

УДК 330.46:332+004.056

DOI 10.5281/zenodo.18048666

**ДОЛБНЯ Наталия Валериевна<sup>1</sup>,**  
**ШПАК Глеб Евгеньевич<sup>1</sup>**

<sup>1</sup> ФГБОУ ВО «Донецкий государственный университет», ул. Университетская, 24, Донецк, Россия, 283001

## **ЦИФРОВАЯ УЯЗВИМОСТЬ БИЗНЕСА: ЭВОЛЮЦИЯ КИБЕРУГРОЗ**

В условиях стремительной цифровой трансформации кибербезопасность перестала быть узкотехнической задачей и превратилась в стратегический элемент корпоративного риск-менеджмента, напрямую влияющий на стоимость компании, её репутацию и инвестиционную привлекательность. Исследование систематизирует современные киберугрозы – от фишинга и мошенничества до сложных атак с использованием программ-вымогателей и двойного вымогательства, – и демонстрирует их экономические последствия: прямые убытки, простои критически важных процессов, регуляторные санкции и репутационный ущерб.

Авторами на основе системного и сравнительного анализа выявлены ключевые различия между малыми и средними предприятиями (МСП) и крупными организациями: компактная, но концентрированная инфраструктура МСП делает их уязвимыми к единичным инцидентам, угрожающим самому существованию бизнеса, тогда как крупные компании, несмотря на развитые системы защиты, несут многомиллионные прямые и косвенные потери.

Статья предлагает унифицированную модель жизненного цикла кибератаки и обобщает тактики злоумышленников, включая социальную инженерию, эксплуатацию уязвимостей удалённого доступа и эксфильтрацию данных через легитимные облачные каналы. Впервые представлена дифференцированная матрица мер защиты – от минимального уровня кибергигиены для МСП до продвинутых практик крупного бизнеса, включая Zero Trust, SIEM/XDR, Threat Hunting и метрики эффективности обучения персонала. С экономической точки зрения подчёркивается, что инвестиции в информационную безопасность следует рассматривать не как издержки, а как механизм снижения премии за риск, повышающий устойчивость к шокам.

В работе обоснована необходимость государственной или отраслевой стандартизации базовых мер киберзащиты для МСП, что снизит системные риски для всей цифровой экономики. Результаты исследования подтверждают: эффективная кибербезопасность требует системного, а не точечного подхода, интегрированного в стратегию управления стоимостью на всех уровнях корпоративного управления.

**Ключевые слова:** кибербезопасность, цифровая экономика, киберугрозы, информационная безопасность, киберриски, цифровая инфраструктура, фишинг, программы-вымогатели.

**Введение.** В условиях стремительной цифровой трансформации экономики вопросы управления рисками претерпевают фундаментальные изменения. Традиционные подходы к корпоративному риск-менеджменту, ориентированные преимущественно на финансовые, рыночные и операционные угрозы, всё более явно демонстрируют свою недостаточность перед лицом новых вызовов, порождённых гиперсвязностью и технологической зависимостью бизнеса. Киберриски, ранее воспринимавшиеся как

узкоспециализированная техническая проблема, сегодня вышли на первый план как системообразующий фактор экономической устойчивости, репутационной целостности и инвестиционной привлекательности компаний любого масштаба.

Анализ современных киберинцидентов – от массовых фишинговых кампаний до высокоорганизованных атак с использованием программ-вымогателей – свидетельствует: экономические последствия таких событий носят не локальный, а стратегический характер. Они напрямую влияют на стоимость компании, волатильность её акций, стоимость заёмного капитала и степень доверия со стороны клиентов, партнёров и регуляторов. В этой связи кибербезопасность перестаёт быть исключительно компетенцией ИТ-подразделений и должна быть интегрирована в систему корпоративного риск-менеджмента как самостоятельный, значимый элемент управления стоимостью.

С экономической точки зрения инвестиции в информационную безопасность целесообразно рассматривать не как операционные издержки, а как механизм снижения премии за риск. Компании с зрелыми практиками кибербезопасности демонстрируют повышенную устойчивость к негативным шокам, быстрее восстанавливаются после инцидентов и, как следствие, становятся более привлекательными для инвесторов, особенно в условиях роста ESG- и cyber-ориентированных критериев оценки корпоративной зрелости. В то же время малые и средние предприятия, составляющие основу предпринимательской экосистемы, зачастую не обладают ни ресурсами, ни экспертизой для самостоятельной реализации даже базовых мер защиты, что создаёт асимметрию рисков, при которой уровень уязвимости малых предприятий становится системным фактором нестабильности для всей цифровой экономики.

Поэтому особую актуальность приобретает разработка и внедрение стандартизированных, доступных и масштабируемых рамок минимальной кибергигиены, поддерживаемых на уровне государства или отраслевых ассоциаций. Такие инициативы позволят не только снизить барьеры входа малого бизнеса в цифровую среду, но и укрепить устойчивость национальной экономики в целом, минимизируя каскадные эффекты от локальных компрометаций.

В данном контексте работа [1] представляет собой краткий обзор актуальных проблем кибербезопасности в условиях роста цифровой экономики. Авторы верно подчёркивают, что в условиях цифровой экономики информация становится стратегическим активом, а кибербезопасность – критически важным элементом устойчивости как для организаций, так и для частных лиц, что соответствует мировым трендам и подтверждается многочисленными исследованиями (например, от IBM, ENISA, Kaspersky и др.). Исследование Я. С. Исламгереевой и З. Р. Эдисултановой [2] содержит оценку государственных инициатив: ГосСОПКА, регулирование критически важных объектов инфраструктуры, импортозамещение, суверенный интернет, что особенно актуально для России и стран с аналогичной политикой цифрового суверенитета. Статья Т.Л. Мартыновой [3] представляет собой аналитическое исследование, посвящённое взаимосвязи между динамикой цифровой трансформации социальных и государственных услуг в России и уровнем их кибербезопасности. Автор справедливо смещает фокус с корпоративной кибербезопасности на граждан как конечных пользователей цифровых госуслуг и финансовых сервисов. Именно они становятся основной жертвой мошенников, особенно в условиях роста социальной инженерии и фишинга. Работа М.Г. Миргородской, О.А. Аничкиной и С.С. Ивановой [4] представляет собой прикладное исследование, посвящённое двойственной роли цифровой трансформации: с одной стороны – как фактора роста и повышения эффективности (повышение конкурентоспособности, доступ к данным, автоматизация), с другой – как источника новых угроз и рисков, особенно в сфере кибербезопасности (кибератаки, утечки, репутационные потери).

Совокупность исследований подтверждает, что кибербезопасность перестаёт быть узкотехнической задачей и становится междисциплинарной областью, требующей интеграции технологических, организационных, правовых и образовательных мер. При этом особую значимость приобретает дифференцированный подход – с учётом масштаба организации, уровня цифровой зрелости и специфики пользовательской аудитории.

Поэтому, настоящая работа направлена на системное осмысление взаимосвязи между уровнем кибербезопасности, структурой киберрисков и экономическими последствиями для организаций разного масштаба, с целью обоснования необходимости институционального включения кибербезопасности в стратегию корпоративного управления рисками.

**Материалы и методы.** Методология исследования базируется на системном анализе, позволяющем рассматривать цифровую инфраструктуру предприятия как целостную социально-техничко-экономическую систему. Дополнительно применён сравнительный анализ для выявления различий в профилях киберрисков, подходах к управлению информационной безопасностью и экономических последствиях инцидентов между малыми и средними предприятиями и крупными организациями. В работе также использованы методы моделирования – построены унифицированные модели жизненного цикла кибератаки и сценариев компрометации, а также индуктивный метод – на основе анализа множества конкретных инцидентов сформулированы обобщённые закономерности и рекомендации.

**Результаты.** За последние годы бизнес практически полностью перешёл в цифровой формат: компании взаимодействуют с клиентами через корпоративные сайты, маркетплейсы, мобильные приложения, социальные сети и мессенджеры, используют облачные хранилища и публичные доменные имена (рис. 1).

Любая из этих площадок может стать входной точкой атаки и источником финансовых и репутационных потерь для компании, что подтверждают исследования российских авторов. Статья А.П. Бувевич [6] представляет собой актуальное и хорошо структурированное исследование, посвящённое растущим киберрискам в банковской сфере и мерам противодействия им. Автор опирается на официальные данные Банка России, экспертные оценки и кейсы: *«По данным Банка России, в 2023 году количество кибератак на кредитные организации увеличилось на 37% по сравнению с предыдущим годом, при этом 68% атак были направлены на клиентские данные и платежные системы, а средний размер ущерба от успешной атаки составил около 15 млн рублей»* [5, с. 48], из чего следует, что кибербезопасность действительно становится вопросом не операционного, а стратегического и национального уровня. Исследованиям кибербезопасности банковского сектора также посвящены работы [6-7], которые также свидетельствуют о важности изучаемого вопроса.

Статья М.С. Мартынюк [8] и исследование Р.А.-М. Айбуевой и Х.Ш. Насурова [9] имеют важное содержательное пересечение, несмотря на различие в методологическом подходе и фокусе. Обе работы рассматривают киберриски не только как ИТ-проблему, но и как угрозу экономической стабильности и национальному суверенитету. Исследование [8] подчёркивает количественную и качественную измеримость защиты в рамках «результативной безопасности», а статья [9] предлагает ROI- и IRR-анализ программ обучения, а также шкалы цифровой зрелости, что полностью соответствует идее измеримости.

Рост цифровизации сопровождался взрывным ростом онлайн-мошенничества. По данным Group-IB, около 73 % всех киберинцидентов во всём мире связано со скамом и фишингом, а на долю более «тяжёлых» высокотехнологичных преступлений, включая программы-вымогатели и атаки на интернет-банкинг, приходится примерно четверть. В

2020 году доля онлайн-мошенничества в общем объёме атак достигла 56%, доля фишинга выросла до 17%, а число нарушений, связанных со скамом и фишингом, в России увеличилось на 35% год к году. При этом жертвами формально становятся клиенты компаний, но экономический и репутационный удар приходится именно по бизнесу<sup>1,2</sup>.

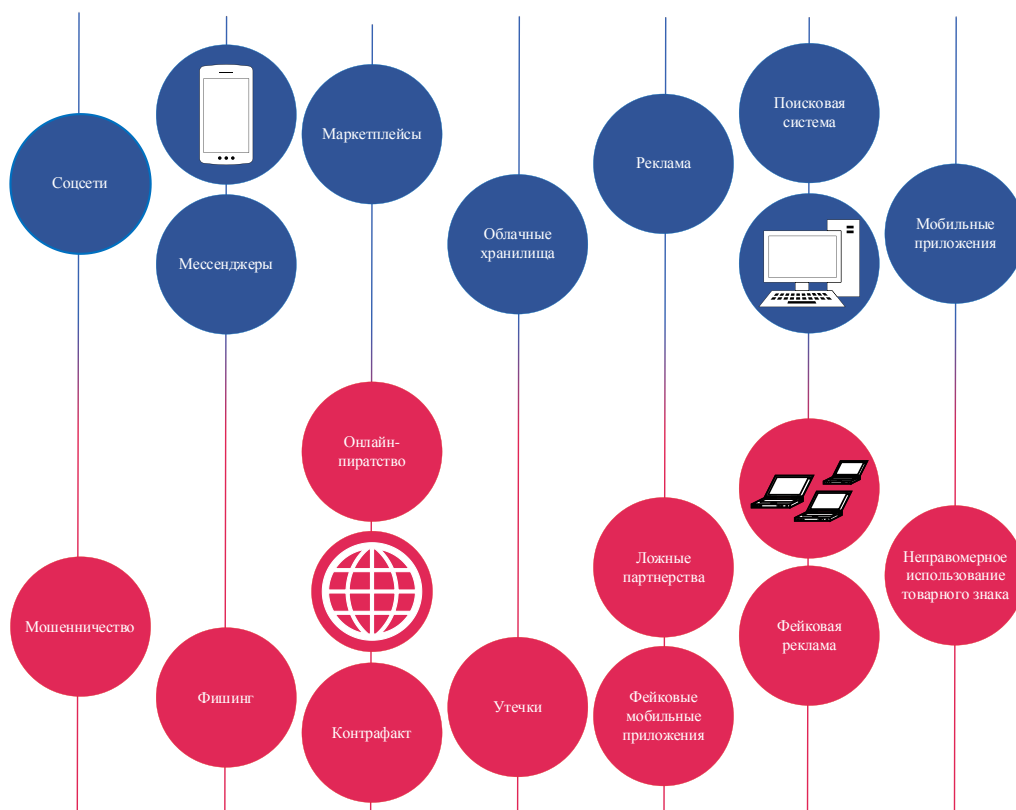


Рис. 1. Области цифрового присутствия компании и связанные типы онлайн-угроз (авторская разработка)

На этом фоне программы-вымогатели стали одним из самых болезненных инструментов монетизации атак. Развитие вымогателей описывается как эволюция «киберимперии»: от первых шифровальщиков PGPcoder в 2004 году, рассчитанных на домашних пользователей, через эпоху Windows-локеров и первые схемы Ransomware-as-a-Service к современным партнёрским программам, нацеленным исключительно на юридических лиц<sup>3</sup>. Поворотным моментом стали кампании WannaCry и NotPetya в 2017 году, когда бизнес впервые массово столкнулся с парализацией инфраструктуры и многомиллионными убытками<sup>4</sup>. С тех пор крупные и средние организации во всём мире рассматриваются операторами вымогателей как основной источник дохода (рис. 2).

<sup>1</sup> Тренды фишинговых атак на организации в 2022–2023 годах [Электронный ресурс]: <https://ptsecurity.com/research/analytics/phishing-attacks-on-organizations-in-2022-2023/>.

<sup>2</sup> Фейк не пройдет: Group-IB представила автоматизированную систему ликвидации цифровых рисков [Электронный ресурс]: <https://www.forbes.ru/partnerskie-materialy/431657-feyk-ne-proydet-group-ib-predstavila-avtomatizirovannuyu-sistemu>.

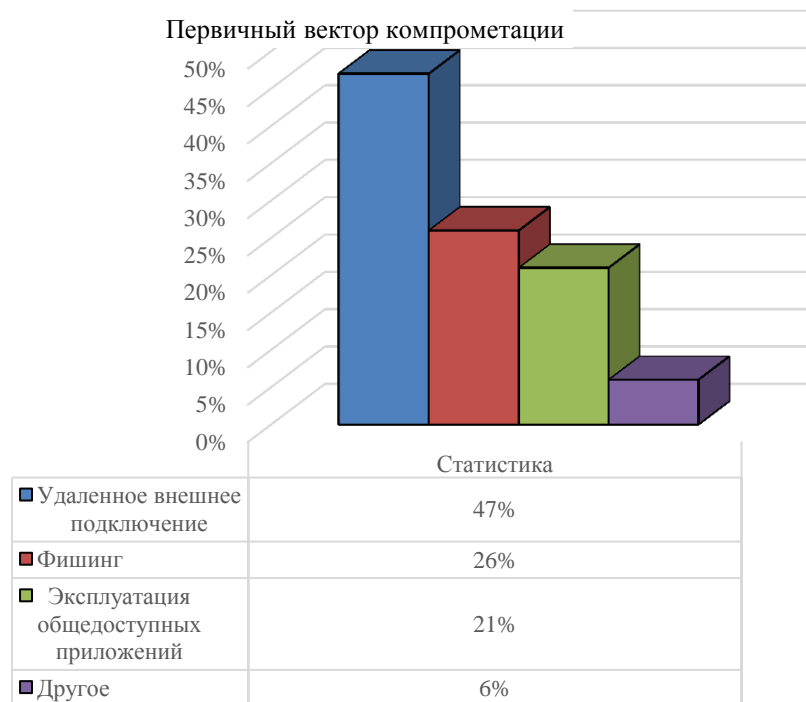
<sup>3</sup> A history of ransomware: The motives and methods behind these evolving attacks [Электронный ресурс]: <https://www.csoonline.com/article/569617/a-history-of-ransomware-the-motives-and-methods-behind-these-evolving-attacks.html>.

<sup>4</sup> Крупнейшие кибератаки в истории [Электронный ресурс]: <https://ddos-guard.ru/blog/krupneishie-kiberataki-v-istorii>.



**Рис. 2. Этапы эволюции программ-вымогателей (авторская разработка)**

Количественные оценки подтверждают, что речь идёт не о единичных эксцессах, а о стабильном рынке. В выпуске, *Ransomware Uncovered 2021/2022*, указывается, что в 2021 году топ-3 операторов составляли LockBit, Conti и Rysa, а доля атак, в которых злоумышленники не только шифровали, но и заранее выводили данные жертв, достигла 63 %<sup>5</sup>. Средний запрашиваемый выкуп вырос до 247 тысяч долларов, максимальный известный запрос – около 240 миллионов долларов<sup>6</sup>. Не менее показательна статистика по первичным векторам компрометации на рисунке 3.



**Рис. 3. Количество публично доступных терминальных серверов в крупных городах России (разработка на основе<sup>7,8</sup>)**

<sup>5</sup> Group-IB назвала среднюю сумму требуемого хакерами-шифровальщиками выкупа [Электронный ресурс]: [https://www.rbc.ru/technology\\_and\\_media/19/05/2022/6285f3c39a7947c2155003ea](https://www.rbc.ru/technology_and_media/19/05/2022/6285f3c39a7947c2155003ea).  
<sup>6</sup> Средний выкуп, запрашиваемый вымогателями, достиг \$247 000 [Электронный ресурс]: <https://www.iksmedia.ru/news/5887498-Srednij-zaprashivaemyj-vyкуп-vymoga.html>.  
<sup>7</sup> Топ 11 провайдеров для аренды терминального сервера Windows — рейтинг 2025-2026 [Электронный ресурс]: [https://dtf.ru/rating\\_top/4046532-top-11-providerov-dlya-arendy-terminalnogo-servera-windows](https://dtf.ru/rating_top/4046532-top-11-providerov-dlya-arendy-terminalnogo-servera-windows).

Российская выборка, приведённая в отчёте *Ransomware in Russia*, подтверждает особую роль удалённого доступа: около 60 % успешных атак на организации в России были связаны с компрометацией публично доступных терминальных серверов и RDP-узлов<sup>9</sup>, при этом количество таких серверов в крупнейших городах измеряется десятками тысяч (рис. 4), при этом причиной успешной компрометации в большинстве случаев становятся слабые пароли и использование стандартных учётных записей. Рост удалённой работы во время пандемии COVID-19 сделал эту поверхность атаки ещё шире и привлекательнее для злоумышленников.

## ПУБЛИЧНО ДОСТУПНЫЕ ТЕРМИНАЛЬНЫЕ СЕРВЕРЫ

МОСКВА	59078
САНКТ-ПЕТЕРБУРГ	14345
ЕКАТЕРИНБУРГ	2148
НОВОСИБИРСК	1830
ЧЕЛЯБИНСК	984
НИЖНИЙ НОВГОРОД	919
КРАСНОЯРСК	845
КРАСНОДАР	820
ПЕРМЬ	780
ВЛАДИВОСТОК	754

Рис. 4. Количество публично доступных терминальных серверов в крупных городах России (разработка на основе<sup>10,11</sup>)

Цель исследования – описать, что может произойти с компанией при целевой атаке, какие типичные сценарии используют злоумышленники, какие этапы проходят в ходе атаки и каковы прямые и косвенные экономические последствия для организаций различного масштаба. Обобщается статистика по векторам первичного доступа и тактикам атак, строится унифицированная модель жизненного цикла атаки на бизнес-инфраструктуру и формулируются практические рекомендации по снижению рисков для малого и крупного бизнеса в рамках процессов информационной безопасности.

Для малых и средних предприятий (МСП) типична компактная, но с точки зрения риска концентрированная ИТ-инфраструктура. Ключевые бизнес-функции часто завязаны на небольшой набор систем и сервисов: один–два публичных веб-ресурса, несколько облачных приложений, средства удалённого доступа, развёрнутые по упрощённым сценариям. Управление безопасностью в таких организациях, как правило, осуществляется в рамках общего ИТ-администрирования и ограничивается базовыми мерами: антивирусной защитой, локальными настройками доступа и отдельными

<sup>8</sup> Russia | Public DNS Server [Электронный ресурс]: <https://publicdnserver.com/>

<sup>9</sup> Родина в опасности: Group-IB назвала топ-3 шифровальщиков, атакующих российский бизнес [Электронный ресурс]: <https://www.fb.ru/media-center/press-releases/top-3-ransomware-2021/>

<sup>10</sup> Топ 11 провайдеров для аренды терминального сервера Windows — рейтинг 2025-2026 [Электронный ресурс]: [https://dtf.ru/rating\\_top/4046532-top-11-provaiderov-dlya-arendy-terminalnogo-servera-windows](https://dtf.ru/rating_top/4046532-top-11-provaiderov-dlya-arendy-terminalnogo-servera-windows)

<sup>11</sup> Russia | Public DNS Server [Электронный ресурс]: <https://publicdnserver.com/>

организационными регламентами. Автор [10] верно подчёркивает, что малый и средний бизнес является высокоприоритетной целью для киберпреступников: ограниченные ресурсы, отсутствие специалистов по ИБ, слабые пароли и устаревшее ПО делают МСП «лёгкой добычей». В свою очередь, в работе [11] подчеркивается, что МСП особенно уязвимы из-за ограниченных бюджетов, отсутствия специалистов по ИБ, зависимости от внешних ИТ-провайдеров.

В крупных организациях, напротив, преобладает распределённая, многослойная инфраструктура, включающая множество доменных зон и внешних сервисов, специализированные порталы для клиентов и партнёров, собственные мобильные приложения, развитые системы удалённого доступа для филиалов и подрядчиков, а также широкий спектр внутренних и внешних бизнес-приложений. В таких условиях, как правило, формируется выделенная функция информационной безопасности, используются специализированные средства мониторинга, привлекаются внешние провайдеры услуг, а процессы управления инцидентами и уязвимостями описываются в нормативных документах.

В малом бизнесе фишинговые рассылки и мошеннические активности вокруг бренда в значительной части случаев ориентированы на прямое изъятие денежных средств у клиентов и самой организации. Компрометация инфраструктуры часто является следствием единичного воздействия на ограниченный круг сотрудников либо администратора средств удалённого доступа. Для крупных структур вектор фишинга и злоупотребления брендом дополняется систематическими попытками получения доступа к доменным службам, бизнес-почте и системам удалённого администрирования, а также активным использованием уже проданных на теневых площадках первоначальных доступов. Для обобщения указанных различий представляется целесообразным использовать сравнительную характеристику (табл. 1), отражающую ключевые аспекты уязвимости к киберугрозам в организациях различного масштаба.

**Таблица 1. Сравнительная характеристика киберугроз для малых и крупных организаций\***

Аспект	Малые и средние предприятия	Крупные организации
Структура инфраструктуры	Небольшое число узлов и сервисов, высокая концентрация критичных данных в отдельных системах	Распределённая многослойная инфраструктура, значительное число взаимосвязанных сервисов и доменов
Управление ИБ	Отсутствие или минимальное развитие выделенной функции ИБ, точечные меры защиты	Выделенные подразделения ИБ, формализованные процессы, использование специализированных средств и внешних сервисов
Типичные уязвимости	Упрощённо настроенный удалённый доступ, единые учётные записи, недостаточная регламентация работы с почтой и файлами	Уязвимости во внешних и «наследуемых» сервисах, неоднородность настроек, риски цепочек поставок и подрядчиков
Преобладающие проявления угроз	Фишинг и мошенничество в отношении клиентов и сотрудников, единичные, но потенциально критичные инциденты с шифровальщиками	Целевые атаки на инфраструктуру, эксплуатация проданных доступов, комбинированные сценарии с вымогательством и утечкой данных
Относительная устойчивость к инцидентам	Высокая чувствительность к единичному инциденту, ограниченные возможности восстановления	Более высокая способность к восстановлению, но существенные прямые и косвенные потери при крупных инцидентах

\*авторская разработка.

На уровне последствий это выражается в том, что для МСП отдельный инцидент с компрометацией инфраструктуры или успешным применением программы-вымогателя может иметь длительный простой критичных систем и необходимость значительных незапланированных затрат ставят под угрозу продолжение деятельности. Для крупной организации аналогичный по техническим параметрам инцидент, как правило, не приводит к немедленному прекращению функционирования, однако сопровождается значительными финансовыми потерями, возможными регуляторными санкциями, судебными исками со стороны контрагентов и клиентов, а также длительными репутационными издержками.

На уровне отдельного рабочего места жизненный цикл атаки часто начинается с доставки многоступенчатой вредоносной нагрузки через социальную инженерию. Обобщённая последовательность действий представлена на рисунке 5.

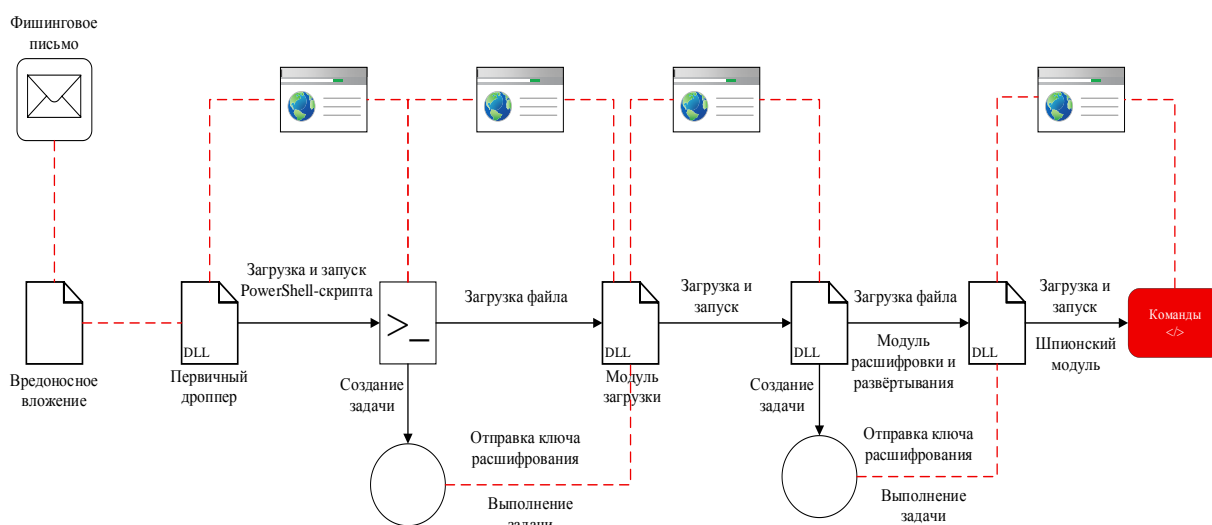


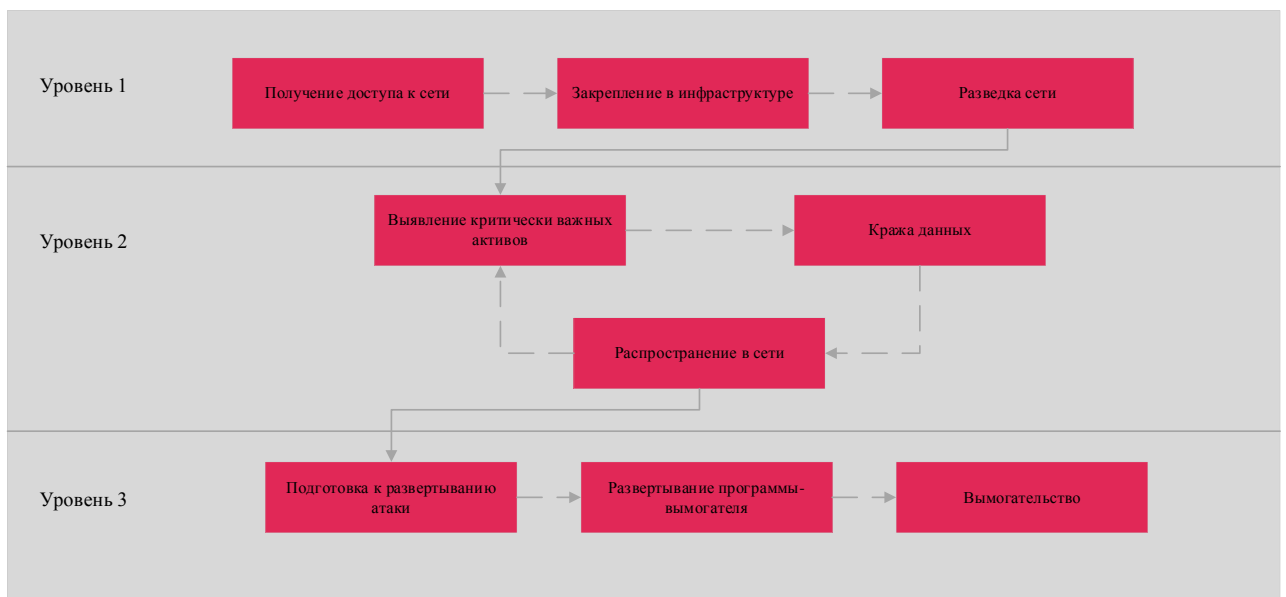
Рис. 5. Цепочка заражения при атаке через фишинговое вложение (авторская разработка)

Сотрудник получает фишинговое электронное письмо с вложением, маскирующимся под деловой документ. Открытие вложения приводит к запуску первичного дроппера в виде DLL-модуля, который, используя встроенные или системные средства, загружает следующий компонент. Далее в систему по цепочке подтягиваются дополнительные модули загрузки и модули расшифровки и развёртывания, каждый из которых реализует ограниченный набор функций и минимальный объём бинарного кода. Такой многоступенчатый подход затрудняет детектирование: часть логики вынесена в сценарии, передаваемые с управляющего сервера, а ключи расшифрования и команды подгружаются уже после успешного закрепления на хосте.

Если рассматривать атаку не с точки зрения отдельного узла, а на уровне всей сети организации, полезно использовать агрегированную модель, отражающую ключевые фазы операции операторов программ-вымогателей. Такая модель представлена на рисунке 6.

Исследование [12] подчёркивает, что Индустрия 4.0 несёт двойственный эффект – рост производительности и одновременно расширение «поверхности атаки», что подтверждается сравнительным анализом ключевые отличия операционных технологий от ИТ: долгий жизненный цикл оборудования, приоритет безопасности процессов, а не конфиденциальности данных, использование устаревших протоколов (Modbus, DNP3), невозможность частых обновлений [12, с. 36] – это фундаментальное различие, которое часто игнорируют при проектировании защиты.

На первом уровне злоумышленники получают доступ к корпоративной сети и закрепляются в инфраструктуре, проводя минимальную разведку. На втором уровне происходит выделение критически важных активов: доменных контроллеров, файловых серверов, систем резервного копирования, бизнес-критичных приложений. Параллельно осуществляется распространение в сети за счёт использования легитимных административных инструментов, механизма Pass-the-Hash, внедрения в планировщики задач и других техник, описанных в MITRE ATT&CK<sup>12</sup>. На третьем уровне, после достижения достаточного контроля над инфраструктурой, инициируется подготовка к развёртыванию шифровальщика, выполняется собственно шифрование данных и запускается стадия вымогательства, которая может включать переговоры, публикацию данных на специализированных ресурсах и дополнительное давление на жертву.



**Рис. 6. Унифицированная структура атак с применением программ-вымогателей (авторская разработка)**

Ключевой особенностью современных атак является смещение акцента с одного лишь шифрования в сторону комбинированных схем, подразумевающих предварительную кражу данных. В этой связи особый интерес представляет этап эксфильтрации<sup>13</sup>. В этом контексте интересна работа [13], которая посвящена альтернативным методам предотвращения утечки данных из корпоративной инфраструктуры организаций, представляющих различные отрасли, а также защите от эксфильтрации информации с мобильных устройств их сотрудников, в работе подчёркивается актуальность пересмотра традиционных подходов и необходимости трансформации самой философии информационной безопасности в условиях современных вызовов.

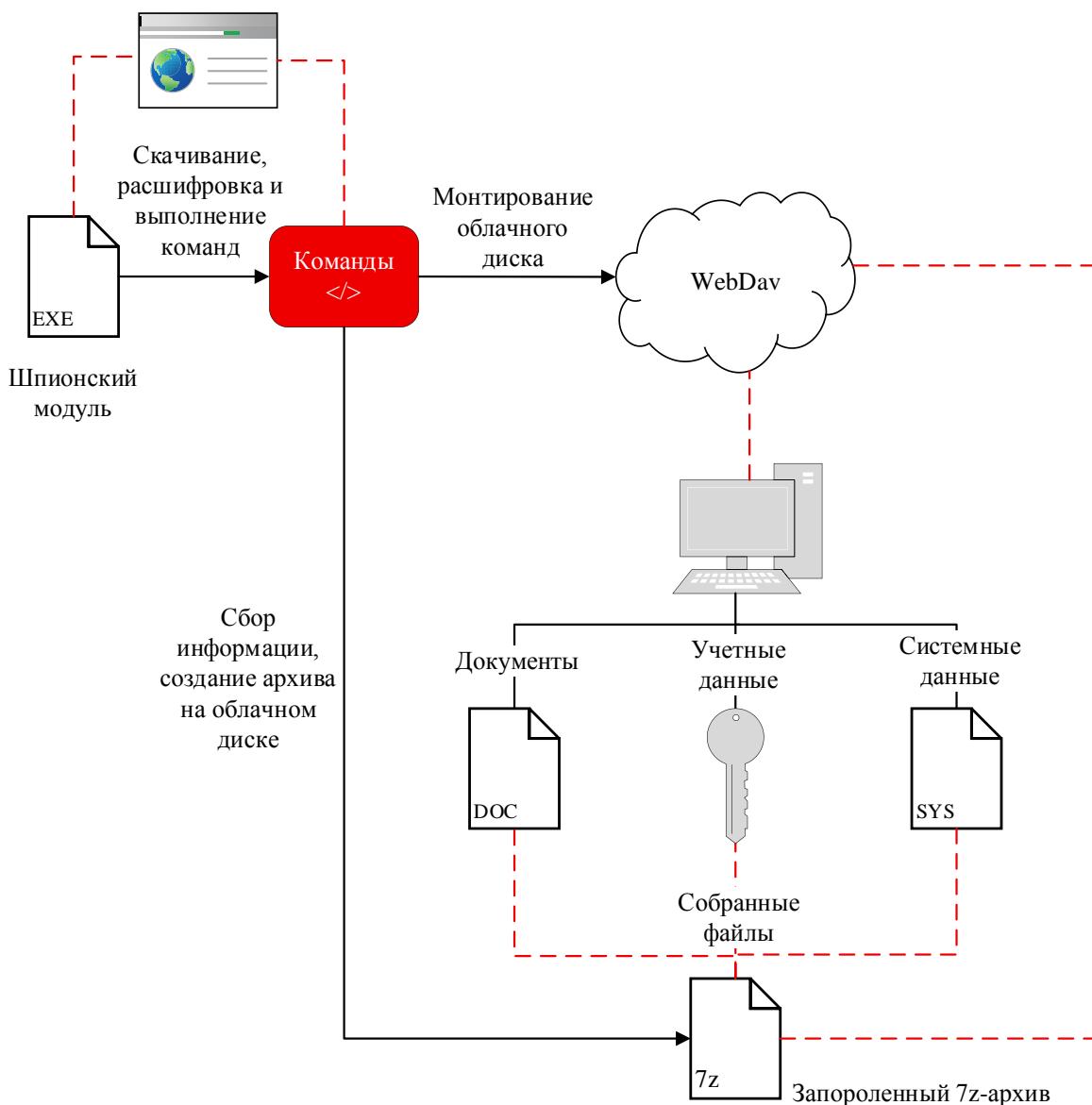
Обобщённый пример такого этапа эксфильтрации показан на рисунке 7.

После закрепления в сети шпионский модуль получает с командного сервера набор зашифрованных инструкций, расшифровывает их и монтирует облачное хранилище по протоколу WebDav. Далее выполняется автоматизированный сбор документов, учётных и

<sup>12</sup> Use Alternate Authentication Material: Pass the Hash [Электронный ресурс]: <https://attack.mitre.org/techniques/T1550/002/>

<sup>13</sup> Кража данных и способы ее реализации [Электронный ресурс]: <https://ptsecurity.com/research/knowledge-base/krazha-dannyh-i-sposoby-ee-realizacii/>

системных данных с локальных и сетевых ресурсов; собранные файлы агрегируются и упаковываются в защищённый архив, который по тому же облачному каналу передаётся злоумышленникам. Такой механизм позволяет маскировать утечку под легитимный сетевой трафик и использовать стороннюю инфраструктуру как промежуточное звено между внутренней сетью жертвы и конечными серверами атакующих.



**Рис. 7. Эксфильтрация корпоративных данных через облачный сервис**  
 (авторская разработка)

Таким образом, жизненный цикл атаки на корпоративную инфраструктуру представляет собой не разовое событие, а последовательность взаимосвязанных этапов, в ходе которых злоумышленники поэтапно переходят от единичного инцидента на рабочем месте к системному контролю над ключевыми цифровыми активами организации.

Для бизнеса критичны не столько технические детали инцидента, сколько длительность простоя ключевых процессов, объём затрат на реагирование и восстановление, а также долговременное влияние на выручку, стоимость бренда и регуляторный статус. Современные кампании программ-вымогателей всё чаще строятся

по схемам двойного и тройного вымогательства: перед шифрованием выполняется эксфильтрация данных, и в большинстве успешных атак злоумышленники не только блокируют, но и похищают конфиденциальную информацию.

Даже при наличии резервных копий организация остаётся под угрозой публикации или продажи украденных массивов, что переводит инцидент в плоскость защиты персональных и коммерчески чувствительных данных. Дополнительную необратимость последствиям придаёт использование устойчивых криптографических схем (AES-256, ChaCha20/Salsa20 в сочетании с RSA-2048/4096 и эллиптическими кривыми)<sup>14</sup>, практически исключающих восстановление без закрытого ключа.

Полученные результаты анализа статистики и сценариев атак позволяют сформулировать практические рекомендации, ориентированные не на отдельные продукты, а на комплекс организационных и технических мер, выстроенных по стадиям жизненного цикла атаки и с учётом различий между малым и крупным бизнесом. На этапе первичного доступа приоритетом является защита удалённых сервисов и публичных приложений: минимизация поверхности атаки, использование VPN с MFA вместо прямого RDP, политика сложных паролей, ограничение доступа по IP и своевременное обновление периметра<sup>15</sup>.

С учётом устойчивого использования фишинга и вредоносных вложений защита должна сочетать современные почтовые шлюзы (анализ вложений, проверка URL, песочницы) с систематическим повышением осведомлённости персонала: для МСП – облачные почтовые сервисы с фильтрацией и простыми симуляциями фишинга, для крупных организаций – специализированные платформы и отработанные процедуры реагирования на подозрительные письма. На стадии продвижения по сети критичен контроль привилегий и мониторинг «инструментов двойного назначения»: внедрение принципа наименьших прав, разделение пользовательских и административных учётных записей, выделенные учётные данные для критичных систем, аудит запуска PowerShell-скриптов, планировщика задач и служебных утилит.

Обеспечение устойчивости к шифрованию и эксфильтрации базируется на наличии актуальных изолированных резервных копий: для МСП – автоматизированные облачные бэкапы с отдельной аутентификацией, для крупных организаций – разнесённые площадки, регулярная проверка сценариев восстановления и сегментация доступа к инфраструктуре бэкапов; одновременно необходимо ограничивать неконтролируемое использование облачных хранилищ и WebDav-каналов. Существенную роль играют подсистемы обнаружения и реагирования: круглосуточный мониторинг событий ИБ, централизованный сбор и корреляция логов, формализованные процедуры реагирования, развитие Threat Hunting; в качестве методологической основы целесообразно использовать матрицу MITRE ATT&CK. Сводно предложенные меры можно представить как минимальный и продвинутый уровни зрелости для организаций разного масштаба (таблица 2).

Исследование показало, что кибербезопасность перестала быть исключительно технической задачей и стала ключевым элементом корпоративного риск-менеджмента, напрямую влияющим на устойчивость, стоимость и репутацию бизнеса. Для малых и средних предприятий киберинциденты могут угрожать самому существованию компании, тогда как крупные организации сталкиваются с масштабными финансовыми,

<sup>14</sup> Современные алгоритмы шифрования: от AES до RSA и Blowfish [Электронный ресурс]: <https://serverflow.ru/blog/stati/sovremennye-algoritmy-shifrovaniya-ot-aes-do-rsa-i-blowfish/>

<sup>15</sup> Ультимативный гайд по защите инфраструктуры от шифровальщиков и вайперов [Электронный ресурс]: <https://habr.com/ru/companies/bizone/articles/962486/>

регуляторными и репутационными потерями. Современные атаки, особенно с использованием программ-вымогателей и двойного вымогательства, требуют системного, а не точечного подхода к защите. Инвестиции в информационную безопасность следует рассматривать как стратегический инструмент снижения премии за риск и повышения инвестиционной привлекательности. Для МСП необходима стандартизация минимальных мер защиты через государственные или отраслевые инициативы, что повысит устойчивость всей цифровой экономики, что перекликается с исследованиями российских ученых [14-15].

Таблица 2. Основные характеристики логистических сервисов\*

Мера защиты	МСП – минимальный уровень	МСП – продвинутый уровень	Крупные организации
1	2	3	4
Защита удалённого доступа	Один VPN-шлюз, отказ от прямого RDP из интернета, сложные пароли	VPN с MFA, ограничение доступа по IP, периодический аудит настроек	Множественные узлы доступа, сегментация, MFA везде, централизованный контроль и журналирование, регулярный внеш. Аудит периметра
Защита почты и веб-трафика	Облачный почтовый сервис с базовой фильтрацией спама и вложений	Дополнительная проверка ссылок и вложений, простые симуляции фишинга	Почтовые шлюзы с песочницами, URL-фильтрация, DMARC/SPF/DKIM, платформа симуляций фишинга и отслеживания метрик обченности
Управление учётными записями и привилегиями	Индивидуальные учётные записи, запрет общих логинов, сложные пароли	Разделение админских и пользовательских учётных записей, регламенты выдачи прав	Политика наименьших привилегий, PAM-решения, регулярный аудит прав, контроль использования админ-инструментов
Резервное копирование и восстановление	Автоматизированные ежедневные резервные копии критичных данных в отдельное хранилище	Периодическая проверка восстановления, хранение части копий офлайн/в другом облаке	Разнесённые площадки, многоуровневые бэкапы, тесты DRP, отдельная зона доверия для инфраструктуры бэкапов
Мониторинг и реагирование	Журналы основных систем, ручной просмотр при инцидентах	Централизованный сбор логов ключевых сервисов, базовые правила корреляции	SIEM/EDR/XDR, 24×7 SOC (внутренний или внешний), формализованный процесс IR, Threat Hunting, регулярный разбор инцидентов
Управление цифровыми рисками и брендом	По возможности – контроль доменного имени, периодический поиск фишинговых страниц «вручную»	Мониторинг упоминаний компании, отслеживание подозрительных доменов/страниц	Сервисы Digital Risk Protection: поиск фишинга, поддельных приложений, утечек данных, процедура блокировки и претензионной работы

Окончание табл. 2

1	2	3	4
Обучение и осведомлённость персонала	Краткий вводный инструктаж по ИБ, памятки о фишинге	Ежегодные тренинги, мини-курсы для сотрудников из «зон риска» (бухгалтерия, продажи и др.)	Непрерывная программа awareness, сегментированные тренинги, метрики поведения, включение ИБ в KPI управленцев
Тестирование защищённости	Разовый внешний сканер уязвимостей или аудит провайдера	Периодические сканирования уязвимостей, эпизодические тесты на проникновение	Регулярный VA/PT, киберучения, Red Teaming, проверка цепочек поставок и подрядчиков, анализ соответствия отраслевым стандартам

\* авторская разработка

**Обсуждение результатов.** Проведенное исследование выявило ключевые особенности современных киберугроз, связанных с ростом цифровизации бизнеса, а также системные различия в уязвимостях и последствиях инцидентов для малых и средних предприятий и крупных организаций. Основные результаты можно сгруппировать по следующим направлениям (табл. 3).

Таблица 3. Критерии уязвимости\*

Критерий	МСП	Крупные организации
Инфраструктура	Компактная, высокая концентрация данных	Распределённая, многослойная
Управление ИБ	Отсутствует или минимизировано	Формализовано, с выделенными командами
Типичные угрозы	Фишинг, мошенничество, единичные атаки вымогателей	Целевые атаки, использование проданных доступов
Последствия	Угроза прекращения деятельности	Значительные финансовые и репутационные потери

\* авторская разработка

Для МСП один инцидент может привести к полной остановке бизнеса, в то время как крупные организации, несмотря на устойчивость, несут многомиллионные убытки и регуляторные риски. Современные кибератаки представляют собой сложные, многоэтапные операции, нацеленные на максимальную монетизацию через комбинацию шифрования, кражи данных и репутационного шантажа. Эффективная защита требует адаптированного подхода, учитывающего масштаб бизнеса, уровень зрелости ИБ и специфику цифровой поверхности атаки. Результаты исследования подтверждают необходимость системной, а не точечной работы с киберрисками на всех уровнях управления.

**Заключение.** Результаты исследования демонстрируют фундаментальную трансформацию экономической природы киберрисков в условиях цифровой экономики. Киберугрозы перестали быть исключительно технической проблемой и превратились в структурный источник операционных, репутационных и стратегических издержек, напрямую влияющих на устойчивость бизнес-моделей. Особенно критичен рост асимметрии рисков между малым и крупным бизнесом: для МСП киберинциденты несут

угрозу выживания (ограниченные ресурсы на восстановление, высокая концентрация активов), тогда как для крупных компаний речь идёт о масштабных транзакционных издержках – прямых (восстановление, выкуп, штрафы) и косвенных (потеря клиентского доверия, снижение капитализации бренда, регуляторное давление). Экономически значимым является переход киберпреступности к моделям двойного вымогательства, что резко повышает стоимость отказа от сотрудничества с атакующими даже при наличии резервных копий. Это формирует новый класс необратимых потерь, связанных с утечкой коммерческой тайны и персональных данных, что в условиях ужесточения регулирования трансформируется в юридико-экономические обязательства.

Необходимость включения кибербезопасности в систему корпоративного риск-менеджмента как самостоятельного элемента, влияющего на стоимость компании, является ключевым в нынешних реалиях. Инвестиции в ИБ следует рассматривать не как издержки, а как фактор снижения премии за риск, повышающий устойчивость к шокам и привлекательность для инвесторов. Для малого бизнеса целесообразна стандартизация минимальных мер защиты через государственные или отраслевые инициативы, что снизит барьеры входа в цифровую экономику и уменьшит системные риски для всей экономики.

**Дополнительная информация.** Исследование проводилось в ФГБОУ ВО «ДонГУ» в рамках НИОКТР №124110700063-1 (Фи-24/4) на 2025 год «Совершенствование методологии процессного моделирования в управлении функционированием и развитием сложных социотехнических и экономических систем».

### Список литературы

1. Цифровая экономика: кибербезопасность в эпоху цифровой экономики: текущие угрозы и защита / А.М. Аннамуратова, М.С. Ишанкулиева, Д. Абыллаев, М. Алланазаров // Матрица научного познания. – 2023. – № 9-1. – С. 205-207. – EDN: SIDVQC.
2. Исламгереева, Я.С. Кибербезопасность в эпоху цифровой экономики: вызовы, угрозы и стратегии защиты / Я.С. Исламгереева, З.Р. Эдисултанова // Научный бюллетень Чеченского государственного университета им. А.А. Кадырова. – 2025. – № 2(6). – С. 21-26. – DOI 10.36684/118-2025-2-6-21-26. – EDN GBNZZD.
3. Мартынова, Т.Л. Цифровизация экономики информационного общества и кибербезопасность социальных услуг / Т.Л. Мартынова // Вестник Университета имени О.Е. Кутафина (МГЮА). – 2024. – № 10(122). – С. 77-84. – DOI 10.17803/2311-5998.2024.122.10.077-084. – EDN MWTWFD.
4. Миргородская, М.Г. Влияние цифровой экономики на экономическую безопасность предприятий / М.Г. Миргородская, О.А. Аничкина, С.С. Иванова // Инновационное развитие экономики. – 2024. – №1(79). – С. 95-99. – DOI 10.51832/222379842024195. – EDN UIJMPK.
5. Буевич, А.П. Киберугрозы как современный вызов безопасности банковского сектора в России / А.П. Буевич // Национальная безопасность / Nota Bene. – 2025. – № 4. – С. 46-55. – DOI 10.7256/2454-0668.2025.4.74921. – EDN RAPRMK.
6. Белалов, М.Р. Киберриски как новый класс операционных рисков банков: экономическая оценка, моделирование потерь и оптимизация затрат на защиту / М.Р. Белалов // Вестник евразийской науки. – 2025. – Т. 17, № S4. – EDN QSKHXS.
7. Юрцев, А.Н. Особенности информационной безопасности банков / А.Н. Юрцев // Международный журнал гуманитарных и естественных наук. – 2023. – № 4-4(79). – С. 142-145. – DOI 10.24412/2500-1000-2023-4-4-142-145. – EDN BKOJJO.
8. Мартынюк, М.С. Организационно-управленческие механизмы обеспечения кибербезопасности российских компаний / М.С. Мартынюк // Финансовые рынки и

банки. – 2023. – № 6. – С. 5-9. – EDN CAILLU.

9. Айбуева, Р.А.М. Кибербезопасность компаний: важность обучения сотрудников цифровой грамотности для защиты корпоративных данных / Р.А.М. Айбуева, Х.Ш. Насуров // Экономика и управление: проблемы, решения. – 2025. – Т. 15, № 2(155). – С. 5-11. – DOI 10.36871/ek.up.p.r.2025.02.15.001. – EDN BPTTAC.

10. Багдасарян, Г.Ф. Кибербезопасность и киберугрозы современного малого и среднего российского бизнеса / Г.Ф. Багдасарян // Вестник евразийской науки. – 2023. – Т. 15, № S2. – EDN AGATBP.

11. Половченко, М.А. Информационная безопасность малых и средних предприятий / М.А. Половченко // Актуальные вопросы современной экономики. – 2025. – № 1. – С. 808-815. – EDN IOLIBK.

12. Трофимова, Н.Н. Индустрия 4.0: баланс между инновациями и рисками кибербезопасности для производственных предприятий / Н.Н. Трофимова // Экономика и управление: проблемы, решения. – 2025. – Т. 11, №2(155). – С. 32-38. – DOI 10.36871/ek.up.p.r.2025.02.11.005. – EDN SEGSGG.

13. Ламинина, О.Г. Философия информационной гигиены: несколько простых способов защитить организацию от утечки данных / О.Г. Ламинина, Р.А. Ламинин // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. – 2022. – № 8. – С. 92-97. – DOI 10.37882/2223-2966.2022.08.25. – EDN ZNPZUH.

14. Ан, Д.С. Формирование культуры информационной безопасности в организации: эффективность использования чек-листов и инфографики в процессе корпоративного обучения / Д.С. Ан, А.С. Зуфарова // ЦИТИСЭ. – 2025. – № 3(45). – С. 455-470. – EDN PRDJSE.

15. Садыхбекова, Л.Д. Некоторые проблемы разработки модели оценки мер защиты информации в системах промышленной автоматизации / Л. Д. Садыхбекова // Журнал высоких гуманитарных технологий. – 2025. – № 2(9). – С. 23-32. – EDN YEINZU.

---

**Долбня Наталия Валериевна**, канд. экон. наук, доцент кафедры бизнес-информатики, ФГБОУ ВО «Донецкий государственный университет», Донецк, Россия

E-mail: [nataliadolbnya@mail.ru](mailto:nataliadolbnya@mail.ru)

ORCID: 0000-0001-7087-6786

AuthorID: 970764

**Шпак Глеб Евгеньевич**, магистр кафедры бизнес-информатики, ФГБОУ ВО «Донецкий государственный университет», Донецк, Россия

E-mail: [g.shpak.e.02@gmail.com](mailto:g.shpak.e.02@gmail.com)

*Поступила в редакцию 01.12.2025 г.*

UDC 330.46:332+004.056

DOI 10.5281/zenodo.18048666

**DOLBANYA Natalia**<sup>1</sup>,  
**SHPAK Gleb**<sup>1</sup>

<sup>1</sup> Donetsk State University, Universitetskaya str., 24, Donetsk, Russia, 283001

## **BUSINESS DIGITAL VULNERABILITY: THE EVOLUTION OF CYBER THREATS**

In the context of rapid digital transformation, cybersecurity has ceased to be a narrowly technical issue and has become a strategic component of corporate risk management, directly affecting a company's valuation, reputation, and investment attractiveness. This study systematizes contemporary cyber threats from phishing and fraud to sophisticated attacks involving ransomware and double extortion and demonstrates their economic consequences: direct financial losses, operational downtime of critical business processes, regulatory sanctions, and reputational damage.

Through systematic and comparative analysis, the authors identify key differences between small and medium-sized enterprises (SMEs) and large organizations. SMEs' compact yet highly concentrated IT infrastructure renders them vulnerable to single incidents that can threaten the very existence of the business, whereas large enterprises – despite having mature security systems – suffer multi-million-dollar direct and indirect losses.

The article proposes a unified model of the cyberattack lifecycle and outlines attacker tactics, including social engineering, exploitation of remote access vulnerabilities, and data exfiltration through legitimate cloud channels. For the first time, a differentiated matrix of protective measures is presented ranging from a baseline level of “cyber hygiene” for SMEs to advanced practices for large enterprises, such as Zero Trust architecture, SIEM/XDR platforms, Threat Hunting, and quantifiable metrics for evaluating staff cybersecurity training effectiveness. From an economic perspective, the study emphasizes that investments in information security should be viewed not as costs, but as a mechanism for reducing risk premiums and enhancing resilience to shocks.

The paper also argues for the necessity of state- or industry-led standardization of basic cybersecurity measures for SMEs, which would mitigate systemic risks across the entire digital economy. The findings confirm that effective cybersecurity requires a systemic, rather than fragmented, approach one that is fully integrated into the corporate value management strategy at all levels of governance.

**Key words:** *cybersecurity, digital economy, cyber threats, information security, cyber risks, digital infrastructure, phishing, ransomware.*

### **References**

1. Annamyradova, A.M., Ishangulyyeva, M.S., Abyllayev, J. & Allanazarov, M. (2023). [Cybersecurity in the digital economy: current threats and protection]. *Matritsa nauchnogo poznaniya = Scientific Matrix of Cognition*, 9-1, 205–207. (In Russian).
2. Islamgereeva, Ya.S. & Edisultanova, Z.R. (2025). [Cybersecurity in the digital economy: challenges, threats and defense strategies]. *Nauchnyy byulleten' Chechenskogo gosudarstvennogo universiteta im. A.A. Kadyrova = Scientific Bulletin of Kadyrov Chechen State University*, 2(6), 21–26. DOI 10.36684/118-2025-2-6-21-26. (In Russian).
3. Martynova, T.L. (2024). [Digitalization of the information society's economy and cybersecurity of social services]. *Vestnik Universiteta imeni O.E. Kutafina (MGYuA) = Kutafin Moscow State Law University Bulletin*, 10(122), 77–84. DOI 10.17803/2311-5998.2024.122.10.077-084. (In Russian).

4. Mirgorskaya, M.G., Anichkina, O.A. & Ivanova, S.S. (2024). [The impact of the digital economy on enterprise economic security]. *Innovatsionnoe razvitie ekonomiki = Innovative Development of the Economy*, 1(79), 95–99. DOI 10.51832/222379842024195. (In Russian).
5. Buevich, A.P. (2025). [Cyber threats as a modern challenge to the security of Russia's banking sector]. *Natsional'naya bezopasnost' / Nota Bene = National Security / Nota Bene*, 4, 46–55. DOI 10.7256/2454-0668.2025.4.74921. (In Russian).
6. Belalov, M.R. (2025). [Cyber risks as a new class of operational banking risks: economic assessment, loss modeling, and optimization of protection costs]. *Vestnik Yevraziyskoy nauki = The Eurasian Scientific Journal*, 17(S4). (In Russian).
7. Yurtshev, A.N. (2023). [Specifics of banking information security]. *Mezhdunarodnyy zhurnal gumanitarnykh i estestvennykh nauk = International Journal of Humanities and Natural Sciences*, 4-4(79), 142–145. DOI 10.24412/2500-1000-2023-4-4-142-145. (In Russian).
8. Martynyuk, M.S. (2023). [Organizational and managerial mechanisms for ensuring cybersecurity of Russian companies]. *Finansovyye rynki i banki = Financial Markets and Banks*, 6, 5–9. (In Russian).
9. Aibueva, R.A.-M. & Nasurov, Kh.Sh. (2025). [Cybersecurity of companies: the importance of training employees in digital literacy to protect corporate data]. *Ekonomika i upravleniye: problemy, resheniya = Economics and Management: Problems, Solutions*, 15(2)(155), 5–11. DOI 10.36871/ek.up.p.r.2025.02.15.001. (In Russian).
10. Bagdasaryan, G.F. (2023). [Cybersecurity and cyber threats facing modern Russian small and medium-sized businesses]. *Vestnik Yevraziyskoy nauki = The Eurasian Scientific Journal*, 15(S2). (In Russian).
11. Polovchenko, M.A. (2025). [Information security of small and medium enterprises]. *Aktual'nyye voprosy sovremennoy ekonomiki = Current Issues of Modern Economics*, 1, 808–815. (In Russian).
12. Trofimova, N.N. (2025). [Industry 4.0: balancing innovation and cybersecurity risks for manufacturing enterprises]. *Ekonomika i upravleniye: problemy, resheniya = Economics and Management: Problems, Solutions*, 11(2)(155), 32–38. DOI 10.36871/ek.up.p.r.2025.02.11.005. (In Russian).
13. Laminina, O.G. & Laminin, R.A. (2022). [The philosophy of information hygiene: several simple ways to protect an organization from data leaks]. *Sovremennaya nauka: aktual'nyye problemy teorii i praktiki. Seriya: Estestvennyye i tekhnicheskiye nauki = Modern Science: Current Issues of Theory and Practice. Series: Natural and Technical Sciences*, 8, 92–97. DOI 10.37882/2223-2966.2022.08.25. (In Russian).
14. An, D.S. & Zufarova, A.S. (2025). [Building a culture of information security in organizations: effectiveness of using checklists and infographics in corporate training]. *TsITISE = CITISE*, 3(45), 455–470. (In Russian).
- Sadykhbekova, L.D. (2025). [Certain issues in developing a model for evaluating information protection measures in industrial automation systems]. *Zhurnal vysokikh gumanitarnykh tekhnologiy = Journal of Advanced Humanities and Technologies*, 2(9), 23–32. (In Russian).

---

**Dolbnya Natalia**, Candidate of Economic Sciences, Associate Professor of the Department of Business Informatics, Donetsk State University, Donetsk, Russia  
E-mail: [nataliadolbnya@mail.ru](mailto:nataliadolbnya@mail.ru)  
ORCID: 0000-0001-7087-6786  
AuthorID: 970764

**Shpak Gleb**, Master of the Department of Business Informatics, Donetsk State University,  
Donetsk, Russia  
E-mail: [g.shpak.e.02@gmail.com](mailto:g.shpak.e.02@gmail.com)

*Received 01.12.2025*