последующее расширение и уточнение Карты за счет информации ДСП. В дальнейшем Карта нуждается в регулярной актуализации – корректировке, изменении и дополнении в соответствии с меняющейся внешней и внутренней конъюнктурой. Система контрмер, разрабатываемая службами, отвечающими за безопасность, должна соответствовать балльной шкале, предложенной во всех четырех разделах Карты.

Исследование проведено авт. коллективом Ассоциации «Стратегия-50»: А. Боков, А. Кривов, А. Шамузафаров, Д. Фесенко, А. Иванов, А. Минеджян, А. Загоруйко

Правиков Д.И., Мурашкин В.А.

Подходы к количественной оценке информационной безопасности на предприятии ТЭК

Аннотация: В данной работе рассматриваются подходы к количественной оценке информационной безопасности на предприятии ТЭК. Проанализированы методы, направленные на оценку текущего состояния безопасности, затрат на защитные меры и эффективности внедрённых решений. Основное внимание уделено таким подходам, как анализ затрат, использование ключевых показателей эффективности, анализ инцидентов и соответствие нормативным требованиям. Предложены методы оценки информационной безопасности на основе времени простоя системы или видимости инцидента. Такой подход позволяет обеспечить объективную и экономически обоснованную оценку уровня защиты критически важной инфраструктуры предприятий ТЭК, а также принимать эффективные решения по улучшению информационной безопасности.

Ключевые слова: информационная безопасность, количественная оценка, ключевые показатели

эффективности, анализ инцидентов, топливно-энергетический комплекс (ТЭК)

При оценке информационной безопасности на предприятиях ТЭК в России применяются подходы, ориентированные на количественную оценку текущего состояния безопасности, затрат и эффективности внедрённых мер защиты. Эти подходы базируются на анализе затрат, показателях эффективности, анализе инцидентов и соблюдении нормативных требований. Ниже представлены основные методы, используемые для такой оценки.

1. Оценка стоимости инцидентов и затрат на меры безопасности

Этот подход направлен на оценку всех затрат, связанных с информационной безопасностью, как в плане предотвращения, так и в случае возникновения инцидентов. Основные аспекты включают:

– оценка текущих затрат на информационную безопасность: определение общей суммы, которую компания тратит на защиту информационных систем, включая технические средства защиты, программное обеспечение, затраты на персонал и обучение;

– оценка прямых и косвенных затрат: анализ всех затрат, связанных с потенциальными инцидентами, включая простои системы, восстановление данных и репутационные издержки;

– экономическая оценка эффективности внедрённых мер: расчёт возврата инвестиций (ROI) для внедрённых технологий и процессов, направленных на улучшение информационной безопасности.

Этот метод позволяет определить экономическую целесообразность вложений в информационную безопасность без привязки к вероятности реализации конкретных угроз [1].

2. Методология KPI и KRI для количественной оценки эффективности

Использование ключевых показателей эффективности (KPI) и ключевых показателей риска (KRI) позволяет проводить измерение и мониторинг состояния информационной безопасности. Данный

подход ориентирован на текущие результаты и тенденции в обеспечении защиты:

KPI (Key Performance Indicators) – оценивают достигнутые результаты и эффективность внедрённых мер. Примеры KPI могут включать:

- время реакции на инциденты;
- время восстановления работы после инцидентов;
- количество устраненных уязвимостей в системе.

KRI (Key Risk Indicators): используют для мониторинга состояния безопасности и выявления потенциальных проблем. Хотя здесь не учитывается оценка рисков, KRI можно использовать для контроля показателей, указывающих на текущий уровень угроз:

- количество выявленных инцидентов в единицу времени;
- доля успешно отражённых атак.

Эти метрики позволяют количественно оценить текущее состояние информационной безопасности и дают возможность измерять, насколько эффективно функционируют системы защиты [2].

3. Анализ инцидентов информационной безопасности

Анализ исторических данных о произошедших инцидентах на предприятии ТЭК позволяет определить тенденции и оценить ущерб от нарушений безопасности без привязки к вероятностям [3]. Основные шаги включают:

- подсчёт количества инцидентов за определённый период;
- оценка ущерба от каждого инцидента;
- идентификация повторяющихся проблем.

4. Методология вычисления уровня соответствия нормативным требованиям

Для российских предприятий ТЭК критически важно соответствие национальным стандартам и нормативным требованиям, таким как Приказ ФСТЭК №239, ГОСТ Р 57580, а также другим регулятивным документам. Оценка уровня соответствия проводится в рамках количественной оценки информационной безопасности:

- аудит на соответствие стандартам;
- количественная оценка уровня соответствия: измерение

степени выполнения всех обязательных требований, например, в процентах (сколько из проверенных параметров соблюдаются);

– расчет затрат на обеспечение соответствия: анализ финансовых вложений, необходимых для приведения инфраструктуры в соответствие с законодательством и стандартами.

Этот подход направлен на количественную оценку состояния информационной безопасности через призму выполнения регуляторных требований и стандартов [4].

5. Оценка затрат и ресурсов на поддержание систем защиты

Этот подход фокусируется на расчете затрат, необходимых для постоянного поддержания уровня информационной безопасности на предприятии:

– расходы на эксплуатацию и техническое обслуживание систем безопасности: определение затрат на текущие и плановые работы по поддержке работоспособности систем;

– затраты на обновление и модернизацию оборудования и ПО: оценка инвестиций, необходимых для поддержания актуального уровня защиты и обновления систем;

– анализ использования человеческих ресурсов: количественная оценка затрат на обучение и повышение квалификации сотрудников, задействованных в поддержке информационной безопасности [5].

Данный подход помогает компании понимать, какие затраты необходимы для поддержания текущего уровня защиты без учета вероятности появления новых угроз.

6. Методология анализа стоимости владения системами безопасности

Подход ТСО позволяет количественно оценить совокупную стоимость владения решениями по информационной безопасности на предприятии. Он учитывает не только начальные инвестиции, но и все эксплуатационные и сопутствующие расходы:

– первоначальные затраты: стоимость приобретения оборудования и программного обеспечения;

– операционные расходы: затраты на поддержку, обслуживание, обновление и модернизацию;

– косвенные расходы: такие как обучение персонала и возможные затраты на устранение инцидентов [6].

Использование TCO позволяет увидеть полную финансовую картину внедрения и эксплуатации систем информационной безопасности.

7. Заключение

Для предприятий ТЭК количественная оценка информационной безопасности включает использование подходов, направленных на анализ эффективности и стоимости защитных мер, мониторинг инцидентов и соответствие нормативным требованиям. Эти методы позволяют получить объективные данные о текущем состоянии информационной безопасности и оценить финансовую целесообразность вложений в защиту критической инфраструктуры.

Мы предлагаем оценивать информационную безопасность по времени простоя системы в результате инцидентов, так как это позволяет напрямую измерить влияние на производственные процессы и финансовые потери [7]. Если оценка по времени простоя невозможна, можно использовать критерий видимости инцидента, определяя его влияние на основные операции и репутацию предприятия. Такой подход обеспечивает гибкость в условиях, когда данные о точных временных затратах недоступны, и позволяет оценить значимость инцидента по его последствиям и влиянию на бизнес.

Литература:

1. *Салютина Т.Ю., Аблогин М.А, Платунина Г.П.* Особенности и механизм измерения и обработки рисков при оценке эффективности системы информационной безопасности бизнеса компании // Экономика и качество систем связи. – 2018. – №3. – URL: https://cyberleninka.ru/article/n/osobennosti-i-mehanizm-izmereniya-i-obrabotki-riskov-pri-otsenke-effektivnosti-sistemy-informatsionnoy-bezopasnosti-biznesa-kompanii (дата обращения 10.10.2024).

2. ISO/IEC 27004:2016 Information technology – Security techniques – Information security management – Measurement (IDT). –

URL: https://www.iso.org/standard/64120.html (дата обращения 10.10.2024).

3. *Голованов В.Б.* Модель зрелости как подход измерения эффективности процессов информационной безопасности // НиКа. – 2006. – URL: https://cyberleninka.ru/article/n/model-zrelosti-kak-podhod-izmereniya-effektivnosti-protsessov-informatsionnoy-bezopasnosti (дата обращения 10.10.2024).

4. CIS Critical Security Controls V7 Measures & Metrics. – URL: https://www.cisecurity.org/insights/white-papers/cis-controls-v7-measures-metrics (дата обращения 10.10.2024).

5. *Слепов А.В., Зефиров С.Л.* Способ риск-ориентированной оценки информационной безопасности организации // Инжиниринг и технологии. – 2018. – Т. 3(2). – С. 32-35.

6. *Егоров И.А., Кондратьев В.Ю.* Методика анализа совокупной стоимости владения (TCO) // Инновации и инвестиции. – 2022. – №11. – URL: https://cyberleninka.ru/article/n/metodika-analiza-sovokupnoy-stoimosti-vladeniya-tco (дата обращения 10.10.2024).

7. *Правиков Д.И., Мурашкин В.А.* Оптимизация процессов управления информационной безопасностью на предприятии ТЭК / Сборник научных трудов Всероссийской научно-технической конференции «Кибернетика и информационная безопасность» «КИБ-2023», Москва, 18-19 октября 2023 года. – Москва: Национальный исследовательский ядерный университет «МИФИ», 2023. – С. 102-103.

Сиротюк В.О.

Решение задач повышения безопасности цифровых систем управления интеллектуальной собственностью

Аннотация: Рассмотрены проблемы обеспечения безопасности и качества патентно-информационных фондов, информационно-технологической инфраструктуры цифровых систем управления интеллектуальной собственностью (ИС), возникающие при решении задач цифровой трансформации традиционных систем