью поведенческого анализа.

— DLP-решения для контроля утечек конфиденциальной информации через электронную почту, мессенджеры и съёмные носители.

— SIEM-системы, собирающие события со всех элементов инфраструктуры и коррелирующие их для обнаружения сложных атак.

— Обязательное шифрование данных при передаче и хранении, внедрение многофакторной аутентификации.

— Резервное копирование с изолированными хранилищами для защиты от программ-вымогателей.

5.2. Организационные меры

— Регулярное обучение персонала основам информационной безопасности, распознаванию фишинга и правилам работы с данными. Компании, внедрившие такие обучения сотрудников, сокращают число инцидентов на 30–40%.

— Принцип минимальных привилегий — доступ к информации предоставляется только в объёме, необходимом для выполнения должностных обязанностей.

— Внедрение процесса управления инцидентами (обнаружение, сдерживание, расследование, восстановление).

— Проверка контрагентов и поставщиков ПО на предмет их собственного уровня кибербезопасности (оценка рисков цепочек поставок).

5.3. Правовые и регуляторные меры

— Совершенствование законодательства в области защиты персональных данных (152-ФЗ), информации (149-ФЗ) и коммерческой тайны. Важно введение обязательного уведомления граждан об утечках их персональных данных и повышение штрафов за сокрытие утечек.

— Развитие национальных стандартов в области кибербезопасности, согласованных с международными подходами, но учитывающих отечественную специфику.

— Страхование киберрисков как инструмент компенсации ущерба от атак, утечек и простоев. Пока этот рынок в России только формируется, но его развитие может стимулировать компании вкладываться в защиту.

5.4. Государственные и национальные проекты

В России ключевым механизмом государственной поддержки цифровой безопасности стал национальный проект «Экономика данных и цифровая трансформация государства» (рассчитан до 2030 года). В его рамках:

— «Инфраструктура кибербезопасности» — создание систем обнаружения и предотвращения атак на объекты критической информационной инфраструктуры, разработка 11 отечественных решений и развёртывание киберполигонов для тренировки специалистов.

— «Отечественные решения» — ускоренный переход государственных органов и стратегических предприятий на российское ПО, снижающий зависимость от зарубежных вендоров.

— Единая антифрод-платформа с участием Банка России, МВД, операторов связи и банков для борьбы с телефонным и интернет-мошенничеством.

Также активно развиваются межведомственные центры реагирования на киберинциденты (ГосСОПКА, CERTы).

5.5. Мониторинг и аудит

— Периодические пентесты (тестирование на проникновение) — минимум раз в полгода или после существенных изменений инфраструктуры.

— Анализ логов доступа к критическим данным с выявлением подозрительных аномалий (доступ в нерабочее время, скачивание больших объёмов информации).

— Независимый аудит информационной безопасности с привлечением сторонних организаций для объективной оценки уровня защищённости.

В заключении хотелось бы отметить, что цифровизация необратимо меняет систему угроз: традиционная модель «защиты периметра» уступает место концепции непрерывной проверки каждого запроса и защиты самих данных независимо от их местонахождения. Возникают новые виды рисков — от атак с использованием ИИ до цифрового неравенства и инфраструктурной зависимости. При этом информационная и экономическая безопасность становятся двумя сторонами одного процесса: любой киберинцидент имеет финансовое измерение, а любое экономическое решение должно учитывать цифровые риски. Минимизация этих рисков требует комплексного подхода, сочетающего современные технологии (EDR, SIEM, DLP), организационные меры (обучение, контроль доступа), совершенствование законодательства и активную государственную поддержку (нацпроект «Экономика данных»). Только такая многоуровневая система защиты позволит обеспечить устойчивое развитие бизнеса и государства в условиях стремительной цифровизации.

Список литературы:

1. Андреев, А. В. Концепция Zero Trust: новый подход к кибербезопасности в условиях размывания периметра / А.В. Андреев, И.С. Петров // Вопросы кибербезопасности. — 2022. — № 3 (47). — С. 12–21.

2. Иванов, С.М. Риски цифровизации и их влияние на экономическую безопасность предприятия / С.М. Иванов // Экономическая безопасность. — 2023. — Т. 6, № 1. — С. 45–60.

3. Смирнова, Е.А. Искусственный интеллект как источник новых киберугроз / Е. А. Смирнова // Защита информации. Инсайд. — 2022. — № 5. — С. 34–39.
4. Лыкова, Е.С. Поиск оптимального уровня конкретизации запроса для максимизации точности релеватности ответов генеративных языковых моделей / Е. С. Лыкова, Е. А. Лыкова // Экономика и предпринимательство. – 2026. – № 2(187). – С. 1089-1094.