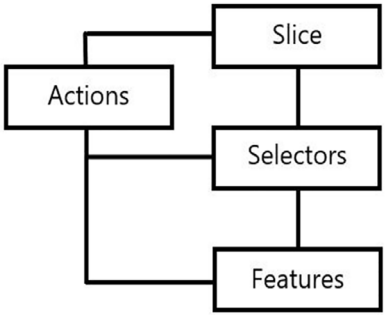


Рис. 7. Схема взаимодействия Redux с Features

На рисунке 7 представлена модель взаимодействия Redux с компонентами, где хранится основная логика приложения – такие компоненты называются Features (основные компоненты, в которых сохраняется логика обработки запросов).

Заключение

Разработанная архитектура демонстрирует эффективное взаимодействие между компонентами системы умного дома. Использование современных технологий обеспечивает:

– Надежную защиту данных через HTTPS

– Оперативную передачу информации посредством WebSocket

– Гибкое хранение данных в MongoDB

– Удобный интерфейс управления на базе React

Система готова к масштабированию и может быть адаптирована под различные задачи автоматизации жилья.

Список литературы

1. Белов А. В. Практическая энциклопедия Arduino. М.: Наука и техника. ДМК Пресс, 2018. 272 с.

2. Блум Д. Изучаем Arduino Инструменты и методы технического волшебства: учебное пособие. М: БХВ-Петербург, 2016. 336 с.

3. Геддес М. 25 крутых проектов с Arduino. М.: Эксмо, 2016.

4. Иго Т. Arduino, датчики и сети для связи устройств. М.: БХВ-Петербург, 2017. 544 с.

5. Володин В. Д., Шаронов А. А., Полевщиков И. С. Средства разработки и отладки программного обеспечения отечественных микропроцессорных устройств (часть 2) // Science Time. 2016. № 1(25). С. 91-94. EDN: VLIUFJ.

АНАЛИЗ СТАНДАРТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И РАЗРАБОТКА ОПЕРАЦИОННОЙ МОДЕЛИ ДЛЯ ПРЕДПРИЯТИЙ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Мельников А. В., Мозговенко А. А.

ФГБОУ ВО «Мелитопольский государственный университет», Мелитополь, e-mail: ya@amozgovenko.ru

Задачи исследования:

1. Провести сравнительный анализ международных и национальных стандартов ИБ, применимых к КИ.

2. Выявить типовые угрозы и сценарии атак на объекты КИ (с учётом специфики энергетики, транспорта, ТЭК, связи и др.).

3. Определить ключевые требования регуляторов (ФСТЭК, ФСБ, Минцифры) к защите КИ.

Материалы и методы исследования

Современные исследования в области ИБ критической инфраструктуры фокусируются на следующих аспектах:

1. Регуляторная среда. Активно анализируются требования ФЗ-187, приказов ФСТЭК № 239 и № 31, а также международные стандарты (ISO/IEC 27001, NIST CSF, IEC 62443 для промышленных систем). Отмечается тенденция к гармонизации российских и зарубежных норм.

2. Киберугрозы для КИ. Публикации 2023–2025 гг. выделяют рост целевых атак (APT) на SCADA/ICS, использование вредоносного ПО типа TRITON/TRISIS, а также угрозы со стороны инсайдеров. Особое внимание уделяется уязвимостям устаревших промышленных протоколов (Modbus, DNP3).

3. Технологии защиты. Исследуются решения для:

− поведенческого анализа трафика (NTA);

− защиты конечных точек в промышленных сетях (EDR для ICS);

− автоматизации реагирования (SOAR);

− киберполигонов для тестирования устойчивости КИ.

4. Управление рисками. Развиваются методики количественной оценки рисков для КИ с учётом каскадных эффектов (например, отключение энергоснабжения ведёт к остановке транспорта).

Цель исследования – проанализировать операционную модель информационной безопасности для предприятий критической инфраструктуры, обеспечивающую соответствие регуляторным требованиям и устойчивую защиту от актуальных киберугроз.

Результаты исследования и их обсуждение

Для внедрения комплексной системы защиты информации и системы управления информационной безопасностью разработан ряд государственных и международных стандартов.

Обычно используют следующие стандарты для анализа, внедрения и постоянного мониторинга за СУИБ:

1. ГОСТ Р ИСО/МЭК 27001-2021 – российский аналог международного стандарта ISO/IEC 27001:2013. Устанавливает требования к созданию, внедрению, поддержанию и постоянному улучшению системы менеджмента информационной безопасности (СМИБ). Включает оценку и обработку рисков, выбор мер защиты, мониторинг эффективности и непрерывное совершенствование системы.

2. ГОСТ Р 50922-2006 – определяет основные термины и определения в области защиты информации. Важен для унификации понятий при разработке документации СУИБ.

3. ГОСТ Р ИСО/МЭК 15408 (три части: 1-2012, 2-2013, 3-2013) – «Общие критерии оценки безопасности информационных технологий». Определяет инструменты и методику оценки безопасности информационных продуктов и систем, включая критерии для сравнения результатов независимых оценок.

4. Стандарт Банка России СТО БР ИББС-1.0-2014 – применяется в банковской сфере. Регламентирует обеспечение информационной безопасности организаций банковской системы РФ, включая требования к защите данных и управлению рисками.

5. ГОСТ Р ИСО/МЭК 27013-2014 – руководство по совместному использованию стандартов ИСО/МЭК 27001 и ИСО/МЭК 20000-1 (менеджмент услуг). Помогает интегрировать требования к информационной безопасности и управлению услугами.

6. ГОСТ Р 51188–98 – регламентирует испытания программных средств на наличие компьютерных вирусов. Хотя стандарт устаревший, он может использоваться в части процедур тестирования ПО.

7. ГОСТ Р 51275-2006 – определяет факторы, воздействующие на информацию в объектах информатизации. Помогает в анализе угроз и уязвимостей.

В результате проведенного анализа государственных и международных стандартов по информационной безопасности, предлагаем использовать разработанную на основе вышеупомянутых стандартов операционную модель, которая состоит из ключевых аспектов, эффективная работа которых помогает обеспечить необходимый уровень ИБ в сочетании с бизнес-процессами.

Операционная модель включает следующие ключевые аспекты: политики, процессы ИБ, корпоративное управление, техническую архитектуру ИБ, организационную структуру, людей, ключевые показатели эффективности (КПЭ) и отчетность.

Процесс анализа операционной модели начинается с нормативной базы документов и процессов ИБ, а также оценки их уровня зрелости. Выполнение этого этапа необходимо для понимания отправной точки внедрения системы управления информационной безопасности на предприятии.

Анализ существующей нормативной базы состоит из следующих шагов:

1. Собрать список документов, разработанных на предприятии и их номенклатуру

2. Проанализировать текущие политики и процедуры, связанные с информационной безопасностью

3. Проанализировать нормативные документы, основные нормы и правила соответствия требованиям регулятора и лучшим практикам (требования к предприятиям критической инфраструктуры, рекомендации ведущих практик ISO, NIST)

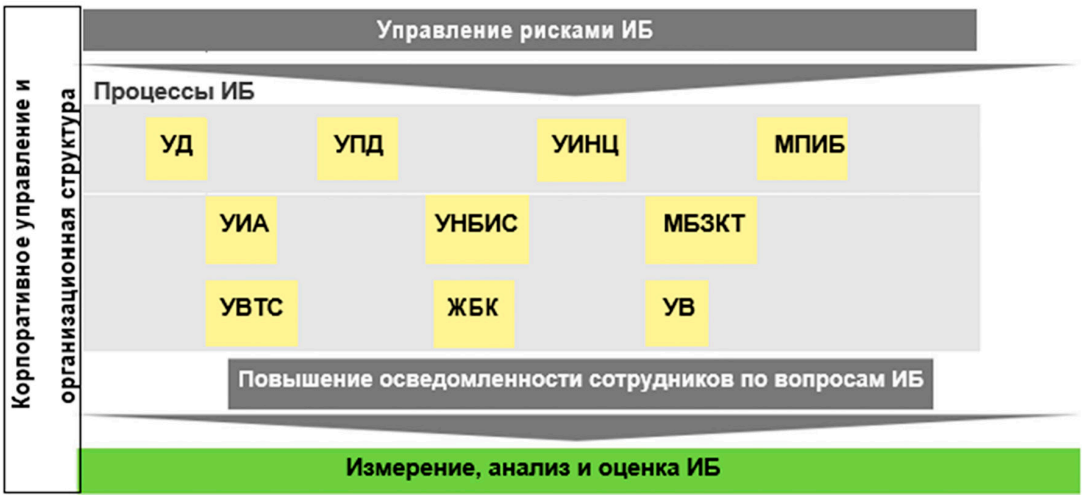
4. Определить недостающие документы и разработать перечень рекомендаций по дополнению существующей нормативной базы

Следующим этапом является оценка уровня зрелости установившихся процессов ИБ на предприятии. Для этого необходимо выполнить определенный перечень действий, а именно:

1. Проанализировать ключевые процессы ИБ

2. Оценить текущий уровень зрелости процессов ИБ и провести сравнительный анализ эффективности процессов с мировой и украинской практикой (бенчмаркинг)

3. Определить направления усовершенствования и развития процессов информационной безопасности



Модель процессов ИБ на предприятии

Оценка процессов ИБ в соответствии с их состоянием

0	Начальный: процесс отсутствует или его элементы выполняются частично
1	Выполняемый: основные элементы выполняются бессистемно. Процесс формально не задокументирован или документирован поверхностно, актуализация документации не выполняется. Эффективность функционирования зависит от индивидуальных знаний и усилий исполнителей
2	Установленный процесс: основные элементы процесса задокументированы и в основном выполняются одинаково для всей организации. Выполняется актуализация документации. Роли и обязанности определены и используются на практике. Процесс автоматизирован с помощью технических решений
3	Управляемый процесс: установленный процесс достигает поставленных результатов и генерирует показатели, на основе которых производится оценка его эффективности и усовершенствования
4	Оптимизированный процесс: высшее руководство принимает участие в анализе недостатков и повышении эффективности процесса. Совершенствование процесса и поддерживаемых технологий проводится регулярно и измеряется

Для оценки зрелости процессов ИБ по разным сферам предприятия, предлагаем использовать методологию для оценки зрелости процессов, разработанную на основе ведущих мировых практик и стандартов информационной безопасности. Для этого была создана референсная модель процессов ИБ по разным сферам предприятия (рисунок).

Были выделены следующие процессы:

− УД – Управление доступом к информационным ресурсам

− УИА – Управление информационными активами

− УПД – управление персональными данными

− УНБИС – Управление настройками безопасности ИС и оборудования

− УИНЦ- Управление инцидентами ИБ

− МБЗКТ – Сетевая безопасность и защита конечных точек

− МПИБ-мониторинг событий ИБ

− УВТС – Управление взаимодействием с третьими сторонами

− ЖБК – Обеспечение безопасности кода

− УВ – управление уязвимостями

Каждый процесс приведенной модели оценивается по пятибалльной шкале в соответствии с состоянием процесса на предприятии, толкование оценки процессов приведено в таблице.

Заключение

В этой статье рассмотрены государственные стандарты информационной безопасности, регламентирующие создание КСЗИ и международные стандарты информационной безопасности, что регламентируют построение СУИБ и определяют подход к построению системы управления кибербезопасностью. Были сравнительно государственные и международные стандарты на их соответствие современным тенденциям кибербезопасности.

Была разработана операционная модель, позволяющая систематизированно проанализировать текущее состояние организации в соответствии с требованиями вышеупомянутых стандартов. Каждый раздел, входящий в операционную модель, был описан и приведен этапы проведения анализа для каждого из разделов. Представлен пример результатов анализа текущего состояния операционной модели предприятия, используя вышеупомянутые этапы и рекомендации.

Список литературы

1. Максимова Е. А. Аксиоматика инфраструктурного деструктивизма субъекта критической информационной инфраструктуры // Информатизация и связь. 2022. № 1. С. 68–74. DOI: 10.34219/2078-8320-2022-13-1-68-74. EDN: ZMOPQB.

2. Роберте Ф. С. Дискретные математические модели с приложениями к социальным, биологическим и экологическим задачам / пер. с англ. М.: Наука, 1986. 496 с.

КИБЕРБЕЗОПАСНОСТЬ. АНАЛИЗ ВИДОВ ЗАЩИТЫ В ИНФОРМАЦИОННОЙ СРЕДЕ

Пелипенко А. П.

ФГБОУ ВО «Мелитопольский государственный университет», Мелитополь, e-mail: elena27712@mail.ru

Научный руководитель: Ступницкий В. С.

Введение

В нынешней цифровой среде обеспечение кибербезопасности приобретает первостепенное значение для устойчивого функционирования любой сферы жизни. Что же такое эта кибербезопасность? Это совокупность технических решений, направленных на защиту сетевых инфраструктур, хранимую информацию, устройств, обеспечение конфиденциальности и целостности. С каждым днём рост кибератак привлекает за собой новые виды угроз, а развитие систем защиты становится критически важным. Только в 2025 году было зарегистрировано более 36 фактов взлома с ущербом от 1 до 223 миллионов (USD). Цели кибератак могут быть разными: от кражи конфиденциальных данных, до нарушения работы систем.