Гильченко Алексей Николаевич, студент
МФЮА
Gilchenko Aleksey Nikolaevich
MFUA

ВЛИЯНИЕ ИНФОРМАЦИОННЫХ УГРОЗ НА ЭКОНОМИЧЕСКУЮ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ: АНАЛИЗ И ПУТИ МИНИМИЗАЦИИ
THE IMPACT OF INFORMATION THREATS ON THE ECONOMIC SECURITY OF AN ENTERPRISE: ANALYSIS AND WAYS TO MINIMIZE

Аннотация. В статье рассматривается влияние информационных угроз на экономическую безопасность предприятия, проводится их анализ и предлагаются пути минимизации

Abstract. The article examines the impact of information threats on the economic security of an enterprise, analyzes them and suggests ways to minimize them

Ключевые слова: Минимизация, нестабильность, информационные угрозы, предприятия, экономическая безопасность

Keywords: Minimization, instability, information threats, enterprises, economic security

В современном мире, где цифровые технологии стремительно интегрируются во все сферы деятельности, предприятия сталкиваются с новыми вызовами, связанными с обеспечением экономической безопасности. Информация становится не только стратегическим ресурсом, но и объектом потенциальных угроз, способных нанести существенный ущерб финансовой стабильности и репутации организации.

Информационные угрозы, такие как кибератаки, утечки конфиденциальных данных, внутренние нарушения и технологические сбои, приобретают всё большую актуальность в бизнес-среде. Их реализация может привести к значительным финансовым потерям, нарушению производственных процессов и снижению доверия со стороны партнёров и клиентов. В условиях высокой конкуренции и нестабильной экономической ситуации обеспечение информационной безопасности становится неотъемлемой частью стратегии экономической устойчивости предприятия.

Несмотря на существование различных методов и стандартов управления информационными рисками, таких как ISO/IEC 27001 и ISO 31000, многие предприятия сталкиваются с трудностями в их адаптации и внедрении, особенно в условиях ограниченных ресурсов и недостаточной осведомлённости персонала. Это подчёркивает необходимость проведения комплексного анализа влияния информационных угроз на экономическую безопасность и разработки эффективных мер по их минимизации.

Цель данной статьи – проанализировать влияние информационных угроз на экономическую безопасность предприятия, выявить основные риски и предложить практические рекомендации по их снижению. Особое внимание уделяется интеграции информационной безопасности в общую систему управления рисками предприятия, а также рассмотрению современных подходов и инструментов, способствующих повышению устойчивости организации в условиях цифровой трансформации.

Информационные угрозы представляют собой потенциальные или реальные действия, способные нарушить конфиденциальность, целостность или доступность информации, что может повлечь за собой негативные последствия для функционирования предприятия. Классификация информационных угроз может быть проведена по различным признакам:

Экономическая безопасность предприятия – это состояние защищенности его экономических интересов от внутренних и внешних угроз, обеспечивающее устойчивое функционирование и развитие в долгосрочной перспективе. Ключевые компоненты экономической безопасности включают [1, с. 178]:

– Финансовая безопасность – обеспечение стабильности финансовых потоков и платежеспособности;

– Информационная безопасность – защита информационных ресурсов от несанкционированного доступа и нарушений;

– Кадровая безопасность – наличие квалифицированного персонала и предотвращение утечки кадров;

Правовая безопасность – соблюдение законодательства и защита прав предприятия;

– Технологическая безопасность – обеспечение надежности и эффективности технологических процессов.

Эти компоненты взаимосвязаны и в совокупности обеспечивают устойчивость и развитие предприятия в условиях внешних и внутренних вызовов.

Информационные угрозы оказывают прямое влияние на экономическую безопасность предприятия. Например, утечка конфиденциальной информации может привести к финансовым потерям, снижению конкурентоспособности и ущербу репутации. Кроме того, кибератаки могут нарушить производственные процессы, что повлияет на финансовые показатели и устойчивость предприятия.

Таким образом, эффективное управление информационными рисками является неотъемлемой частью стратегии обеспечения экономической безопасности. Предприятия должны интегрировать меры по информационной безопасности в общую систему управления рисками, чтобы минимизировать потенциальные угрозы и обеспечить стабильное функционирование в долгосрочной перспективе.

Оценка информационных угроз включает анализ вероятности их возникновения и потенциального воздействия на деятельность предприятия. Для этого используются как качественные, так и количественные методы оценки рисков. Качественные методы основаны на экспертных оценках и анализе сценариев, тогда как количественные методы предполагают использование статистических данных и математических моделей для определения вероятности и последствий угроз. Применение стандарта ISO 31010 предоставляет рекомендации по выбору и применению различных методов оценки рисков, включая анализ сценариев, анализ дерева отказов и другие подходы.

Рассмотрим несколько примеров инцидентов информационной безопасности и их последствия:

– Кибератаки с использованием программ-вымогателей (ransomware): такие атаки могут привести к блокировке доступа к критически важной информации и требованию выкупа за восстановление доступа [7, с. 242]. Это может вызвать значительные финансовые потери и нарушение бизнес-процессов;

– Утечки конфиденциальных данных: потеря или несанкционированное раскрытие информации может повлечь за собой юридические последствия, штрафы и ущерб репутации предприятия [8, с. 169];

– Простои систем и сервисов: технические сбои или атаки, приводящие к недоступности информационных систем, могут вызвать остановку производственных процессов и финансовые убытки.

Существуют различные методики оценки информационных рисков, включая [6, с. 437]:

– Качественные методы: основаны на экспертных оценках и анализе сценариев развития событий;

– Количественные методы: используют статистические данные и математические модели для определения вероятности и последствий угроз;

– Комбинированные методы: сочетают элементы качественного и количественного подходов для более точной оценки рисков.

Международные стандарты ISO/IEC 27001 и ISO 31000 предоставляют рамки для управления информационными рисками:

– ISO/IEC 27001: определяет требования к созданию, внедрению, поддержанию и постоянному улучшению системы управления информационной безопасностью [4];

– ISO 31000: предоставляет принципы и рекомендации по управлению рисками, включая процессы идентификации, оценки и обработки рисков [5].

Применение этих стандартов позволяет предприятиям систематически подходить к управлению информационными рисками и интегрировать процессы безопасности в общую систему управления.

Головко М. В., Анцибор А. В., Рогачева Ж. С. отмечают, что для минимизации информационных угроз предприятия могут использовать следующие инструменты и подходы [2, с. 66]:

– Внедрение систем обнаружения и предотвращения вторжений (IDS/IPS): позволяет выявлять и блокировать подозрительную активность в сети;

– Регулярное обновление программного обеспечения и систем безопасности: обеспечивает защиту от известных уязвимостей;

– Обучение персонала основам информационной безопасности: повышает осведомленность сотрудников о потенциальных угрозах и способах их предотвращения;

– Разработка и тестирование планов реагирования на инциденты: обеспечивает готовность предприятия к быстрому и эффективному реагированию на инциденты безопасности.

Эффективная стратегия информационной безопасности должна включать:

– Анализ текущего состояния информационной безопасности: определение уязвимых точек и потенциальных угроз;

– Постановку целей и задач в области безопасности: определение приоритетов и направлений развития;

– Разработку и внедрение политик и процедур безопасности: установление правил и стандартов поведения для сотрудников;

– Мониторинг и оценку эффективности мер безопасности: регулярный анализ и корректировка стратегии в зависимости от изменений во внешней и внутренней среде.

Как указывает Горина М.С., создание системы мониторинга и реагирования включает [3, с. 113]:

– Установку средств мониторинга сетевой активности и системных журналов: позволяет своевременно обнаруживать аномалии и потенциальные угрозы;

– Определение процедур реагирования на инциденты: включает действия по локализации, устранению и восстановлению после инцидентов;

– Назначение ответственных лиц и формирование команды реагирования: обеспечивает координацию действий при возникновении инцидентов.

Обучение сотрудников и формирование культуры безопасности включает:

– Проведение регулярных тренингов и семинаров по информационной безопасности: повышает осведомленность и компетентность персонала;

– Разработка и распространение материалов по лучшим практикам безопасности: обеспечивает доступ к актуальной информации и рекомендациям.

– Внедрение системы поощрения за соблюдение политики безопасности: стимулирует ответственное поведение сотрудников.

Таким образом, в условиях цифровой трансформации и увеличения количества информационных угроз предприятия сталкиваются с необходимостью обеспечения экономической безопасности через эффективное управление информационными рисками. Идентификация и оценка угроз, применение международных стандартов ISO/IEC 27001 и ISO 31000, а также внедрение практических мер по минимизации рисков являются ключевыми элементами стратегии безопасности. Формирование культуры безопасности и обучение персонала способствуют укреплению защиты информационных ресурсов и обеспечению устойчивости предприятия в долгосрочной перспективе.

Список литературы:

1. Бондарева С. А., Печерская К. А. Риски цифровизации в системе обеспечения экономической безопасности предприятия //Проблемы развития национальной экономики в условиях глобальных инновационных преобразований. – 2021. – С. 178-181.

2. Головко М. В., Анцибор А. В., Рогачева Ж. С. К вопросу о влиянии цифровых технологий на экономическую безопасность предприятий //Безопасность ядерной энергетики: тезисы докладов XVII Международной научно-практической конференции, 26–28 мая 2021 г./НИЯУ МИФИ [и др.].–Волгодонск: ВИТИ НИЯУ МИФИ, 2021.–132 с. – 2021. – С. 66.

3. Горина М. С. Оценка рисков и угроз экономической безопасности предприятия //Естественно-гуманитарные исследования. – 2024. – №. 3 (53). – С. 113-119.

4. ГОСТ Р ИСО/МЭК 27001-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. Утверждён и введён в действие приказом Росстандарта от 27 декабря 2021 г. № 375-ст.

5. ГОСТ Р ИСО 31000-2019. Менеджмент риска. Принципы и руководство. – Идентичен ISO 31000:2018. Утверждён приказом Росстандарта от 10 декабря 2019 г. № 1379-ст.

6. Ибыжанова А. Д. Информационные риски в формировании политики экономической безопасности организации. НАО «Западно-Казахстанский аграрно-технический университет имени Жангир хана», г. Уральск. – 2024. – С. 437-445.

7. Одаховская Д. А., Пятков С. В., Черных М. А. Информационные риски: анализ и расчеты //Прикладные экономические исследования. – 2024. – №. 2. – С. 242-247.

8. Тимохина В. С. Анализ и оценка рисков информационной безопасности на предприятии //Проблемы и перспективы развития российской. – С. 169.