ИНФОРМАЦИОННАЯ ЗАЩИТА КАК ЭЛЕМЕНТ СТРАТЕГИЧЕСКОГО ПЛАНИРОВАНИЯ И УПРАВЛЕНИЯ РИСКАМИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ ЭКОНОМИКИ

ИНЕВАТОВА Ольга Александровна
кандидат экономических наук, доцент
ТЫРСИН Артем Павлович
студент
Оренбургский государственный университет
г. Оренбург, Россия

В условиях цифровизации экономики кибербезопасность становится критическим элементом устойчивости бизнеса и национальной безопасности. Данная статья рассматривает киберугрозы как экономические риски, а инвестиции в кибербезопасность — как инструмент минимизации потенциального ущерба. Проанализированы модели оценки выгод от защитных мер, рассмотрены эмпирические примеры инцидентов, подтверждающие экономическую целесообразность проактивной киберполитики. Сделан вывод о необходимости интеграции киберрисков в стратегическое планирование компаний и государств.

Ключевые слова: цифровизация экономики, информационная защита, стратегическое планирование, риски в деятельности предприятий, кибербезопасность, инвестиции в информационную защиту, цифровая среда.

Введение. Развитие цифровых технологий приводит к стремительному росту числа киберинцидентов. Атаки на информационную инфраструктуру становятся все более изощренными, затрагивая не только частные компании, но и государственные учреждения. По данным IBM (2023), средний ущерб от одной утечки данных составил $4,45 млн, а к 2025 г. общий мировой ущерб от киберпреступности может достичь $10,5 трлн ежегодно.

В связи с этим вопрос инвестиций в кибербезопасность выходит за рамки технической проблематики и становится предметом экономического анализа. Основная цель статьи – показать, что в современных условиях защита от киберугроз часто обходится дешевле для предприятий, чем последствия их реализации.

1. Кибербезопасность как объект экономического анализа.

В экономике, управление рисками рассматривается через соотношение между вероятностью наступления события и его потенциальным ущербом. Киберугрозы можно анализировать аналогично, применяя модели оценки эффективности затрат на защиту (https://www.upguard.com/).

Одной из таких моделей является соотношение:

$C < P \times L$,

где C – затраты на меры безопасности,

P – вероятность наступления инцидента,

L – величина потенциального ущерба.

Если стоимость защиты меньше ожидаемого убытка, инвестиции считаются экономически обоснованными.

Кроме того, на недоинвестирование в безопасность влияют экстерналии: компании могут перекладывать последствия инцидентов на клиентов или партнеров. Информационная асимметрия также мешает корректной оценке рисков, особенно в малом и среднем бизнесе.

2. Эмпирические примеры и кейсы.

Характерным примером является кибератака на Colonial Pipeline (США, 2021), которая привела к остановке работы трубопроводной системы и временной нехватке топлива на востоке страны. Прямой ущерб составил более $100 млн, а косвенные потери были еще выше. При этом эксперты оценивают стоимость своевременной модернизации системы безопасности

в сумму до $10 млн.

Другой случай – утечка данных из Equifax (2017), затронувшая 147 млн человек. Компания понесла прямые расходы в размере $700 млн. При этом адекватные превентивные меры могли стоить в десятки раз меньше.

Другим знаковым инцидентом стала атака на компанию Yahoo, в результате которой в 2013-2014 гг. были скомпрометированы учетные данные всех 3 миллиардов пользователей. Ущерб от инцидента включал не только прямые затраты на урегулирование последствий, но и значительное снижение рыночной стоимости компании. Сумма сделки по продаже Yahoo компании Verizon была снижена на $350 млн – с $4,83 млрд до $4,48 млрд, что отражает прямое влияние киберинцидента на стоимость бизнеса.

Ещё один пример – инцидент с атакой программой-вымогателем WannaCry в 2017 г., который поразил более 200 тысяч компьютеров в 150 странах. Серьёзно пострадала британская Национальная служба здравоохранения (NHS), что привело к отмене тысяч приёмов пациентов и нарушению работы медицинских учреждений. По оценке Национального аудиторского управления Великобритании, ущерб NHS составил около £92 млн. Анализ показал, что простые меры (обновление ОС и установка патчей безопасности) могли бы предотвратить атаку.

Эти кейсы демонстрируют, что своевременные инвестиции в защиту способны значительно сократить возможные убытки и снизить репутационные риски.

3. Кибербезопасность как стратегическая инвестиция.

В условиях стремительной цифровизации бизнес-среды кибербезопасность становится неотъемлемой частью стратегического управления и инвестиционного планирования. Для современных компаний информационная защита – это не просто форма затрат на IT-инфраструктуру, а долгосрочная инвестиция в устойчивость, непрерывность процессов и конкурентоспособность [1].

Во-первых, кибербезопасность позволяет снижать не только прямые операционные риски, но и репутационные, юридические и стратегические. В условиях высокой конкуренции инциденты, связанные с утечкой данных, могут подорвать доверие клиентов, вызвать отток пользователей и даже привести к снижению капитализации компании.

Во-вторых, соблюдение международных нормативных актов, таких как GDPR (в ЕС), HIPAA (в США) или ФЗ-152 (в России), требует от организаций внедрения эффективных механизмов защиты персональных данных. Несоблюдение этих требований ведёт к значительным штрафам и санкциям, что усиливает мотивацию к инвестициям в безопасность.

С экономической точки зрения, затраты на киберзащиту могут рассматриваться аналогично страховым премиям: это расходы, направленные на снижение вероятности убытков в будущем. В этом контексте показатель возврата инвестиций (ROI) приобретает особое значение:

$ROI = (L \times P - C) / C$,

где L – потенциальные убытки, P – вероятность инцидента,

C – затраты на защиту.

Если значение ROI положительно, то инвестиции в кибербезопасность являются экономически обоснованными.

Дополнительно важно учитывать так называемую стоимость простоя (downtime cost) – расходы, возникающие при временной недоступности сервисов. Для крупных промышленных, логистических или финансовых структур одна атака может привести к остановке бизнес-процессов и убыткам в миллионы долларов. Например, кибератака на Maersk (2017) обошлась компании в $300 млн, большая часть из которых – результат остановки цепей поставок.

Кроме того, на стратегическом уровне наличие устойчивой киберинфраструктуры способствует укреплению доверия со стороны инвесторов, акционеров и клиентов. Это особенно важно для публичных компаний, финансовых институтов и технологических стартапов, работающих в условиях высокой неопределённости и информационных рисков [2].

Таким образом, кибербезопасность приобретает статус не только операционного ин-

струмента, но и ключевого элемента стратегического планирования и управления рисками в цифровую эпоху.

Наряду с экономическим эффектом, кибербезопасность становится важным компонентом стратегического планирования компаний. В условиях высокой технологической взаимозависимости и глобальной цифровой трансформации управление киберрисками становится неотъемлемой частью корпоративного и государственного стратегического управления [3].

Во многих отраслях предприятия переходят от реактивного подхода к превентивной киберполитике, формируя долгосрочные стратегии цифровой устойчивости. Это означает не только инвестирование в технические средства защиты, но и интеграцию механизмов кибербезопасности в процесс принятия управленческих решений: от аудита поставщиков до оценки инвестиционных проектов (https://www.everytag.ru/leaks-in-healthcare-sphere). Киберриски рассматриваются как ключевые стратегические риски, наряду с операционными, правовыми и рыночными.

Финансовые и нефинансовые показатели всё чаще включают метрики, отражающие уровень зрелости в области ИБ (например, наличие систем мониторинга, готовность к инцидентам, скорость реагирования, обучение персонала). Наличие стратегического плана обеспечения кибербезопасности становится показателем зрелости управления и повышает доверие внешних стейкхолдеров, включая регуляторов, инвесторов и партнёров.

Особое внимание уделяется созданию систем управления инцидентами (Cyber Incident Response Plan, C-IRP), внедрению сценарного моделирования атак (Threat Modelling) и интеграции киберрисков в общекорпоративные системы оценки рисков (ERM – Enterprise Risk Management). Это позволяет организациям оперативно адаптироваться к внешним угрозам и минимизировать потери при их реализации.

Таким образом, кибербезопасность перестаёт быть функцией ИТ-отдела и становится сквозным стратегическим элементом, охватывающим корпоративное управление, финансы, HR, PR и юридическую службу. Это фундамент для построения цифрово устойчивых организаций в долгосрочной перспективе.

С точки зрения теории управления, стратегическое планирование – это процесс постановки долгосрочных целей организации, определения направлений развития и выработки механизмов достижения желаемых результатов с учётом внешних и внутренних факторов риска. В современном контексте цифровой экономики одним из таких факторов становится информационная безопасность [4].

Включение кибербезопасности в стратегическое планирование предполагает не только бюджетирование защитных мер, но и их интеграцию в ключевые бизнес-функции – финансовое планирование, управление персоналом, цифровые трансформации, инновационную деятельность и цепочки поставок. Это означает, что вопросы киберрисков должны учитываться уже на стадии разработки стратегий роста, выхода на новые рынки, внедрения новых технологий или цифровых сервисов.

Организации, ориентированные на устойчивое развитие, разрабатывают киберстратегии, включающие оценку угроз, сценарное моделирование, определение приоритетов инвестиций в ИБ и формирование культуры безопасности на всех уровнях (https://tass.ru/ekonomika/19369297). Такой подход способствует формированию так называемой цифровой устойчивости (cyber resilience), которая является критически важной для сохранения конкурентоспособности в долгосрочной перспективе.

Вывод. Цифровизация современного общества привела к качественно новому уровню взаимосвязанности, при котором устойчивость экономических субъектов во многом определяется их способностью противостоять киберугрозам. Кибербезопасность перестала быть сугубо технической сферой – сегодня она представляет собой важный экономический фактор, оказывающий прямое влияние на финансовые результаты, деловую репутацию и стратегическую устойчивость компаний.

Рассмотренные в статье примеры киберинцидентов, а также анализ затрат и потенциальных убытков показывают, что проактивные инвести-

ции в защиту информации зачастую являются более экономически целесообразными, чем покрытие последствий атак. Формализация оценки рисков и применение количественных моделей позволяют включить кибербезопасность в систему корпоративного управления наравне с другими ключевыми направлениями.

В условиях цифровой экономики кибербезопасность должна рассматриваться как элемент долгосрочной инвестиционной политики и инструмент устойчивого развития как на уровне отдельных организаций, так и на макроэкономическом уровне.

Цифровизация современного общества привела к качественно новому уровню взаимосвязанности, при котором устойчивость экономических субъектов во многом определяется их способностью противостоять киберугрозам. Кибербезопасность перестала быть сугубо технической сферой – сегодня она представляет собой важный экономический фактор, оказывающий прямое влияние на финансовые результаты, деловую репутацию и стратегическую устойчивость компаний [5].

Рассмотренные в статье примеры киберинцидентов, а также анализ затрат и потенциальных убытков показывают, что проактивные инвестиции в защиту информации зачастую являются более экономически целесообразными, чем покрытие последствий атак. Формализация оценки рисков и применение количественных моделей позволяют включить кибербезопасность в систему корпоративного управления наравне с другими ключевыми направлениями.

Более того, на современном этапе развития цифровой экономики кибербезопасность приобретает системообразующий характер – она формирует основу для стратегических решений на уровне как отдельных компаний, так и национальных экономик. Её интеграция в стратегическое планирование позволяет не только минимизировать потери от инцидентов, но и строить долгосрочную конкурентоспособность, основанную на доверии клиентов, партнёров и регуляторов.

В условиях глобальной цифровой конкуренции и быстро меняющейся ландшафтной структуры угроз организации, неспособные учитывать киберриски в своей стратегии, оказываются в уязвимом положении. Это особенно актуально для высокотехнологичных отраслей, финансового сектора, логистики, медицины и критически важной инфраструктуры, где последствия инцидентов могут быть катастрофическими.

Поэтому сегодня кибербезопасность должна рассматриваться не как отдельная функция, а как интегральная часть системы управления рисками (ERM) и устойчивого развития. Это предполагает участие высшего руководства, бюджетирование на уровне стратегических инициатив, регулярную оценку угроз и готовность к их отражению.

Таким образом, кибербезопасность в современном мире – это не просто защита от угроз, а основополагающий элемент стратегического управления, финансовой устойчивости и долгосрочного роста, без которого невозможно развитие цифровой экономики.

СПИСОК ЛИТЕРАТУРЫ

1. *Вострецова Е.В.* Основы информационной безопасности: учебное пособие для студентов вузов. – Екатеринбург: Изд-во Урал. ун-та, 2019. – 204 с.
2. *Дементьева М.А.* Киберпреступления в банковской сфере РФ: способы выявления и противодействия / М.А. Дементьева [и др.] // Экономические отношения. – 2021. – № 2. – С. 109-120.
3. *Иневатова О.А.* Кибератаки и их место в экономике промышленных предприятий / О.А. Иневатова, Е.В. Чеботаева // Наука сегодня: глобальные вызовы, пути развития: материалы XIV всерос. науч.-практ. конф., Рязань, 22 июня 2023 г. – Рязань: Изд-во «Концепция», 2023. – Сер. Гуманитарные исследования. – С. 197-201. – URL:https://www.elibrary.ru/item.asp?id=54259882 (дата обращения: 15.05.2025).
4. *Струнин Д.А.* Кибератаки и их влияние на цифровую экономику // Молодой ученый. – 2023. – № 5(452). – С. 15-16. – URL:https://moluch.ru/archive/452/99590/ (дата обращения: 15.05.2025).

5. *Чайковский Н.С.* Статистика киберпреступности в Российской Федерации / Н.С. Чайковский, М.А. Кухенная // Оценка социально-экономического развития: опыт и перспективы: сб. материалов междунар. конф. (Донецк, 04-05 апр. 2021 г.). – Донецк, 2021. – С. 399-401.

INFORMATION PROTECTION AS AN ELEMENT OF STRATEGIC PLANNING AND RISK MANAGEMENT IN THE CONTEXT OF THE DIGITALIZATION OF THE ECONOMY

INEVATOVA Olga Alexandrovna
Candidate of Sciences in Economics, Associate Professor
TYRSIN Artem Pavlovich
Student
Orenburg State University
Orenburg, Russia

In the context of the digitalization of the economy, cybersecurity is becoming a critical element of business sustainability and national security. This article considers cyber threats as economic risks, and investments in cybersecurity as a tool to minimize potential damage. Models for assessing the benefits of protective measures are analyzed, empirical examples of incidents confirming the economic feasibility of proactive cyber policy are considered. It is concluded that it is necessary to integrate cyber risks into the strategic planning of companies and states.
Keywords: digitalization of the economy, information security, strategic planning, risks in the activities of enterprises, cybersecurity, investments in information security, digital environment.