РАЗДЕЛ 5
ЭКОНОМИКА

УДК 338

ЭКОНОМИЧЕСКИЕ ПОСЛЕДСТВИЯ КИБЕРИНЦИДЕНТОВ ДЛЯ ХОЗЯЙСТВУЮЩЕГО СУБЪЕКТА И МЕТОДЫ ИХ КОЛИЧЕСТВЕННОЙ ЦЕНКИ

Ляховая А.А., Бородина Ю.И.
Южно-Российский институт управления- филиал Российской академии народного хозяйства и государственной службы при Президенте РФ

Исследование посвящено анализу экономических последствий киберинцидентов для хозяйствующего субъекта в условиях цифровизации хозяйственной деятельности. Обосновано понимание киберинцидента как внутреннего цифрового шока, влияющего на операционные процессы, финансовые результаты, инвестиционную динамику и занятость. Систематизированы направления ущерба и предложен матричный метод количественной оценки, обеспечивающий перевод вероятностных и качественных характеристик инцидента в сопоставимое стоимостное выражение. Разработанный подход ориентирован на повышение обоснованности управленческих решений в сфере киберустойчивости предприятий.

Ключевые слова: киберинцидент, экономический ущерб, хозяйствующий субъект, цифровые риски, количественная оценка, матричная модель, киберустойчивость.

ECONOMIC CONSEQUENCES OF CYBER INCIDENTS FOR AN ECONOMIC ENTITY AND METHODS OF THEIR QUANTITATIVE ASSESSMENT

Lyakhovaya A.A, Borodina Yu. I.
South Russian Institute of Management is a branch of the Russian Presidential Academy of National Economy and Public Administration

The study is devoted to the analysis of the economic consequences of cyber incidents for an economic entity in the context of digitalization of economic activity. The understanding of a cyber incident as an internal digital shock affecting operational processes, financial results, investment dynamics and employment is substantiated. The directions of damage are systematized and a matrix method of quantitative assessment is proposed, which ensures the translation of the probabilistic and qualitative characteristics of the incident into a comparable value expression. The developed approach is aimed at increasing the validity of management decisions in the field of cyber resilience of enterprises.

Key words: cyber incident, economic damage, business entity, digital risks, quantitative assessment, matrix model, cyber resilience.

Современная экономическая система функционирует в условиях углубляющейся цифровой взаимозависимости хозяйствующих субъектов, при которой информационная инфраструктура постепенно приобретает статус ключевого производственного ресурса, сопоставимого по значимости с капиталом и трудом. Расширение цифровых контуров управления, финансовых расчетов, логистических операций и взаимодействия с контрагентами формирует качественно новую конфигурацию рисков, среди которых киберинциденты занимают особое место вследствие их способности вызывать комплексные экономические потери, выходящие за пределы прямого ущерба информационным системам. Нарушение целостности данных, блокирование цифровых сервисов, компрометация коммерческой информации и остановка технологических процессов трансформируются в сбои производственной деятельности, разрывы контрактных отношений, утрату рыночных позиций и снижение занятости, что придает проблематике экономических последствий киберинцидентов системный характер.

Объекты и методы исследования

Объектом исследования выступают экономические процессы функционирования хозяйствующего субъекта в условиях воздействия киберинцидентов, проявляющиеся через изменения производственной, финансовой и трудовой динамики. Методологическую основу составляют методы экономического анализа, сравнительного и структурного подхода, а также элементы экономико-математического моделирования, позволяющие количественно интерпретировать последствия цифровых нарушений и обосновать их стоимостную оценку.

Результаты и их обсуждение

За последние 5 лет проблематика киберинцидентов особенно актуализировалась. в По данным от компании Check Point Research, в 2021 году число кибератак против компаний по всему миру выросло на 40% относительно 2020 года. В среднем, в 2021 году каждая организация подвергалась 925 атакам еженедельно. В 2023 году угрозы в сфере кибербезопасности для бизнеса сохранялись на высоком уровне. Согласно данным группы компаний «Солар», к августу 2024 года доля целенаправленных кибератак на российские организации существенно возросла, достигнув 44%, что указывает на усиление опасности со стороны опытных хакеров. По статистике коммерческих центров мониторинга, в России финансовые потери от примерно каждого пятого инцидента могут оказаться более миллиона рублей

При этом практика реагирования на киберинциденты преимущественно сосредоточена на техническом восстановлении инфраструктуры, в то время как экономические последствия фиксируются постфактум и редко подвергаются системной количественной оценке. В результате управленческие решения в сфере кибербезопасности принимаются при ограниченной информации о масштабах потенциальных потерь, что снижает обоснованность инвестиционной политики и искажает приоритеты распределения ресурсов внутри хозяйствующего субъекта, что обуславливает актуальность исследования.

Касаемо правого регулирования исследуемого вопроса, в настоящее время существует ряд нормативных документов и инструкций коммерческих организаций, описывающих действия специалистов при расследовании и реагировании на компьютерные атаки и оценке их последствий. Вместе с тем, в государственных стандартах не определены критерии и показатели оценки качества проведения расследования киберинцидентов. Например, в руководящем документе ГОСТ Р 59709-20226 представлены только термины и определения, а также их взаимосвязи в рамках данных процессов. В документе ГОСТ Р 59712-20227, приведено только организационное описание действий подразделений управления киберинцидентами.

В методическом документе Федеральной службы по техническому и экспортному контролю «Методика оценки угроз безопасности информации» перечислены десять основных тактик и соответствующие им типовые техники, используемые для построения сценариев реализации угроз безопасности информации. При разработке данного перечня за основу взята матрица MITRE ATT&CK. Согласно ГОСТ Р ИСО/МЭК ТО 18044-200710 при обнаружении первых признаков инцидента ИБ перед компьютерными криминалистами появляется задача определения их причин. В связи с этим производится сбор цифровых артефактов, основными источниками которых являются: копии жестких дисков, дампы оперативной памяти, журналы событий безопасности, а также трафик сетевых устройств.

Однако текущие нормативы не способны в полной мере оценить всю совокупность последствий на нарушения информационной безопасности предприятия, так как на современном этапе экономические последствия киберинцидентов охватывают все ключевые аспекты деятельности хозяйствующего субъекта (Таблица 1).

Таблица 1

Последствия киберинцидента для хозяйствующего субъекта

Направление воздействия	**Конкретные проявления киберинцидента**	**Экономические последствия для предприятия**	**Потенциальные показатели количественной оценки**
Операционная деятельность	Блокирование информационных систем управления производством, логистикой, продажами	Снижение объемов выпуска и реализации продукции, простои, нарушение производственных циклов	Потери выручки, объем недопроизводства, длительность простоя
Финансовые потоки	Недоступность платежной инфраструктуры, искажение финансовых данных	Нарушение расчетов с контрагентами, кассовые разрывы, рост штрафных санкций	Просроченная кредиторская задолженность, штрафные выплаты, снижение ликвидности
Издержки функционирования	Необходимость восстановления систем, привлечения внешних специалистов, модернизации защиты	Рост внеплановых расходов, перераспределение бюджета в ущерб развитию	Дополнительные операционные затраты, доля расходов на ИБ в издержках
Рыночные позиции	Утечка коммерческой информации, сбои клиентских сервисов	Потеря клиентов, снижение доверия, ухудшение конкурентного положения	Снижение объема заказов, отток клиентов, изменение доли рынка
Инвестиционная активность	Перенос или отмена проектов из-за необходимости финансирования восстановления	Замедление технологического обновления и расширения бизнеса	Сокращение инвестиций, доля отложенных проектов
Трудовые ресурсы	Простой персонала, перераспределение функций, оптимизация численности	Снижение занятости, изменение структуры кадров, падение производительности труда	Потери рабочего времени, сокращение штата, выработка на работника
Деловая репутация	Публичное раскрытие инцидента, снижение доверия партнеров	Ухудшение условий контрактов и финансирования	Изменение стоимости заимствований, число расторгнутых контрактов
Стратегическая устойчивость	Долгосрочное снижение цифровой надежности и инвестиционной привлекательности	Утрата темпов развития, рост стратегических рисков	Темпы роста выручки, рентабельность, рыночная стоимость

Представленная структура демонстрирует, что экономический ущерб предприятия формируется как совокупность взаимосвязанных эффектов, охватывающих текущую деятельность и долгосрочную динамику развития. Подобное распределение последствий по функциональным контурам позволяет перейти от описательного восприятия киберинцидента к его измерению через систему экономических показателей, сопоставимых с традиционными факторами хозяйственного риска.

Вместе с тем, необходимо учитывать существенные юридические последствия киберинцидентов. На сегодняшний день штрафы и судебные издержки могут составлять значительную долю стоимости киберинцидента. Для компаний с большими массивами персональных данных регуляторный ущерб от кибератаки часто становится критичным. Помимо текущих штрафов по ст. 13.11 КоАП РФ, возможно применение оборотных штрафов за утечки данных, которые могут исчисляться сотнями миллионов рублей. Кроме того, в России начинает формироваться практика коллективных исков от пострадавших пользователей. Юридическое сопровождение таких процессов, выплаты компенсаций и затраты на уведомление субъектов данных формируют внушительную статью расходов. Требования регуляторов становятся одним из главных драйверов роста стоимости инцидентов.

Так, например, если компания с оборотом в **1,2 млрд руб.** в год допустила утечку **10 000 записей персональных данных клиентов, в том числе ФИО, телефонов, e-mail, платежных данных то совокупность последствий будет следующая (Таблица 2).**

Таблица 2

Юридические последствия киберинцидента

Штраф / статья затрат	**Причина штрафа / расходов**	**Размер штрафа / затрат**	**Прочие обязанности компании по ликвидации инцидента**
Административные штрафы (ст. 13.11 КоАП РФ)	Утечка персональных данных клиентов, включая платежную информацию. Нарушение требований к защите ПДн, обработка ПДн без достаточных мер безопасности, отягчающие обстоятельства (массовость, чувствительность данных)	300 000 – 1 000 000 руб. (в зависимости от квалификации и повторности нарушения)	Проведение внутренней проверки, подготовка материалов для регулятора, устранение выявленных нарушений
Выполнение требований 152-ФЗ	Законодательная обязанность реагирования на инцидент с ПДн	1,3 – 2,7 млн руб.	Внутреннее расследование, фиксация инцидента, уведомление Роскомнадзора, уведомление 10 000 субъектов ПДн, организация поддержки клиентов
Гражданско-правовые иски	Индивидуальные и коллективные иски о компенсации морального вреда со	4,5 – 5 млн руб.	Судебное и юридическое сопровождение,

	стороны пострадавших клиентов		участие в разбирательствах, возможные мировые соглашения
Расследование инцидента	Необходимость расследования причин инцидента и восстановления уровня безопасности	1,5 – 4,5 млн руб.	ИБ-аудит, внедрение внеплановых мер защиты
Репутационные и коммерческие потери	Снижение доверия клиентов, падение продаж, рост оттока, увеличение маркетинговых затрат	6 – 12 млн руб. (0,5–1% годового оборота)	Антикризисные коммуникации, PR-активности, программы удержания клиентов

Систематизация экономических последствий киберинцидента по функциональным контурам деятельности хозяйствующего субъекта логически подводит к необходимости их количественного измерения, поскольку именно сопоставимость эффектов в стоимостном или производственном выражении позволяет интегрировать цифровые риски в систему экономического анализа и управленческого планирования. При этом специфика киберинцидента как внутреннего цифрового шока предопределяет многоуровневый характер оценки, в которой фиксируются как прямые потери текущего периода, так и отложенные изменения динамики хозяйственной деятельности. Методический инструментарий количественной оценки в данном контексте формируется на стыке анализа производственных потерь, финансовых отклонений и институциональных эффектов, отражающих изменение поведения предприятия и его контрагентов.

Оценка операционных потерь, возникающих вследствие блокирования или деградации информационных систем, основывается на сопоставлении фактических параметров выпуска и реализации с расчетной траекторией деятельности при отсутствии инцидента. В простейшем приближении потери выручки определяются через произведение среднесуточного объема продаж на длительность простоя, скорректированное на коэффициент последующего восстановления спроса, отражающий способность предприятия компенсировать недопоставку в последующие периоды. Более точное измерение предполагает использование производственных функций или временных рядов выпуска, позволяющих оценить отклонение фактической производственной динамики от ожидаемой. В подобной модели киберинцидент интерпретируется как структурный разрыв во временном ряду, а величина операционного ущерба выражается через интеграл недополученного выпуска за период восстановления.

Финансовые последствия, связанные с нарушением расчетов и искажением данных, количественно выявляются через анализ отклонений денежных потоков и структуры обязательств. Методически обоснованным является сопоставление фактического графика поступлений и платежей с плановым бюджетом движения денежных средств, что позволяет выделить кассовый разрыв, индуцированный киберинцидентом. Дополнительные потери оцениваются через начисленные штрафы, пени и рост стоимости краткосрочного заимствования, вызванный ухудшением платежной дисциплины. В агрегированном выражении финансовый ущерб определяется как сумма прямых санкций и стоимости привлеченного капитала, необходимого для компенсации временной утраты ликвидности.

Измерение роста издержек функционирования требует выделения затрат, непосредственно обусловленных инцидентом, из общей динамики операционных расходов. Для этого применяется подход инкрементального анализа, при котором фактические расходы периода сопоставляются с нормативной или трендовой траекторией затрат при сохранении прежнего режима деятельности. Разница интерпретируется как дополнительные издержки восстановления и усиления киберустойчивости. В расширенной модели учитывается также вытеснение инвестиционных расходов, когда финансирование антикризисных мер осуществляется за счет переноса проектов развития. В этом случае количественная оценка включает дисконтированную стоимость отложенных инвестиционных эффектов, отражающую упущенную экономическую выгоду.

Рыночные последствия киберинцидента проявляются через изменение спроса и контрактных условий, что требует применения методов оценки утраченной клиентской базы и ухудшения конкурентных позиций. Практически применимым является анализ клиентов, позволяющий определить долю контрагентов, прекративших сотрудничество после инцидента, а также динамику объемов заказов у сохранившихся партнеров. Потери выручки в данном случае рассчитываются как разность между прогнозируемым объемом продаж без инцидента и фактическим уровнем спроса в посткризисный период, с учетом средней маржинальности продукции. Для долгосрочной оценки используется метод дисконтированных денежных потоков, позволяющий измерить снижение ожидаемой стоимости клиентских отношений вследствие падения доверия.

Оценка влияния на занятость и производительность труда опирается на анализ изменений использования рабочего времени и кадровой структуры. Потери трудового потенциала в период простоя определяются через произведение численности персонала, вовлеченного в нарушенные процессы, на длительность вынужденной неэффективной занятости и среднюю добавленную стоимость на работника. При последующих сокращениях численности количественный эффект отражается через снижение фонда оплаты труда и сопутствующее уменьшение выпуска, что позволяет оценить структурный ущерб занятости. Дополнительно применяется показатель недополученной добавленной стоимости, рассчитанный как произведение сокращенной численности на среднюю производительность труда, скорректированную на отраслевую динамику.

Репутационные и финансово-рыночные эффекты количественно выявляются через изменение условий контрактов и стоимости привлеченного капитала. В корпоративной практике подобные последствия фиксируются в росте процентных ставок по займам, ужесточении требований обеспечения и сокращении сроков контрактов.

Экономический ущерб определяется через разность приведенной стоимости обязательств до и после инцидента, что отражает удорожание финансирования вследствие снижения доверия. Для публичных компаний применяется событийный анализ рыночной стоимости, при котором измеряется отклонение капитализации от ожидаемой динамики в период раскрытия информации о киберинциденте.

Стратегические последствия, связанные с замедлением развития и утратой инвестиционной привлекательности, требуют оценки через долгосрочные показатели экономической динамики предприятия.

Методически оправданным является сравнение фактической траектории выручки, рентабельности и инвестиций с контрфактическим сценарием развития без киберинцидента, построенным на основе исторических темпов роста или отраслевых аналогов. Разница между сценариями интерпретируется как стратегический ущерб, отражающий снижение потенциала развития. В интегральном выражении он может быть представлен через уменьшение дисконтированной стоимости будущих денежных потоков, обусловленное устойчивым ухудшением экономических параметров.

В этом ключе, как отмечает Хамидуллин Д.Р., «учитывая сложность оценки киберрисков, необходимо использовать инструменты анализа рисков, которые обеспечивают целостный, дифференцированный подход к выявлению киберрисков, выходящий за рамки традиционного внимания к безопасности и включающий другие проблемы, такие как финансовые или операционные последствия. Анализ киберрисков использует количественные, полуколичественные или качественные методы для определения уровня риска для установки, системы или компонента. Однако из-за ограниченных данных и проблем с моделированием динамических аспектов угрозы и уязвимости количественные методы определения киберриска по своей сути являются ошибочными». В связи с этим представляется необходимым разработка новых подходов к оценке последствий киберинцидентов, учитывающие данные ошибки.

Предлагаемый метод формируется как прикладная матрица, в которой каждый элемент служит для перевода качественного эффекта инцидента в количественную оценку, позволяющую получить как индекс относительного ущерба, так и его потенциальное стоимостное выражение. Применение матрицы начинается с идентификации зон воздействия внутри хозяйствующего субъекта и определения базовых показателей экспозиции, после чего для каждой зоны фиксируются оценки немедленных потерь, краткосрочных косвенных потерь и долгосрочных структурных последствий, далее эти оценки агрегируются с учетом вероятности и временного коэффициента восстановления (таблица 3).

Таблица 3

Матрица оценки последствий кибернцицидента

Зона воздействия	**Базовый показатель экспозиции**	**Оценка немедленных потерь (0–5)**	**Оценка краткосрочных косвенных потерь (0–5)**	**Оценка долгосрочных структурных потерь (0–5)**	**Вероятность реализации последствия, p (0–1)**	**Коэффициент времени восстановления (дни)**
Операционная деятельность	Среднесуточная выручка, руб.					
Финансовые потоки	Плановый денежный поток за период, руб.					
Издержки функционирования	Средние операционные расходы за период, руб.					
Рыночные позиции	Годовая выручка от ключевых клиентов, руб.					
Инвестиционная активность	Объем отложенных/планируемых инвестиций, руб.					
Трудовые ресурсы	Средняя добавленная стоимость на работника, руб./день					
Деловая репутация	Стоимость привлечения капитала или изменение стоимости заимствований					

В рамках данной методики для каждой зоны воздействия определяется базовая экспозиция, это показатель, позволяющий выразить максимальный потенциальный экономический эффект в стоимостном выражении, далее экспертным путем или с использованием эмпирических временных рядов присваиваются три субоценки влияния по шкале 0-5, где значение 0 означает отсутствие эффекта, значение пять соответствует полной утрате соответствующего компонента деятельности в рассматриваемом горизонте. Затем для учета вероятности реализации каждого вида потерь применяется множитель p находящийся в интервале от нуля до единицы, что позволяет снизить влияние редких событий на итоговый индекс ущерба, одновременно вводится временной коэффициент, измеряемый в днях для корректировки оценки операционных потерь с учетом длительности простоя или периода восстановления.

Стоимостная оценка ущерба по зонам дает инструмент для приоритизации инвестиций в защиту, оценки целесообразности страхового покрытия и разработки мер поддержки занятости в постинцидентный период. Внедрение матрицы предполагает регулярное обновление входных параметров и переоценку весов по мере изменения внутренней структуры предприятия и внешней среды, что обеспечивает адаптивность метода и возможность его использования как в оперативной аналитике, так и в стратегическом планировании.

Выводы

Таким образом, проведенное исследование позволяет утверждать, что киберинцидент в современной цифровой экономике выступает системным фактором трансформации хозяйственной деятельности, воздействуя на операционные процессы, финансовые потоки, инвестиционную динамику и занятость через взаимосвязанные механизмы распространения ущерба. Разработанная в работе матричная модель количественной оценки создает методологическую основу для перевода разнородных последствий цифрового нарушения в сопоставимое стоимостное выражение, что обеспечивает интеграцию киберрисков в систему экономического анализа и управленческого планирования. Практическая значимость предложенного подхода заключается в возможности формирования обоснованных решений по распределению ресурсов, страховой защите и поддержанию устойчивости занятости, что усиливает экономическую рациональность политики киберустойчивости хозяйствующего субъекта.

Список литературы

1. Национальный стандарт РФ ГОСТ Р 59709-2022 "Защита информации. Управление компьютерными инцидентами. Термины и определения" (утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 29 ноября 2022 г. № 1375-ст) // СПС «Гарант» (дата обращения: 01.03.2025)
2. ГОСТ Р 59712-2022 "Защита информации. Управление компьютерными инцидентами. Руководство по реагированию на компьютерные инциденты" // СПС «Гарант» (дата обращения: 01.03.2025)
3. "Методический документ. Методика оценки угроз безопасности информации" (утв. ФСТЭК России 05.02.2021) // СПС «Консультант плюс» (дата обращения: 01.03.2025)
4. Национальный стандарт РФ ГОСТ Р ИСО/МЭК ТО 18044-2007 "Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности" (утв. приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2007 г. N 513-ст) // СПС «Гарант» (дата обращения: 01.03.2025)
5. Мусхаджиева Т. И., Исаева Л. М. Кибербезопасность в цифровой экономике: риски, стратегии защиты и страхование // Вестник науки. 2025. №6 (87)
6. Смирнов С.И., Еремеев М.А., Магомедов Ш.Г., Изергин Д.А. Критерии и показатели оценивания качества проведения расследования инцидента информационной безопасности при целевой кибератаке.

Russian Technological Journal. 2024;12(3):25-36. https://doi.org/10.32362/2500-316X-2024-12-3-25-36. EDN: LNWLOK
7. Хамидуллин Р.Д. Методика оценки киберрисков корпоративного центра ИТ-мониторинга // КЭ. 2023. №12.
8. Информационный портал «Cisoclub» [Электронный ресурс] – URL: https://cisoclub.ru/kak-gramotno-poschitat-ushherb-ot-kiberincidentov-dlja-finansovogo-planirovanija/ (Дата обращения: 02.03.2025)
9. Информационный портал «Falconegaze» https://falcongaze.com/ru/pressroom/publications/kiberbezopasnost/ekonomika-kiberincidenta.html (Дата обращения: 02.03.2025)

Ляховая Анастасия Алексеевна, студент, Южно-Российский институт управления- филиал Российской академии народного хозяйства и государственной службы при Президенте РФ.
344002, Россия, г. Ростов-на-Дону, ул. Пушкинская, 70/54,
Телефон: 89085166017
E-mail: lyakhovaya.nastya@mail.ru

Бородина Юлия Ивановна, кандидат экономических наук, доцент, Южно-Российский институт управления – филиал Российской академии народного хозяйства и государственной службы при Президенте РФ
344002, Россия, г. Ростов-на-Дону, ул. Пушкинская, 70/54
Телефон: 89281618188
E-mail: borodina-yi@ranepa.ru