УДК 338

ОСНОВНЫЕ АСПЕКТЫ УПРАВЛЕНИЯ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Малиновская О.А.

к.э.н., доцент

Вятский государственный университет,

Россия, г. Киров

Сиреджук С.С.

студент,

Вятский государственный университет,

Россия, г. Киров

Аннотация. В данной статье рассмотрены основные аспекты управления рисками информационной безопасности предприятия. Информационная безопасность предприятия выступает одним из ключевых элементов его устойчивого функционирования в условиях современного цифрового мира. Риск, связанный с информационной безопасностью, может иметь серьезные последствия, включая финансовые потери, утечку конфиденциальных данных и репутационные потери. В ходе статьи мы рассмотрели теоретическую составляющую, связанную с рисками информационной безопасности, также выделили методологии и меры управления этими рисками.

Ключевые слова: информационная безопасность, риски, предприятие, методология управления, меры управления.

THE MAIN ASPECTS OF ENTERPRISE INFORMATION SECURITY RISK MANAGEMENT

Malinovskaya O.A.
Candidate of Economics, Associate Professor
Vyatka State University,
Kirov, Russia

Siredzhuk S.S.
student,
Vyatka State University,
Kirov, Russia

Annotation. This article discusses the main aspects of enterprise information security risk management. The information security of an enterprise is one of the key elements of its sustainable functioning in the modern digital world. The risk associated with information security can have serious consequences, including financial losses, leakage of confidential data and reputational losses. In the course of the article, we examined the theoretical component associated with information security risks, and also identified methodologies and measures for managing these risks.
Keywords: information security, risks, enterprise, management methodology, management measures.

Информационная безопасность предприятия выступает одним из ключевых элементов его устойчивого функционирования в условиях современного цифрового мира. Риск, связанный с информационной безопасностью, может иметь серьезные последствия, включая финансовые потери, утечку конфиденциальных данных и репутационные потери. Таким образом, управление рисками представляет собой важный процесс, направленный на выявление, оценку и минимизацию влияния угроз на информационные активы предприятия [2].

Управление рисками информационной безопасности начинается с определения понятий, связанных с рисками. Риск в контексте информационной безопасности — это вероятность возникновения событий, способных негативно повлиять на конфиденциальность, целостность и доступность информации и информационных систем.

В рамках управления рисками выделяются следующие ключевые аспекты:

1. Выявление рисков. На этом этапе необходимо идентифицировать возможные угрозы и уязвимости информационных систем. Угрозами могут быть как внешние, так и внутренние факторы: кибератаки, ошибки пользователей, несанкционированный доступ и так далее.

2. Измерение и оценка рисков. После выявления рисков необходимо оценить их влияние и вероятность возникновения. Это позволит понять, какие риски являются наиболее критичными для функционирования предприятия. Важно учитывать не только финансовые последствия, но и возможные репутационные потери и нарушения законодательства.

3. Управление рисками. На данном этапе разрабатываются стратегии по минимизации или устранению идентифицированных рисков. Возможно применение различных методов, таких как избежание риска (отказ от конкретной деятельности), снижение риска (внедрение защитных мер) или принятие риска (умышленное его оставление на определенном уровне) [5].

Существует несколько подходов и методологий для эффективного управления рисками информационной безопасности. Одной из наиболее распространенных является методология NIST (National Institute of Standards and Technology), которая включает следующие шаги:

1. Подготовка. Определение организованной структуры, политик и процедур по управлению рисками.

2. Идентификация. Выявление активов, уязвимостей и угроз, а также оценка их значимости.

3. Оценка. Определение уровня риска для каждого из выявленных уязвимых мест в системе, а также разработка стратегий по их минимизации.

4. Обработка. Реализация мер для устранения или снижения рисков через различные механизмы защиты.

5. Мониторинг. Постоянное отслеживание изменений в уровне рисков, а также оценка эффективности принятых мер [4].

Параллельно с методологией NIST, необходимо учитывать стандарты ISO/IEC 27001. Стандарты информационной безопасности, которые обязаны соблюдать предприятия в России, такие как ISO17799, BS7799, ISO27001, предусматривают механизмы управления ИТ-рисками.

ISO/IEC 27001 — международный стандарт по информационной безопасности, разработанный совместно Международной организацией по стандартизации и Международной электротехнической комиссией. Стандарт содержит требования в области информационной безопасности для создания, развития и поддержания Системы менеджмента информационной безопасности (СМИБ).

ISO 27001 устанавливает требования к системе менеджмента информационной безопасности для демонстрации способности организации защищать свои информационные ресурсы. В стандарте ISO/IEC 27001 (ISO 27001) собраны описания лучших мировых практик в области управления информационной безопасностью. ISO 27001 устанавливает требования к системе менеджмента информационной безопасности для демонстрации способности организации защищать свои информационные ресурсы. Настоящий стандарт подготовлен в качестве модели для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения Системы Менеджмента Информационной Безопасности (СМИБ) [1].

Для эффективного управления рисками информационной безопасности важно сочетание как технологических, так и организационных мер.

Использование современных технологий безопасности является важной составляющей в управлении рисками. Это включает:

- Антивирусные решения. Необходимо оснащение рабочих станций и серверов антивирусным программным обеспечением.

- Системы обнаружения и предотвращения вторжений (IDS/IPS). Они помогают предотвращать несанкционированные попытки доступа к системе.

- Шифрование данных. Защита конфиденциальных данных с помощью средств шифрования.

- Резервное копирование данных. Регулярное создание резервных копий обеспечивает защиту данных от потери [3].

Организационные меры включают:

- обучение сотрудников. Проведение регулярных тренингов по вопросам информационной безопасности и практикам безопасного поведения в цифровой среде [2];

- создание политики безопасности. Формирование четкой политики безопасности с определением ролей и обязанностей всех сотрудников;

- периодический аудит. Проведение регулярных проверок систем безопасности и анализ их эффективности.

Далее приведу в пример реализацию системы ИБ на примере АЭС. Управление станциями осуществляет концерн «Росэнергоатом».

Цифровая трансформация «Росэнергоатома» началась в 2017 году, когда были поставлены две цели:

1. Создание цифрового шаблона опыта эксплуатаций АЭС. Единый инструмент управления системами АЭС должен позволить решать задачи управления процессами и рисками не только на российских, но и на зарубежных проектах концерна, если их собственники будут готовы приобрести информационный продукт. Решение должно быть полностью готово и интегрировано с установленной на всех 16 энергетических объектах SAP ERP к концу 2021 года.

2. Переход на модель управления в рамках интеллектуальной энергетической системы России (ИЭСР). С ее помощью будет происходить управление рисками кибербезопасности на всех энергетических объектах России – от АЭС до гидроэлектростанций. Решение будет реализовано на базе создаваемой в рамках проекта «Цифровая экономика» платформы IoT Energy.

Работа по построению единой системы кибербезопасности предприятий АЭС ведется в рамках решений по проекту «Цифровая экономика» и на основе системополагающих решений МАГАТЭ и Росэнергоатома. Основным требованием до последнего времени являлось полное исключение подключения АСУ ТП АЭС к Интернету, но реализация проекта ИЭСР внесет коррективы в эту политику.

В 2015 году было зафиксировано более десяти существенных инцидентов кибербезопасности, в основном в США, связанных с проникновением в сеть АЭС извне. Они не привели к авариям, только к массовым отключениям электроэнергии, что стало причиной существенного ущерба. С учетом подобных фактов требуется максимально обезопасить каналы связи АСУ ТП АЭС от внешних подключений.

С точки зрения изучения примеров построения системы информационной безопасности предприятия интересно, как в разных странах разрабатывается модель информационных угроз для АЭС:

1) в США используется программа, предназначенная для расчета рисков и их вероятности, установленная на самом объекте;

2) Нидерланды привлекают внешних консультантов, имеющих большой опыт аналитики и прогнозирования в сфере информационной безопасности;

3) некоторые страны Африки (Зимбабве) применяют метод Дельфи для определения угроз атомной инфраструктуре.

Еще одной особенностью управления рисками кибербезопасности на предприятиях АЭС является то, что современные программные средства защиты

считаются недостаточно безопасными для внедрения в программную среду АСУ ТП АЭС, поэтому решением становится ее изоляция от внешнего вмешательства, построение максимально возможной прочной системы внешней защиты. Но это не снимает риски инсайдерских инцидентов. Так, распространенным способом атак стали фишинговые письма, направляемые на электронные почтовые ящики сотрудников АЭС. Эту проблему в сфере информационной безопасности предполагается решать системным обучением персонала.

Таким образом, управление рисками информационной безопасности — это непрерывный процесс, требующий комплексного подхода и постоянного обновления в ответ на изменяющиеся угрозы и технологии. Понимание основных аспектов управления рисками позволяет предприятиям не только защитить свои информационные активы, но также обеспечить свою конкурентоспособность и доверие со стороны клиентов. В условиях динамичного цифрового ландшафта создание эффективной системы управления рисками является необходимостью для обеспечения долгосрочной устойчивости бизнеса.

Библиографический список

1. ГОСТ "ГОСТ Р ИСО/МЭК 27001-2021" от 2022-01-01 // Электронный фонд правовых и нормативных документов

2. Риски информационной безопасности // rt-solar.ru URL: https://rt-solar.ru/products/solar_dozor/blog/3320/ (дата обращения: 21.09.2024)..

3. Пашков Н.Н., Дрозд В.Г. Анализ рисков информационной безопасности и оценка эффективности систем защиты информации на предприятии //Современные научные исследования и инновации. 2020. № 1 [Электронный ресурс]. URL: https://web.snauka.ru/issues/2020/01/90380 (дата обращения: 20.09.2024).

4. Павлов, О. Н. "Основы информационной безопасности: Технологии и методики." – М.: Инфра-М, 2022. с. 7-10

5. Руслан Рахметов, Управление рисками информационной безопасности. Часть 7. Стандарт ISO/IEC 27005:2018 (продолжение). Стандарт IEC 31010:2019 // Security Vision. – 2020

Оригинальность 79%