Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет
имени первого Президента России Б.Н. Ельцина»

Институт радиоэлектроники и информационных технологий – РТФ
Школа профессионального и академического образования

ДОПУСТИТЬ К ЗАЩИТЕ ПЕРЕД ГЭК

Обабков И.Н.
(подпись) (Ф.И.О.)
« 29 » мая 2023 г.

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

ПРОЕКТИРОВАНИЕ СИСТЕМЫ ДЛЯ АВТОМАТИЗАЦИИ ПРОЦЕССА ПРОВЕДЕНИЯ АУДИТА ДЛЯ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Научный руководитель: Ронкин Михаил Владимирович
кандидат технических наук
Нормоконтролер: Огуренко Егор Владимирович
Студент группы РИМ-210990 Василенко Алина Олеговна

Екатеринбург –2023

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

Институт радиоэлектроники и информационных технологий – РтФ
Школа профессионального и академического образования
Направление подготовки 09.04.04 Программная инженерия
Образовательная программа Программная инженерия

УТВЕРЖДАЮ
РОП _____
«29» мая 202 г.

ЗАДАНИЕ

на выполнение выпускной квалификационной работы

студента *Василенко Алины Олеговны* **группы** *РИМ-210990*
(фамилия, имя, отчество)

1. Тема выпускной квалификационной работы *Проектирование системы для автоматизации процесса проведения аудита для объектов критической информационной инфраструктуры*

Утверждена распоряжением по институту от «____» _____ 202 г. № ___

2. Руководитель Ронкин Михаил Владимирович, к.т.н.
(Ф.И.О., должность, ученое звание, ученая степень)

3. Исходные данные к работе материалы, полученные в ходе преддипломной практики, ГОСТы, техническая литература

4. Перечень демонстрационных материалов презентация в MS PowerPoint

5. Календарный план

№ п/п	Наименование этапов выполнения работы	Срок выполнения этапов работы	Отметка о выполнении
1.	*Изучение предметной области*	до _ 2023 г.	
2.	*Анализ инструментов для проведения аудита*	до 2023 г.	
3.	*Проектирование системы*	до 2023 г.	
4.	*ВКР в целом*	до _____ 2023 г.	

Руководитель _____ *Ронкин М.В.*
(подпись) Ф.И.О.

Задание принял к исполнению 15.02.2023 _____
дата (подпись)

6. Выпускная квалификационная работа закончена «5 мая 2023г. считаю возможным допустить Василенко Алину Олеговну к защите выпускной квалификационной работы закончена в Государственной экзаменационной комиссии.

Руководитель _____ Ронкин М.В. _____
(подпись) Ф.И.О.

7. Допустить Василенко Алину Олеговну к защите магистерской диссертации в Государственной экзаменационной комиссии.

РОП _____ Обабков И.Н. _____
(подпись) Ф.И.О.

РЕФЕРАТ

Магистерская диссертация состоит из введения, трех глав и заключения, изложенных на 69 страницах, а также библиографического списка. В работе имеется 5 рисунков. Библиографический список состоит из 53 наименований.

АУДИТ ИНФООРМАЦИОННОЙ БЕЗОПАСНОСТИ, ВЫЯВЛЕНИЕ КРИТЕРИЕВ ОЦЕНКИ СОБЛЮДЕНИЯ МЕР, АВТОМАТИЗАЦИЯ ПРОВЕРКИ МЕР, ПРОЕКТ ПО ПРОЕКТИРОВАНИИ СИСТЕМЫ.

Целью работы является: проектирование системы для атомизации проведения аудита технических мер безопасности по результатам работы ПО DATAPK.

Объектом исследования является ПО для проведения аудита технических мер защиты информации.

Методы исследования: анализ, сравнение, систематизация и обобщение данных о существующих и разработанных способах проведения аудита информационной безопасности, анализ технических мер информационной безопасности.

Результаты работы является техническое задание на разработку автоматизированной системы для проведения аудита, сопроводительная документация и шаблон технического отчета.

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И УСЛОВНЫХ ОБОЗНАЧЕНИЙ

В настоящей работе будут применяться следующие обозначения и определения:

ВКР – выпускная квалификационная работа.

КИИ – критическая информационная инфраструктура.

ПО – программное обеспечение.

ИБ – информационная безопасность.

ОЗ – объект защиты.

АСУ ТП – автоматизированная система управления технологическим процессом.

ОС – операционная система.

САЗ – средства антивирусной защиты.

ИС – информационная система.

ВВЕДЕНИЕ

На сегодняшний день ни одна современная организация не обходится без использования компьютерных технологий. Каждый день тысячи сотрудников компаний используют персональный компьютер, десктопы, ноутбуки, ультрабуки на которых хранится и обрабатывается огромное количество различных данных. И нередко стоимость этих данных в несколько раз превышает цену всей технической системы, которая хранит эту информацию.

Существуют субъекты Критической информационной инфраструктуры – это компании, работающие в стратегически важных для государства областях, таких как здравоохранение, наука, транспорт, связь, энергетика, банковская сфера, и т. д.

Государство требует обеспечивать информационную безопасность данных субъектов согласно Федеральному закону от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

Существует методический документ, утвержденный ФСТЭК России от 11.02.2014, в котором прописаны меры для защиты информации в государственных информационных системах. Методический документ детализирует организационные и технические меры защиты информации, применяемые в государственных информационных системах в соответствии с Требованиями о защите информации, а также определяет содержание мер защиты информации и правила их реализации. Приказ предусматривает возможность применения мер защиты, сгруппированных в 15 групп.

Для проверки соблюдения требованиям безопасности на предприятии проводится аудит.

Существуют различные инструменты для проведения аудита, и заказчик использует программно-аппаратный комплекс DATAPK. Продукт

обеспечивает оперативный мониторинг и контроль состояния защищенности систем.

Периодически субъектам КИИ необходимо проводить аудит информационной безопасности. Для этого необходимо каждый объект защиты проверить на соответствие 15 групп мер. Для этого высококвалифицированный человек – аудитор запускает сбор данных с помощью ПО DATAPK и вручную делает выводы о выполнимости технических мер на основе собранных данных.

Но ручная проверка отнимает огромное количество времени, а результат может быть неточным за счет человеческого фактора. Также ПО DATAPK не имеет функционала поиска беспроводных точек доступа.

Актуальность темы исследования обусловлена потребностью заказчика в автоматизации проведения аудита и проверки на соответствие техническим мерам безопасности.

Гипотеза исследования: на основе полученных данных ПО DATAPK могут быть выявлены критерии принятии решений и построена автоматизированная система проверки выполнимости технических мер.

Целью исследования является: проектирование системы для атомизации проведения аудита технических мер безопасности по результатам работы ПО DATAPK.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Ознакомиться с требованиями о защите информации.
2. Изучить систему сбора данных ПО DATAPK.
3. Разработать критерии оценки соблюдения мер.
4. Разработать шаблон технического отчета с результатами проведения аудита субъекта КИИ.
5. Разработать сопроводительную документацию.
6. Разработать техническое задание.

Объектом исследования является ПО для проведения аудита технических мер защиты информации.

Предметом исследования является автоматизированная система для проведения аудита технических мер защиты информации.

Методы исследования включают в себя:

– анализ бизнес-процесса КИИ;

– анализ требований о защите информации;

– анализ решений для сбора необходимых данных;

– выявление критериев проверки технических мер;

– интервью с потенциальными пользователями для сбора требований и формирования видения процесса, который автоматизирует система.

Научная новизна заключается в проектировании новой системы, подходящей под цели государственного заказчика.

Теоретической основой исследования стали системы сбора данных: ПО DATAPK и программы для мониторинга сети.

Теоретическая и практическая значимость разработана архитектура нового программного обеспечения атомизации проведения аудита технических мер безопасности по результатам работы программного обеспечения DATAPK

База исследования является информационная среда субъекта КИИ и ПО DATAPK.

Магистерская диссертация состоит из введения, трех глав и заключения, изложенных на 69 страницах, а также библиографического списка. В работе имеется 5 рисунков. Библиографический список состоит из 53 наименований.

В первой главе изложено теоретическое обоснование работы, рассмотрены особенности проведения аудита на предприятии, выявлены и проанализированы проблемы связанные с бизнес-процессом проведения аудита на предприятии заказчика.

Вторая глава представляет собой анализ инструмента для проведения аудита. Выявлены критерии оценки соблюдения мер на основе полученных

данных от инструмента для проведения аудита. Выявлены недостатки используемого инструмента и меры, для которых инструмент не имеет необходимого функционала. Осуществлен сравнительный анализ существующих инструментов для обнаружения уязвимостей.

В третьей главе приведено итоговое решение архитектуры системы, определены требования к системе.

В заключении интерпретируются основные выводы, полученные из всей работы.

Общий объем магистерской диссертации составляет 115 страниц. Работа содержит 10 таблиц, 5 рисунков, 4 приложения.

1. Изучение предметной области

1.1 Определение критической информационной инфраструктуры

Критическая информационная инфраструктура (КИИ) – это информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов КИИ, а также сети электросвязи, используемые для организации их взаимодействия. [1]

Критическая информационная инфраструктура относится к компьютерным системам, которые необходимы для функционирования экономики страны, безопасности и общественной безопасности. Это активы и системы, которые настолько жизненно важны, что их разрушение или уничтожение может оказать существенное влияние на национальную безопасность, общественное здравоохранение, экономическую стабильность или любой другой критический аспект инфраструктуры страны.

К объектам КИИ относятся [2]:

– Информационные системы субъектов КИИ;

– Информационно-телекоммуникационные сети субъектов КИИ;

– Автоматизированные системы управления субъектов КИИ;

– Единая сеть электросвязи, обеспечивающая взаимодействие вышеуказанных объектов.

К субъектам КИИ относятся [2]:

– Государственные органы и государственные учреждения;

– Организации здравоохранения;

– организации науки;

– Организации транспорта;

– Организации связи;

– Организации энергетики;

– Организации банковской сферы и иных сфер финансового рынка;

– Организации топливно-энергетического комплекса;

– Организации атомной энергии;

– Организации оборонной промышленности;

– Организации ракетно-космической промышленности;

– Организации горнодобывающей промышленности;

– Организации металлургической промышленности;

– Организации химической промышленности;

– Российские юридические лица, которые обеспечивают взаимодействие указанных субъектов.

В 2017 г. в России был принят федеральный закон 187-ФЗ «О безопасности критической информационной инфраструктуры РФ». Закон обязывает организации, которые относят себя к КИИ, определять уровень критичности их ПО в масштабах государства. Прежде всего речь идет об оценке информационных систем [7].

Данный закон наделяет Правительство Российской Федерации полномочиями устанавливать правила и требования по обеспечению информационной безопасности КИИ, а также осуществлять контроль и надзор за соблюдением этих требований.

Информационная безопасность (ИБ) – это состояние защищенности информационной среды организации, обеспечивающее его функционирование и развитие в соответствии с его целями и задачами [5].

При обеспечении ИБ наряду с процессами реализации защитных мер, обучения персонала, внедрения политики безопасности и т. д., важное значение имеют процессы контроля и проверки состояния ИБ. Такой контроль позволяет выявить уязвимости в существующих системах КИИ. Среди процессов контроля и проверки ИБ особое положение занимает аудит ИБ, основным назначением которого является формирование независимой оценки уровня ИБ.

Рассмотрим особенности проведения аудита информационной безопасности на критической информационной инфраструктуре.

1.2 Особенности проведения аудита критической информационной инфраструктуры

Аудит информационной безопасности – комплекс организационно технических мероприятий, проводимых независимыми экспертами, имеющих целью оценить состояние ИБ объекта аудита и степени его соответствия критериям аудита [4].

Проведения аудита на КИИ – это систематическая оценка безопасности, надежности и доступности систем информационных технологий, поддерживающих работу критической инфраструктуры. Задачами аудита является:

1. Оценка рисков. Включает в себя выявление потенциальных угроз, уязвимостей и последствий взлома или сбоя.

2. Оценка мер безопасности. Сюда входят политики, процедуры и технические элементы управления, такие как системы обнаружения вторжений и средства контроля доступа.

3. Планы реагирования на инциденты. Существуют для устранения инцидентов безопасности или системных сбоев. Это включает в себя оценку эффективности планов и процедур их тестирования и обновления.

4. Проверка устойчивости системы. Аудитор должен проверить устойчивость систем критической инфраструктуры, чтобы убедиться, что они могут продолжать работать во время и после кибератаки, стихийного бедствия или другого разрушительного события.

5. Проверка соответствия. Аудитор должен проверить соблюдение соответствующих правил, стандартов и передовых методов обеспечения безопасности критически важных систем инфраструктуры. Это включает в себя оценку политик и процедур организации, документации и программ обучения.

6. Формирование рекомендаций по комплексу мер, направленных на повышение эффективности существующей системы защиты. Составление технической документации.

В целом цель аудита КИИ состоит в выявлении слабых мест в состоянии безопасности систем и предоставлении рекомендаций по повышению их безопасности, надежности и отказоустойчивости.

При проведении аудита ИБ обычно проводится следующая последовательность мероприятий [5, 6]:

1. этап – подготовительный:

– Выбор субъекта аудита;

– Выбор критериев и методов аудита;

– Выбор средств и способов аудита;

– Формирование команды аудиторов;

– Определение объема и масштаба аудита, установление его сроков.

2. этап – основной:

– Определение объектов защиты;

– Анализ состояния ИБ объекта аудита;

– Регистрация, сбор и проверка статистических данных и результатов инструментальных измерений уязвимостей и угроз;

– Оценка результатов проверки;

– Формирование отчета о результатах проверки по отдельным элементам объекта аудита и различным аспектам ИБ.

3. этап – заключительный:

– Составление итогового отчета;

– Формирование рекомендаций по комплексу мер, направленных на повышение эффективности существующей системы защиты;

– Указание на угрозы информационной безопасности в компании клиента и задачи, которые служба ИБ должна закрыть;

– Разработка плана мероприятий по устранению уязвимостей и недостатков в обеспечении ИБ.

Для проведения аудита критической информационной инфраструктуры аудитор должен хорошо разбираться в информационной безопасности, а также в соответствующих отраслевых стандартах и правилах. Аудитор также должен обладать следующими компетенциями:

– Техническими знаниями. Аудитор должен иметь четкое представление о технических аспектах информационной безопасности, включая сетевую безопасность, шифрование, уметь работать с системами обнаружения и предотвращения вторжений, а также с инструментом оценки уязвимостей.

– Нормативные знания. Аудитор должен хорошо разбираться в соответствующих отраслевых стандартах, правилах и законе № 187-ФЗ.

– Управление рисками. Аудитор должен хорошо понимать принципы управления рисками, включая оценку, снижение и мониторинг рисков. Он должен уметь выявлять потенциальные риски и уязвимости безопасности и разрабатывать стратегии по их снижению.

– Аналитические навыки. Аудитор должен обладать сильными аналитическими навыками и уметь выявлять закономерности и тенденции в данных. Он должны уметь использовать инструменты и методы анализа данных для выявления потенциальных угроз безопасности и уязвимостей.

В целом, аудитор должен обладать сочетанием технических и социальных навыков для эффективного аудита критической информационной инфраструктуры. Он должен уметь работать независимо и в составе команды, а также уметь адаптироваться к изменяющимся обстоятельствам и требованиям.

1.3 Аудит на соответствие требованиям приказа ФСТЭК № 187-ФЗ

Аудит информационных систем проводится на соответствие требованиям законодательства Российской Федерации и нормативных документов в области защиты информации.

Приказ ФСТЭК № 187-ФЗ утверждает, что наиболее критичные объекты КИИ необходимо защищать особыми мерами. Что именно нужно делать, описывает Приказ ФСТЭК № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры РФ» от 25 декабря 2017 года. [7]

В 239-м Приказе ФСТЭК России изложены требования к обеспечению информационной безопасности критической информационной инфраструктуры в стране. Ключевые требования 239-го Приказа включают:

– Идентификация и классификация активов. Организации должны идентифицировать и классифицировать свои активы, включая оборудование, программное обеспечение, данные и каналы связи.

– Оценка рисков. Организации должны проводить регулярные оценки рисков, чтобы выявлять и снижать потенциальные риски безопасности для своих активов.

– Контроль доступа: доступ к активам должен строго контролироваться и предоставляться только уполномоченному персоналу. Доступ должен предоставляться на основе принципа наименьших привилегий.

– Защита данных: активы должны быть защищены от несанкционированного доступа, модификации или уничтожения. Это включает в себя использование шифрования, резервного копирования и мер по предотвращению потери данных.

– Сетевая безопасность: активы должны быть защищены от внешних угроз, таких как взлом, вредоносное ПО и атаки типа «отказ в обслуживании». Это требует реализации мер сетевой безопасности, таких как брандмауэры,

системы обнаружения и предотвращения вторжений, а также инструменты мониторинга безопасности.

– Реагирование на инциденты. Организации должны иметь план реагирования на инциденты, чтобы быстро и эффективно реагировать на инциденты безопасности. План должен включать процедуры обнаружения, сообщения и реагирования на инциденты, анализ и документирование инцидента, а также процедуры восстановления нормальной работы.

Приказ предусматривает возможность применения мер защиты, сгруппированных в 15 групп.

1. Идентификация и аутентификация (ИАФ) – мера посвящена обеспечению безопасной идентификации и аутентификации пользователей, имеющих доступ к ресурсам критической информационной инфраструктуры.

Мера ИАФ включает следующие требования к организациям, эксплуатирующим активы:

– Надежные пароли. Приказ требует использования надежных паролей, отвечающих определенным требованиям сложности, таким как минимальная длина и комбинация букв, цифр и символов.

– Механизм одноразовых паролей при аутентификации пользователей, осуществляющих удаленный или локальный доступ;

– Многофакторная аутентификация. Приказ требует использования многофакторной аутентификации для пользователей, которые получают доступ к активам. Это включает использование смарт-карт, токенов, биометрической аутентификации или других методов.

2. Управлением доступа (УПД) – основное внимание уделяется внедрению эффективных мер контроля доступа, чтобы гарантировать, что только авторизованные пользователи имеют доступ к ресурсам критической информационной инфраструктуры.

Мера УПД приказа ФСТЭК включает следующие требования к организациям:

– Управление доступом на основе ролей. Требуется реализация управления доступом на основе ролей для управления доступом к активам КИИ.

– Управление учетными записями пользователей. Приказ требует безопасного управления учетными записями пользователей, включая создание, изменение и удаление учетных записей. Приказ также требует, чтобы неактивные учетные записи пользователей отключались или удалялись по истечении определенного периода времени.

– Разделение полномочий. Приказ требует реализации разделения ролей для предотвращения конфликта интересов и несанкционированных действий.

– Мониторинг доступа и регистрации. Приказ требует регистрации всех попыток доступа к активам. Это включает в себя отслеживание успешных и неудачных попыток входа в систему, изменения разрешений на доступ и доступ к конфиденциальным данным.

3. Защита машинных носителей информации (ЗНИ) -особое внимание уделяется защите конфиденциальности и целостности активов критической информационной инфраструктуры, которые хранятся на машинных носителях, таких как жесткие диски, твердотельные накопители и другие устройства хранения.

Мера ЗНИ включает следующие требования к организациям:

– Контроль перемещения машинных носителей информации за пределами контролируемой зоны. Требуется безопасное обращения с машинными носителями как во время использования, так и при их транспортировке или хранении. Это включает в себя защиту носителей от физического повреждения, кражи и несанкционированного доступа.

– Исключение возможности несанкционированного чтения информации на машинных носителях информации. Требуется шифрование машинных носителей, на которых хранятся важные или конфиденциальные данные. Шифрование должно выполняться с использованием надежных

алгоритмов и длин ключей, а ключи должны быть защищены и управляться надежно.

4. Аудит безопасности (АУД) -основное внимание уделяется обеспечению проведения регулярных аудитов безопасности для выявления и снижения рисков безопасности для активов критической информационной инфраструктуры.

Мера АУД включает следующие требования к организациям:

– Генерирование временных меток и синхронизация системного времени. Требуется, чтобы системное время на разных устройствах в активах синхронизировалось точно и последовательно. Это включает в себя использование таких протоколов, как NTP или PTP, для синхронизации времени между устройствами и обеспечение того, чтобы синхронизация выполнялась безопасно и в соответствии с передовыми методами.

– Регистрация событий безопасности. Приказ требует, чтобы создавались и хранились журналы событий безопасности, включая попытки доступа, изменения конфигурации и другие события, связанные с безопасностью. Журналы должны храниться надежно и защищены от несанкционированного доступа или изменения.

– Реагирование на сбои при регистрации событий безопасности. Требуется, чтобы у организаций был задокументированный план реагирования на инциденты, который включает процедуры реагирования на инциденты безопасности, обнаруженные с помощью анализа журналов. План следует регулярно тестировать и обновлять по мере необходимости.

5. Обеспечение целостности (ОЦЛ) -основное внимание уделяется обеспечению целостности и подлинности активов критической информационной инфраструктуры, таких как программное обеспечение, микропрограммы и аппаратные компоненты.

Мера ОЦЛ включает следующие требования к организациям: [8]

– Контроль целостности программного обеспечения. Требуется, чтобы программное обеспечение, используемое в активах, было проверено,

чтобы гарантировать, что оно является подлинным и не было изменено или подделано. Это включает в себя проверку цифровых подписей, контрольных сумм или других криптографических механизмов для обеспечения целостности программного обеспечения.

– Ограничения по вводу информации в информационную (автоматизированную) систему. Приказ требует, чтобы доступ к информации, введенной в активы, контролировался для предотвращения несанкционированного доступа или модификации. Это включает в себя использование контроля доступа, механизмов аутентификации и других мер безопасности для защиты конфиденциальной информации.

– Контроль ошибочных действий пользователей по вводу и передаче информации и предупреждение пользователей об ошибочных действиях. Приказ требует, чтобы организации применяли меры по контролю ошибок для предотвращения ошибочного ввода или передачи информации. Это включает в себя использование проверки ввода, механизмов исправления ошибок и других мер для предотвращения ошибок.

6. Обеспечение доступности (ОДТ) -основное внимание уделяется управлению доступностью активов критической информационной инфраструктуры, чтобы обеспечить их доступность для авторизованных пользователей, когда это необходимо.

Мера ОДТ включает следующие требования к организациям:

– Контроль безотказного функционирования средств и систем. Требуется использование отказоустойчивых технических средств в системах, поддерживающих критичные бизнес-процессы или предоставляющих критичные сервисы пользователям.

– Резервное копирование информации. Приказ требует, чтобы организации внедрили соответствующие механизмы резервного копирования и восстановления для обеспечения доступности данных и систем в случае сбоя. Это включает в себя регулярное резервное копирование и обслуживание резервных систем, которые можно активировать в случае сбоя.

– Обеспечение возможности восстановления информации. Это включает в себя регулярное резервное копирование критически важных данных и поддержку резервных систем, которые можно активировать в случае сбоя.

7. Защита информационной (автоматизированной) системы и ее компонентов (ЗИС) -включают ряд мер безопасности, таких как механизмы контроля доступа, шифрование, системы обнаружения и предотвращения вторжений, антивирусное программное обеспечение и брандмауэры. Мера предназначена для предотвращения несанкционированного доступа к системе, защиты от вредоносных программ и других угроз безопасности, а также для обеспечения целостности и конфиденциальности данных, обрабатываемых системой.

Мера ЗИС включает следующие требования к организациям: [8]

– Разделение функций по управлению информационной системой с иными функциями.

– Использование программного обеспечения, функционирующего в средах различных операционных систем.

– Реализация электронного почтового обмена с внешними сетями через ограниченное количество контролируемых точек.

– Защита информации при ее передаче по каналам связи.

– Запрет несанкционированной удаленной активации периферийных устройств.

– Использование устройств терминального доступа.

– Защита беспроводных соединений.

– Управление сетевыми соединениями.

– Защита информации при использовании мобильных устройств.

8. Реагирование на компьютерные инциденты (ИНЦ) -включает в себя создание групп реагирования на инциденты и разработку планов реагирования на инциденты, в которых излагаются процедуры выявления, сдерживания, анализа и разрешения инцидентов безопасности.

Мера ИНЦ включает следующие требования к организациям: [8]

– Выявление компьютерных инцидентов.

– Информирование о компьютерных инцидентах.

– Устранение последствий компьютерных инцидентов.

– Хранение и защита информации о компьютерных инцидентах.

9. Управление конфигурацией (УКФ) -включает установление процедур управления конфигурацией и разработку базовых показателей конфигурации, определяющих авторизованную конфигурацию системы. Эти базовые показатели должны включать информацию об оборудовании, программном обеспечении и других компонентах системы, а также любые параметры безопасности или другие параметры конфигурации.

Мера УКФ включает следующие требования к организациям: [8]

– Управление изменениями. Приказ требует механизм контроля изменений в конфигурации системы, включая внедрение процессов и процедур управления изменениями, аудит и проверку конфигурации, а также механизмы контроля версий.

– Установка только разрешенного к использованию программного обеспечения.

Далее необходимо проанализировать проведение аудита на предприятии заказчика.

1.4 Проведение аудита на предприятии заказчика

На данный момент процесс проведения аудита информационной безопасности выглядит следующим образом.

Высококвалифицированный человек -аудитор, приходит на территорию субъекта критической информационной инфраструктуры с вспомогательными инструментами для сбора необходимых данных. Аудиторов может быть несколько.

Группа аудиторов вместе с руководством предприятия определяет объем аудита, критические активы и системы, подлежащие аудиту. Также определяются цели аудита, методологии и сроки.

Затем группа прибывает на предприятие заказчика, где с помощью сторонних инструментов собирает данные из сети, проверяя входящий и исходящий трафик сети, наличие не одобренных потоков, наличие уязвимостей. После чего проверяет на соответствие техническим мерам безопасности вручную.

На каждом объекте защиты (сокращенно ОЗ) аудитор, с помощью сторонних инструментов собирает данные о политиках, процедурах, системах и средствах контроля предприятия. Количество таких объектов защиты может достигать сотни. После чего проверяет на соответствие техническим мерам безопасности вручную.

В случае, если с помощью вспомогательного инструментария не были собраны необходимые данные, аудитор проверяет каждый объект защиты вручную. Например: наличие антивирусной программы, длину пароля, наличие политик по ограничению неуспешных попыток и так далее.

Также аудитор проверяет отчет с предыдущей проверки, проводит анкетирование и анализ документов. По завершению аудитор подготавливает исчерпывающий отчет, в котором излагаются выводы, рекомендации и корректирующие действия, которые необходимо предпринять для повышения безопасности, надежности и доступности критически важных систем инфраструктуры.

Бизнес-процесс проведения аудита представлен на рис. 1.

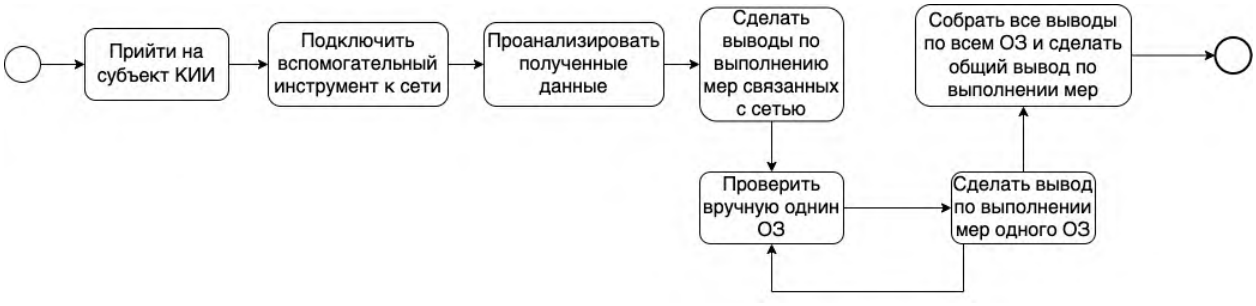

Рисунок 1 -Бизнес-процесс аудита

Далее я рассмотрю проблемы и узкие места в текущем бизнес-процессе аудита.

1.5 Проблемы бизнес-процесса проведения аудита на предприятии заказчика.

Проведя интервью с заказчиком и проанализировав бизнес-процесс, выявились следующие проблемы:

1. На проведение аудита тратиться большое количество времени, от нескольких дней до месяца.

Одной из серьезных проблем, связанных с проведением аудита, является большое количество времени, необходимое для проведения процесса. Продолжительность аудита может варьироваться в зависимости от размера и сложности критической информационной инфраструктуры организации. Для проведения тщательной оценки может потребоваться несколько недель или даже месяцев.

Аудитор обязан проверить каждый объект на выполнимость 20 технических мер. Для этого необходимо проанализировать большой объем данных и документации, чтобы получить всестороннее представление о критически важной информационной инфраструктуре организации. Из-за этого на 1 объект тратиться от 1 до 3 часов.

Кроме того, аудит проводится с высокой степенью строгости и вниманием к деталям, поскольку безопасность и отказоустойчивость критически важной информационной инфраструктуры имеют первостепенное значение. Аудиторы должны тщательно оценить все потенциальные риски и уязвимости, чтобы убедиться, что критическая информационная инфраструктура организации адекватно защищена от киберугроз.

Таким образом, проблема большого количества времени на проведение аудита связана со сложностью и важностью процесса оценки. Хотя это может занять много времени, это имеет решающее значение для обеспечения

безопасности и устойчивости критически важной информационной инфраструктуры организации.

2. Аудитор проверяет только часть объектов.

Из-за большого количества объектов защиты на предприятии аудитор ввиду своей невнимательности или даже лени может пропустить несколько объектов защиты для проверки, например в связи с тем, что на большинстве проверенных объектов защиты технические меры были выполнены.

Проблема с проверкой только части объектов может привести к упущению значительных уязвимостей безопасности.

Если аудиторы сосредоточатся только на определенных объектах, они могут пропустить критические недостатки или угрозы, существующие в других частях инфраструктуры.

Например, предположим, что в организации есть объект, который не проверяется в рамках аудита. В этом случае он может быть уязвим для киберугроз, и организация может не знать об этой уязвимости, пока не станет слишком поздно. Точно так же, если аудитор не проверят все сетевые сегменты или устройства, некоторые потенциальные атаки могут остаться незамеченными.

Более того, аудиторы могут сосредоточиться только на конкретных компонентах, которые они считают наиболее важными, игнорируя потенциальный риск, связанный с другими компонентами, которые могут быть не столь очевидными. Это может привести к ложному чувству безопасности и оставить организацию открытой для атак.

Поэтому важно провести аудит всех объектов защиты организации, чтобы гарантировать, что процесс оценки является всеобъемлющим и эффективным. Проверяя только часть ресурсов, организация может пропустить критические уязвимости и не достичь намеченных целей аудита, заключающихся в обеспечении безопасности и отказоустойчивости критической информационной инфраструктуры.

3. Аудитор совершает ошибки при проверке выполнимости мер.

Так как аудит проводит человек, а не система, всегда существует риск совершения ошибки за счет человеческого фактора. Даже небольшая ошибка или недосмотр могут иметь серьезные последствия.

Ошибки в процессе аудита могут привести к неточным или неполным оценкам состояния безопасности организации, что может сделать организацию уязвимой для кибератак.

Некоторые из распространенных ошибок, которые аудиторы могут совершать в процессе аудита КИИ, перечислены ниже:

– Некорректное понимание инфраструктуры организации. Аудиторы могут неправильно понять критическую инфраструктуру организации, что приведет к неполной оценке рисков безопасности.

– Плохая коммуникация: недопонимание между аудиторами и персоналом организации может привести к упущенным уязвимостям, упущенным из виду рискам и неверным предположениям.

– Недостаток опыта: неопытные аудиторы могут пропустить критические уязвимости, неправильно интерпретировать данные или не выявить потенциальные угрозы.

– Некорректная документация: если аудит не задокументирован должным образом, может быть сложно отслеживать ход выполнения, определять области, требующие улучшения, или проверять соответствие.

– Игнорирование ключевых элементов управления. Аудиторы могут упускать из виду критические элементы управления безопасностью, что приводит к упущенным уязвимостям и подвергает организацию риску кибератак.

Проблема человеческого фактора при аудите может быть решена путем использования автоматизированных инструментов и технологий, что также повысит точность результатов аудита.

4. Результаты аудита не соответствует действительности.

Отчет об аудите является важнейшим результатом процесса аудита критической информационной инфраструктуры, и его точность имеет

решающее значение для принятия организацией обоснованных решений о своем состоянии безопасности. Однако, в некоторых случаях заключение может не соответствовать действительности, что может привести к существенным проблемам для организации.

Проблема с неточным отчетом заключается в том, что он может создать у организации ложное ощущение безопасности. Если в отчете указано, что критическая инфраструктура организации защищена, хотя на самом деле это не так, организация может не принять надлежащих мер по устранению уязвимостей, что приведет к повышенному риску кибератак.

Существует несколько причин, по которым отчет может не соответствовать действительности, в том числе:

– Неполный аудит: если аудиторы не протестируют все критические компоненты инфраструктуры организации, они могут пропустить уязвимости, которые могут быть использованы злоумышленниками.

– Сбор неточных данных: если аудиторы собирают неточные или неполные данные в процессе аудита, результаты аудита могут не отражать фактическое состояние безопасности организации.

– Отсутствие понимания: если аудиторы не полностью понимают критическую инфраструктуру организации, они могут упустить из виду потенциальные уязвимости или не определить соответствующие меры безопасности.

– Предвзятая отчетность: если у аудиторов есть конфликт интересов или они предвзято относятся к организации, они могут подготовить отчет, который не отражает фактическое состояние безопасности.

5. Нехватка высококвалифицированных кадров.

Проблема нехватки квалифицированных кадров для проведения аудита КИИ является серьезной проблемой, с которой сталкиваются многие организации. Аудит требует специальных навыков и опыта в таких областях, как кибербезопасность, управление рисками, приказы РФ. Отсутствие

квалифицированного персонала может привести к ряду проблем в процессе аудита, в том числе:

– Неточные оценки. Недостаток опыта может привести к неправильной оценке рисков безопасности и уязвимостей инфраструктуры организации.

– Нехватка квалифицированного персонала может привести к задержкам в процессе аудита, что приведет к увеличению сроков и затрат.

– Повышенный риск кибератак: нехватка квалифицированного персонала может сделать организацию уязвимой для кибератак, поскольку уязвимости и угрозы могут остаться незамеченными.

Ниже представлен SWOT-анализ [9] предприятия заказчика в таблице 1.

Таблица 1 – SWOT-анализ предприятия

Сильные стороны	Слабые стороны
Всесторонний анализ. Индивидуальный подход.	Отнимает много времени. Дорого. Неполный аудит.
Возможности	Угрозы
Повышение эффективности за счет автоматизации.	Ошибки за счет человеческого фактора. Изменение нормативно-правовой базы.

Сильные стороны:

– Всесторонний анализ. Ручной аудит позволяет аудиторам провести тщательный анализ критической инфраструктуры организации, выявляя потенциальные уязвимости и риски, которые могут быть упущены автоматическими инструментами.

– Индивидуальный подход. Ручной аудит можно адаптировать к конкретным потребностям организации, уделяя особое внимание областям, наиболее важным для деятельности организации.

Слабые стороны:

– Отнимает много времени. Ручной аудит может занять много времени, требуя значительных усилий для проверки всех критических компонентов инфраструктуры и выявления потенциальных рисков.

– Дорого. Ручной аудит может быть дорогим, требуя квалифицированного персонала со специальными знаниями и потенциально специализированным оборудованием или инструментами.

– Неполный аудит. Ручной аудит может не охватывать все критические компоненты системы, что может привести к потенциальным пробелам в процессе аудита и невозможности выявить все риски и уязвимости.

Возможности:

– Повышение эффективности. Автоматизация процесса проведения аудита может помочь повысить эффективность ручного аудита, позволяя аудиторам проводить аудит быстрее и с большей точностью.

Угрозы:

– Человеческий фактор. Ручной аудит может быть подвержен человеческому фактору, что может привести к неправильной оценке рисков безопасности и уязвимостей.

– Изменение нормативно-правовой базы. Изменения в нормативных актах и требованиях соответствия могут повлиять на процесс аудита, требуя от аудиторов адаптации своего подхода и потенциально увеличивая время и стоимость аудита.

1.6 Выводы по первой главе

Подводя итог материалу первой главы, можно сделать следующие краткие обобщенные выводы.

1. Критическая информационная инфраструктура – это информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов КИИ, а также сети электросвязи, используемые для организации их взаимодействия.

2. Аудит является важной формой контроля и проверки состояния ИБ. Такой контроль позволяет проверить адекватность выбранных мер и средств защиты, а также выявить уязвимости в существующих информационных системах.

3. Аудит информационных систем проводится на соответствие Приказу ФСТЭК № 187-ФЗ. В приказе изложены требования, в виде технических мер, к обеспечению информационной безопасности критической информационной инфраструктуры в стране.

4. Бизнес-процесс проведения аудита заказчика имеет серьезные проблемы:

– На проведение аудита тратиться большое количество времени, от нескольких дней до месяца.

– Аудитор проверяет только часть объектов.

– Аудитор совершает ошибки при проверке выполнимости мер.

– Результаты аудита не соответствует действительности.

– Нехватка высококвалифицированных кадров.

2. Анализ инструментов для проведения аудита

2.1 Система сбора данных «DATAPK»

Заказчик использует инструмент для проведения аудита - «DATAPK». CL DATAPK – программно-аппаратный комплекс российского производства, обеспечивающий кибербезопасность автоматизированной системы управления технологическим процессом (АСУ ТП) [10].

Программно-аппаратный комплекс «CL DATAPK» разрабатывается компанией «СайберЛимфа». Продукт обеспечивает оперативный мониторинг и контроль состояния защищенности систем автоматизации критически важных объектов и объектов критической информационной инфраструктуры, в частности АСУ ТП [10].

По состоянию на 2015 год программный комплекс «CL DATAPK» являлся одним из трёх российских решений по защите АСУ ТП [11]. В апреле 2017 года ФСТЭК России внесла CL DATAPK в Государственный реестр сертифицированных средств защиты информации [12]. В сентябре 2018 года комплекс внесен в Единый реестр российских программ для электронных вычислительных машин и баз данных [13].

DATAPK спроектирован таким образом, что предусматривает возможность эксплуатации в иерархических распределённых системах. Иерархия DATAPK может насчитывать до трёх уровней, на каждом из которых применяется наиболее эффективный вариант исполнения аппаратной платформы специального назначения: [14]

- DATAPK уровня технологического комплекса – реализует базовый набор функций по сбору информации непосредственно с объектов защиты, включающий автоматическое определение состава АСУ ТП, сбор событий, анализ защищённости и др.;
- DATAPK уровня филиала – дополнительно к базовому набору реализует возможности нормализации, корреляции событий, выявления инцидентов ИБ, визуализации информации;

– DATAPK уровня предприятия – реализует максимальный набор функций, помимо двух предыдущих уровней включающий возможности централизованного обновления ПО, а также управления подчинёнными DATAPK всей иерархии.

Архитектура типовой иерархической системы на основе комплексов DATAPK представлена на рисунке 2.

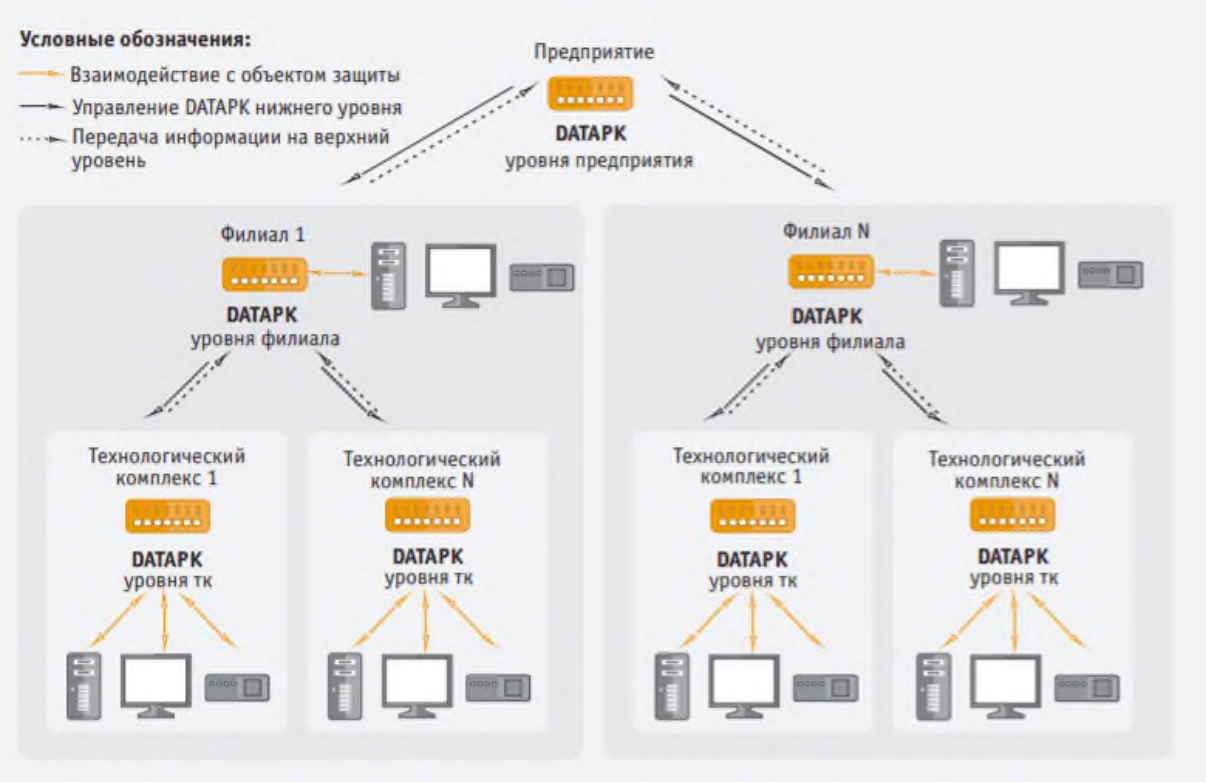

Рисунок 2 -Иерархия комплексов DATAPK

«DATAPK» – программный комплекс, предназначенный для оперативного мониторинга состояния информационной безопасности и контроля состояния защищенности производственных и технологических комплексов. Основной функционал программного комплекса перечислен ниже.

Мониторинг и анализ событий информационной безопасности. ПО отслеживает различные события, связанные с информационной безопасностью, включая попытки несанкционированного доступа, системные сбои, вирусные атаки и другие инциденты, связанные с безопасностью. Система анализирует события и оповещает в режиме реального времени.

Оценка и управление рисками. Программный комплекс оценивает и анализирует риски, связанные с угрозами и уязвимостями информационной безопасности, и дает рекомендации по снижению этих рисков. Система предоставляет инструменты для управления рисками, включая оценки рисков, планы управления рисками и стратегии снижения рисков.

Контроль доступа к информационным ресурсам. Программный комплекс контролирует доступ к информационным ресурсам и системам, обеспечивая доступ к конфиденциальной информации только авторизованным пользователям. Система предоставляет инструменты для аутентификации пользователей, контроля доступа и авторизации.

Обнаружение и предотвращение кибератак. Программный комплекс обнаруживает и предотвращает кибератаки, в том числе вирусы, черви, трояны и другое вредоносное ПО. Система предоставляет инструменты для выявления и нейтрализации угроз, включая межсетевые экраны, системы обнаружения вторжений и антивирусное программное обеспечение.

Реагирование на инциденты и восстановление. Программный комплекс предоставляет инструменты для реагирования на инциденты и восстановления в случае нарушения безопасности или другого инцидента, связанного с безопасностью. Система предоставляет инструменты управления инцидентами, включая планы реагирования на инциденты, отчеты об инцидентах и их расследование.

DATAPK предназначен для выявления: [15]

– Несанкционированных изменений в АСУ ТП;

– Незащищенных компонентов АСУ ТП;

– Компонентов АСУ ТП, подверженных критическим уязвимостям;

– Попыток эксплуатации уязвимостей компонентов АСУ ТП до момента их устранения;

– Регистрации событий ИБ в АСУ ТП;

– Автоматизированного контроля выполнения требований ИБ в АСУ ТП.

Распределение основных поддерживаемых функций DATAPK по уровням иерархии приведены на рисунке 3.

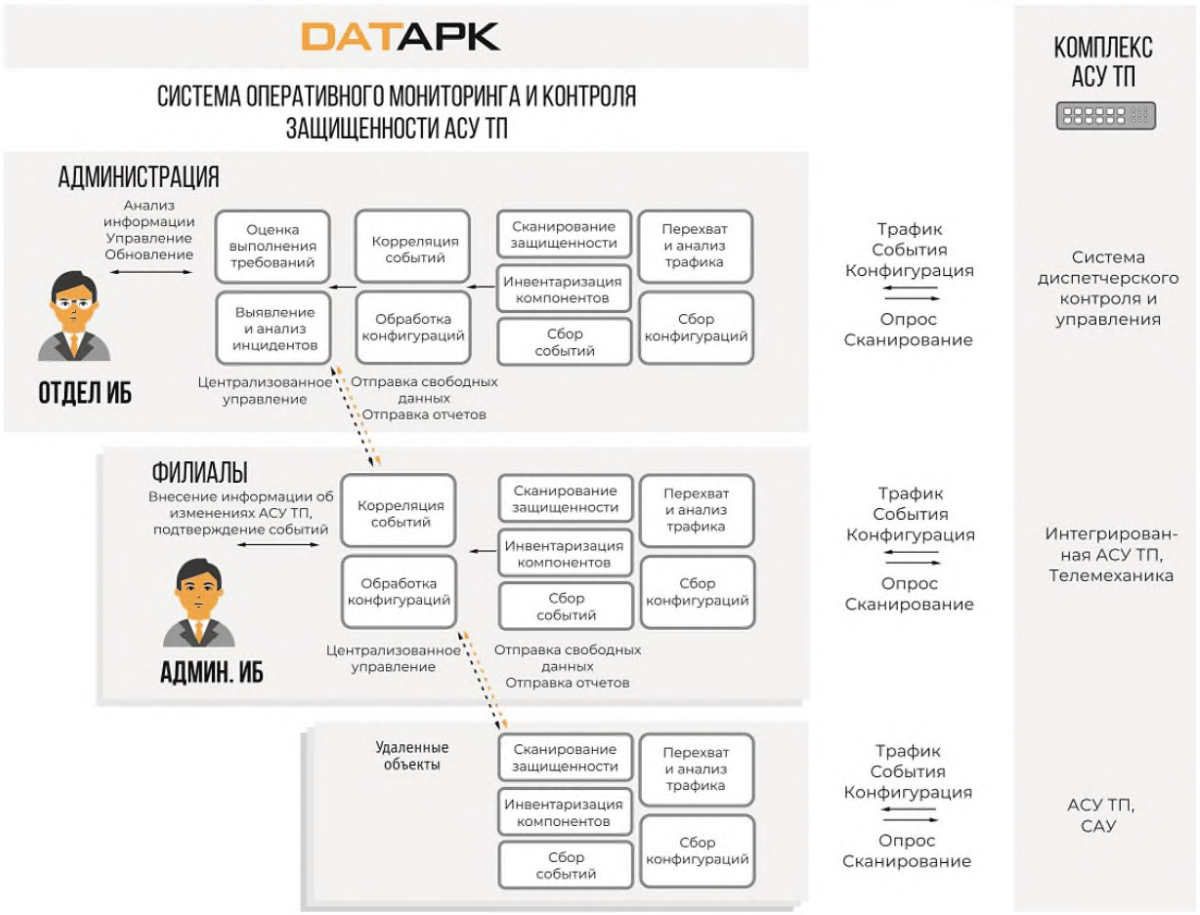

Рисунок 3 -Типовая функциональная архитектура DATAPK в распределённой конфигурации

DATAPK может функционировать в одном из двух режимов, различающихся объёмом собираемых сведений и степенью влияния на компоненты АСУ ТП:

1. Пассивный мониторинг -однонаправленное получение информации.[16] Сбор событий возможен только в том случае, если её компоненты настроены на самостоятельную отправку событий, при которой не требуется подтверждение их получения со стороны сервера

2. Активный мониторинг -обмен информации с компонентами АСУ ТП с использованием штатных механизмов взаимодействия. [16]

2.2 Выявление критериев оценки соблюдения мер

Для каждой технической меры необходимо выявить критерии оценки выполнимости мер, а также проверить достаточность данных в DATAPK для проверки всех мер.

1. ИАФ.1 – Идентификация и аутентификация пользователей и инициированных ими процессов. Для выполняемости меры должна отсутствовать возможности беспарольного входа на конечных ОЗ. DATAPK возвращает параметр default password и minimalPassworgLength. Параметр default password – это парольная политика, запрещающая вход без ввода пароля, должен отсутствовать или быть выключенным. Параметр minimalPassworgLength – это минимальная длина пароля, должен быть больше или равен заданному, пользователем, значению.

2. ИАФ.2 – Идентификация и аутентификация устройств. Для проверки данной меры необходимо собрать информацию по всем существующим ОЗна предприятии. DATAPK не имеет необходимого функционала для проверки данной меры.

3. ИАФ.3 – Управление идентификаторами. Для проверки данной меры необходимо выявить наличие установленной операционной системы (сокращенно ОС) семейства Windows, Linux. DATAPK возвращает список ОС, установленных на каждом ОЗ.

4. ИАФ.4 – Управление средствами аутентификации. Для выполняемости меры должна быть настроена парольная политика с указанными параметрами аутентификации. DATAPK возвращает следующие параметры:

- Минимальная длина пароля;
- Максимальный срок действия пароля;
- Минимальный срок действия пароля;
- Пароль должен отвечать требованиям сложности;
- Требовать не повторяемости паролей;

– Хранить пароли, используя обратимое шифрование.

Необходимо все возвращаемые параметры сравнить с заданными, пользователем, значениями, так как проверка меры не автоматизирована.

5. ИАФ.7 – защита аутентификационной информации при передаче. Для выполняемости меры должны быть настроены параметры защиты трафика аутентификации на ОЗ. DATAPK возвращает следующие параметры:

– отправлять не зашифрованный пароль сторонним SMB-серверам;

– минимальная сеансовая безопасность для клиентов на базе NTLM SSP (включая безопасный RPC).

Необходимо все возвращаемые параметры сравнить с заданными, пользователем, значениями, так как проверка меры не автоматизирована.

6. УПД.4 – разделение полномочий (ролей) пользователей. Для проверки данной меры необходимо наличие ролевой модели в политике управления доступом. Должно существовать минимум две группы пользователей: администратор и обычный пользователь и хотя бы один пользователь должен не состоять в группе администраторы.

Необходимо выявлять количество групп пользователей на каждом ОЗи проверять на наличие ролевой модели.

7. УПД.6 – ограничение неуспешных попыток доступа в автоматизированную систему управления (доступа к системе). Для проверки данной меры необходимо наличие политики УЗ, ограничивающей число неуспешных попыток входа в систему. На ОЗ должно быть установлено ограничение на количество попыток входа в систему, параметр порогового значения блокировки учетной записи должен быть задан больше, чем введенное, пользователем, значение.

8. УПД.7 – предупреждение пользователя при его доступе к информационным ресурсам. Для проверки данной меры необходимо наличие параметров оповещения пользователей.

Требуется добавить строковые параметры legalnoticecaption и legalnoticetext с указанием заголовка и предупреждения пользователя о том,

что в информационной системе реализованы меры защиты информации, а также о том, что при работе в информационной системе пользователем должны быть соблюдены установленные оператором правила и ограничения на работу с информацией в редакторе реестра.

9. УПД.8 – оповещение пользователя при успешном входе о предыдущем доступе к информационной (автоматизированной) системе. Для проверки данной меры необходимо наличие политики "Отображать при входе пользователя сведения о предыдущих попытках входа" в редакторе локальной групповой политики.

10. УПД.9 – ограничение числа параллельных сеансов доступа. Для проверки данной меры необходимо наличие параметров ограничения сеансов. DATAPK возвращает параметр SingleSessionPerUser. Критерий выполнимости меры – это значение данного параметра должен быть отличным от нуля.

11. УПД.10 – блокирование сеанса доступа пользователя при неактивности. Для проверки данной меры необходимо наличие политики блокирования сеанса доступа пользователя при неактивности. DATAPK возвращает параметры блокирования сеанса, который, для выполняемости меры, должен быть настроен.

12. УПД.13 – реализация защищенного удаленного доступа. Для проверки данной меры необходимо наличие параметров защиты удаленного доступа, таких как: Security Packages и SecurityProviders.

13. УПД.14 – контроль доступа из внешних информационных (автоматизированных) систем. Для проверки данной меры необходимо проверить копию сетевого трафика предприятия на наличие внешних информационных потоков. Для этого необходимо проверить легитимность данных потоков по правилам политики, полученным с межсетевого экрана.

14. АУД.1 -инвентаризация информационных ресурсов. Для выполняемости меры, на каждом ОЗ должна быть информация об установленном ПО, ОС и настроенных сервисов ОЗ.

15. АУД.2 – анализ уязвимостей и их устранение. Для проверки данной меры необходимо произвести сигнатурный анализ копии сетевого трафика и проверить на наличие ПО, подверженного критической уязвимости. DATAPK не имеет необходимого функционала для проверки данной меры.

16. АУД.3 – генерирование временных меток и (или) синхронизация системного времени. Необходимо провести анализ копии сетевого трафика на предмет наличия сообщений протокола синхронизации времени (NTP) от зафиксированных ОЗ.

17. АУД.4 – регистрация событий безопасности. Для выполняемости меры должны быть стандарты регистрации и передачи событий безопасности. Необходимо провести анализ копии сетевого трафика на предмет наличия событий типа Syslog и WinRM и настроек политики аудита безопасности в ОЗ, таких как: AuditSystemEvents, AuditLogonEvent, AuditPolicyChange, AuditAccountManage, AuditAccount.

18. АУД.5 – контроль и анализ сетевого трафика. Для проверки меры необходимо провести анализ копии сетевого трафика на наличие статусов информационных потоков сети. Должен быть контроль наличия и одобрения информационных потоков для обследуемых сегментов сети. DATAPK не имеет необходимого функционала для проверки данной меры.

19. ЗИС.2 – защита периметра информационной автоматизированной системы. Для проверки меры необходимо провести анализ копии сетевого трафика на наличие внешних информационных потоков. Необходимо проверить легитимность данных потоков по правилам политики, полученным с межсетевого экрана. DATAPK не имеет необходимого функционала для проверки данной меры.

20. ЗИС.6 – управление сетевыми потоками. Для выполняемости данной меры необходим контроль наличия и одобрения информационных потоков для обследуемых сегментов сети. Необходимо выявить не одобренные потоки.

21. ЗИС.8 – сокрытие архитектуры и конфигурации информационной (автоматизированной) системы. Необходимо получить информацию о

наличии в ОЗ межсетевого экрана. Получить структурную схему сети ОКИИ. Сравнить данные об МЭ и имеющихся на схеме.

22. ЗНИ.5 – контроль использования интерфейсов ввода (вывода) информации на машинные носители информации. Для выполняемости данной меры необходимо наличие параметров, отвечающие за ввод(вывод) информации. DATAPK возвращает параметры разрешение запуска ресурсов: floppydisk, cdrom, usb.

23. ОПО.4 – установка обновлений программного обеспечения. Необходимо выявить на каждом ОЗ установленную версию ОС и дату последнего обновления ОС.

24. АВЗ.1 – реализация антивирусной защиты. Для выполняемости данной меры необходимо наличие установленного средства антивирусной защиты (САЗ) Kaspersky Endpoint Security на ОЗ.

25. АВЗ.4 – обновление базы данных признаков вредоносных компьютерных программ. Для выполнимости меры необходимо проанализировать копию сетевого трафика ОКИИ, на наличие протокола KSC. А также проверить актуальных баз данных САЗ на ОЗ.

26. Защита беспроводных соединений. Для проверки необходимо проанализировать радиочастоты диапазона работы Wi-Fi в 3 различных географических координатах ОКИИ. После анализа необходимо вывести список устройств, являющихся точками доступа, а также карту с примерным местоположением данных точек.

Таблица с описанием критериев оценки соблюдения технических мер представлена в Приложении В.

По итогам анализа построена таблица 2, в которой отображена информация о том, какие меры ПО DATAPK имеет возможность автоматизировано проверить, по каким только возвращает необходимые данные и по каким не имеет необходимого функционала.

Таблица 2 – Возможность проверки мер с помощью ПО DATAPK

Название меры	Автоматическая проверка	Ручная проверка	Не проверяется
ИАФ.1	+	-	-
ИАФ.2	-	-	+
ИАФ.3	-	+	-
ИАФ.4	+	-	-
ИАФ.7	+	-	-
УПД.1	+	-	-
УПД.4	-	+	-
УПД.6	+	-	-
УПД.7	-	+	-
УПД.8	+	-	-
УПД.10	-	+	-
УПД.11	+	-	-
УПД.14	-	-	+
АУД.1	-	+	-
АУД.2	-	-	+
АУД.3	-	+	-
АУД.4	-	+	-
АУД.5	-	-	+
ЗИС.2	-	-	+
ЗИС.6	-	-	+
ЗНИ.5	+	-	-
ОПО.4	-	+	-
АВЗ.1	+	-	-
АВЗ.4	+	-	-

Продолжение таблицы 2

Защита беспроводных соединений	-	-	+

Необходимо подобрать решение для обнаружения уязвимостей и беспроводных точек доступа в сети.

2.3 Инструмент для обнаружения уязвимостей

Уязвимость – слабый компонент информационной системы (ИС) какой-либо организации. Под анализом уязвимостей понимаются процессы, направленные на поиск любых угроз, уязвимых точек и рисков потенциального несанкционированного проникновения злоумышленников в информационной системе.

Ниже перечислены наиболее распространенные промышленные уязвимости:

– Устаревшие системы;

– Отсутствие сегментации;

– Слабый контроль доступа;

– Программное обеспечение без исправлений;

– Отсутствие шифрования.

Наличие уязвимостей в информационных системах, узлах инфраструктуры или элементах комплекса защиты информации является большой проблемой для подразделений ИБ [21].

В ПО DATAPK отсутствует функционал обнаружения уязвимостей, поэтому необходимо найти готовое бесплатное решение.

Сканер уязвимостей – это программное или аппаратное решение, позволяющее проводить диагностику и мониторинг ИС в настоящем времени с целью оценки безопасности и обнаружения брешей в защите [22].

Необходимо подобрать сканер, соответствующий следующим критериям: он должен быть бесплатным, с открытым исходным кодом, кросс платформенным и должен уметь хорошо работать с большими сетями.

Наиболее заметными на российском рынке сканеров являются следующие продукты: [21]

- MaxPatrol 8 (Positive Technologies);
- RedCheck («АЛТЭКС-СОФТ»);
- ScanOVAL (ФСТЭК России);
- XSpider;
- Сканер-ВС.

Из зарубежных сканеров уязвимостей будут рассмотрены:

- F-Secure Radar;
- Nessus Professional;
- Vulnerability Control;
- Nikto;
- OpenVAS.

1. MaxPatrol 8 – система предназначена для контроля защищенности информационных систем и их соответствия стандартам безопасности [23]. MaxPatrol 8 использует комбинацию активных и пассивных методов сканирования для обнаружения уязвимостей. Предлагает расширенные возможности настройки политик сканирования и отчетов, позволяя пользователям настраивать сканирование в соответствии со своими конкретными потребностями.

MaxPatrol 8 можно интегрировать с другими инструментами и решениями по обеспечению безопасности, такими как системы SIEM, чтобы обеспечить всестороннее представление о состоянии безопасности организации [24].

MaxPatrol является платным инструментом, поэтому данный сканер не подходит под критерии заказчика.

2. RedCheck – сканер использует комбинацию активных и пассивных методов сканирования для обнаружения уязвимостей. RedCheck известен своим удобным интерфейсом и настраиваемой отчетностью, которая позволяет пользователям легко выявлять и расставлять приоритеты уязвимостей на основе их критичности [25].

Его ключевой особенностью является работа с унифицированным SCAP-контентом [26]. По сравнению с другими сканерами RedCheck поддерживает широкий спектр операционных систем, устройств и приложений и может быть настроен в соответствии с потребностями различных организаций. Возможности создания отчетов RedCheck также легко настраиваются, что позволяет пользователям создавать отчеты, отвечающие их конкретным требованиям.

RedCheck является коммерческим продуктом, не имеющий открытый исходный код.

3. ScanOVAL – это бесплатный сканер уязвимостей с открытым исходным кодом, который использует стандарт OVAL (Open Vulnerability and Assessment Language) для выявления уязвимостей на сетевых устройствах [27]. ScanOVAL в первую очередь является активным сканером, что означает, что он активно отправляет запросы на устройства для выявления уязвимостей. Может быть интегрирован с другими инструментами, такими как системы SIEM [28].

Минусом ScanOVAL является то, что он ограничен использованием формата OVAL (Open Vulnerability and Assessment Language) для определения уязвимости. Этот формат может быть не таким полным или актуальным, что может повлиять на точность сканирования ScanOVAL.

4. XSpider – предназначен для компаний с количеством узлов до 10 000. Он позволяет сканировать сеть на наличие уязвимостей, проводить тесты на проникновение, проверять веб-приложения сторонней и внутренней разработки на возможность внедрения SQL-кода [29].

Обладает широкими возможностями настройки, что позволяет пользователям определять собственные политики сканирования и настраивать уровни серьезности выявленных уязвимостей [30]. Он также имеет механизм сценариев, который позволяет писать свои собственные плагины для расширения функциональных возможностей сканера.

Из недостатков XSpider может не обеспечивать такой же уровень возможностей отчетности и исправления, по сравнению с другими. может быть ресурсоемким и медленным, особенно при сканировании больших сетей.

5. Сканер-ВС – система комплексного анализа защищенности, позволяющая обеспечить своевременное выявление уязвимостей в ИТ-инфраструктуре организаций любого масштаба. С помощью Сканера-ВС можно проводить тестирование на проникновение, сканирование уязвимостей, а также анализ конфигурации, организовать непрерывный контроль защищенности [31].

Из преимуществ Сканер-ВС имеет интуитивный интерфейс пользователя, в котором можно разобраться за 5 минут [37], позволяет проверять защищенность изолированных компьютерных сетей без вмешательства в имеющуюся инфраструктуру, имеет открытый API, является кроссплатформенным.

6. OpenVAS – это полнофункциональный сканер уязвимостей. Его возможности включают не аутентифицированное и аутентифицированное тестирование. Различные высокоуровневые и низкоуровневые интернет-протоколы, настройку производительности для крупномасштабного сканирования. И мощный внутренний язык программирования для реализации любого типа теста на уязвимость [32].

OpenVAS может быть ресурсоемким и медленным, особенно при сканировании больших сетей. Инструмент не кроссплатформенный, он не может обеспечивать такой же уровень поддержки для некоторых операционных систем и платформ.

7. Nmap – один из самых полезных сетевых инструментов, позволяющий составлять карты сетей, обнаруживать хосты, сканировать порты, диагностировать сетевые проблемы, обнаруживать и использовать уязвимости и многое другое [33]. Одним из главных преимуществ Nmap является его скорость и эффективность. Nmap разработан, чтобы быть быстрым и масштабируемым, что делает его идеальным для сканирования больших сетей. Кроме того, Nmap бесплатен для использования, что делает его доступным для широкого круга пользователей. Но Nmap может не обнаруживать все типы уязвимостей или эксплойтов и может не подходить для всех типов сетей или сред [34].

Из недостатков Nmap может работать медленнее других сканеров при сканировании больших сетей. Хотя он может идентифицировать открытые порты и службы, работающие на этих портах, он может не обеспечивать такой же уровень детализации потенциальных уязвимостей, по сравнению с другими решениями.

8. F-Secure Radar – находит и удаляет вредоносные объекты с вашего компьютера, используя технологию антивирусного сканирования F-Secure Lighthouse [35]. Обеспечивает всестороннюю оценку уязвимости всей сетевой инфраструктуры, включая серверы, рабочие станции и сетевые устройства. F-Secure Radar предоставляет удобную панель инструментов, которая предоставляет подробную информацию об обнаруженных уязвимостях и ранжирует их по степени серьезности [36].

Это коммерческий продукт, для которого требуется подписка, а цена может быть выше, чем у некоторых других решений на рынке. F-Secure Radar не кроссплатформенный, он не может обеспечивать такой же уровень поддержки для некоторых операционных систем и платформ.

9. Rustscan – это быстрый и легкий сканер портов, написанный на языке программирования Rust. Поддерживает IPv6, CIDR, ввод через файлы. Инструмент может сканировать 65 тыс. портов примерно за 7–8 секунд, что намного быстрее аналогов [38]. Имеет полную поддержку скриптов. Rustscan

легко настраивается, он позволяет пользователям настраивать параметры сканирования и предоставляет ряд опций для управления процессом сканирования.

Но в настоящее время сканер поддерживает только сканирование TCP и не имеет такого же уровня расширенных функций и опций, как некоторые из наиболее известных сканеров на рынке. Кроме того, Rustscan не предоставляет функций отчетности и оценки уязвимостей.

10. FlanScan – это надстройка для сканера сетевой безопасности Nmap, что делает его полнофункциональным инструментом для определения уязвимых хостов в больших сетях [39]. Он имеет простой интерфейс командной строки и может быть быстро и легко установлен на самых разных платформах. Пользователи могут настроить скорость сканирования, количество потоков, тип сканирования и многое другое [40].

Из минусов инструмент плохо работает с большими сетями, и не такой быстрый как другие сканеры.

По результатам анализа инструментов для сканирования уязвимости построена таблица сравнения (Таблица 3), где указаны плюсы и минусы инструментов. Исходя из таблицы можно сделать вывод что всем критериям удовлетворяет Сканер-ВС.

Таблица 3 – Сравнительная таблица инструментов сканирования

	Бесплатный	Сканирование больших сетей	Работа с IP адресами	Гибкость настроек	Отчеты	Кроссплатформенность	API
MaxPatrol 8	-	-	+	-	-	-	-
RedCheck	-	+	+	+	+	-	-
ScanOVAL	+	-	+	-	-	-	+
XSpider	-	-	+	-	+	+	-
Сканер-ВС	+	+	+	+	+	+	+
OpenVAS	-	+	+	+	+	-	-
Nmap	+	-	+	+	+	+	-
F-Secure Radar	+	-	+	+	-	-	-
Rustscan	+	+	+	-	+	+	-
FlanScan	+	-	+	+	+	+	+

2.4 Инструмент для обнаружения беспроводных точек

Использование беспроводных технологий дает пользователям способ свободного передвижения без потери связи, создателям сети больше возможностей для организации соединений, а также способствует появлению множества новых устройств доступа в сеть.[17]

Преимущества, которые беспроводные сети дают людям и бизнесу, огромны, однако такие сети несут с собой дополнительные угрозы информационной безопасности.[18] Ниже перечислены актуальные угрозы информации для беспроводной сети: [19]

– Перехват и нарушение целостности конфиденциальной информации, передаваемой по беспроводным сетям. Хакеры могут перехватывать беспроводные передачи и подслушивать сообщения, получая доступ к конфиденциальной информации, такой как имена пользователей, пароли и конфиденциальные данные.

– Нарушение доступности информации. Злоумышленники могут перехватывать беспроводную связь и изменять передаваемые данные, что позволяет им украсть данные или внедрить вредоносное ПО.

– Имитация точки доступа. Злоумышленники могут настроить мошеннические точки доступа, чтобы имитировать точки доступа, обманом заставляя пользователей подключаться к ним и получать доступ к их устройствам и информации.

– Атаки вредоносных программ. Злоумышленники могут внедрять вредоносные программы в беспроводные сети, которые могут быстро распространяться и заражать несколько устройств, вызывая потерю данных или простои системы.

В ПО DATAPK отсутствует функционал обнаружения беспроводных точек, поэтому необходимо найти готовое решение. Необходимо подобрать сканер, соответствующий критериям: он должен быть бесплатным, с открытым исходным кодом и кроссплатформенным.

Будут рассмотрены следующие программы для мониторинга локальной сети являющиеся самыми актуальными в 2023 году [41]:

- Network Olympus;
- Observium;
- Nagios;
- PRTG Network Monitor;
- Kismet;
- WireShark;
- NeDi;
- Zabbix;
- Total Network Monitor 2.

1. Network Olympus – предоставляет многочисленные возможности мониторинга различных параметров Windows-серверов, начиная от использования памяти и заканчивая количеством выполняемых системой процессов. Вся эта информация записывается в реальном времени и постоянно анализируется [42].

Главная особенность – конструктор сценариев, позволяющий отойти от выполнения примитивных проверок, которые не позволяют учитывать те или иные обстоятельства работы устройств.

Из недостатков сканер работает только на Windows, является платным инструментом. Network Olympus может потребовать значительных системных ресурсов, включая память и вычислительную мощность, особенно при мониторинге больших сетей с многочисленными устройствами и службами.

2. Observium – может автоматически обнаруживать сетевые устройства и службы, собирать показатели производительности и генерировать предупреждения при обнаружении проблем. Observium включает в себя веб-интерфейс, который позволяет пользователям просматривать состояние сети и показатели производительности в режиме реального времени, а также исторические данные [43]. Сканер поддерживает широкий спектр типов устройств, платформ и операционных систем.

Но сканер не имеет открытого исходного кода, а так плохо работает с большими сетями.

3. Nagios – предоставляет гибкую и настраиваемую платформу мониторинга, которая позволяет пользователям отслеживать широкий спектр систем и служб, включая серверы, приложения, сетевые устройства и протоколы [44]. Nagios – это программное обеспечение с открытым исходным кодом.

Из недостатков Nagios имеет ограниченные возможности отчетности, что может затруднить анализ и интерпретацию данных мониторинга. Также инструмент плохо работает с большими сетями.

4. PRTG Network Monitor – с его помощью можно выполнить диагностику работоспособности всей сети предприятия буквально в пару кликов мыши без необходимости устанавливать какие-либо сторонние программы [45]. Предлагает возможности облачного мониторинга, упрощающие мониторинг систем и служб, расположенных в удаленных и распределенных местах.

Инструмент не бесплатен, бесплатным является лишь пробный 30-дневный период [46]. Имеет ограниченные возможности отчетности, что может затруднить анализ и интерпретацию данных мониторинга.

5. Kismet – является программным обеспечением с открытым исходным кодом, что означает, что может быть настроено и изменено в соответствии с конкретными потребностями пользователя. Kismet доступен для нескольких платформ, включая Linux, macOS, Windows и Android, что делает его доступным для широкого круга пользователей [47].

Из минусов Kismet имеет базовый пользовательский интерфейс, который может быть менее интуитивным и удобным для пользователя, чем другие сетевые сканеры.

6. WireShark – бесплатный open-source анализатор трафика. Wireshark доступен для нескольких платформ, включая Linux, macOS и Windows, что делает его доступным для широкого круга пользователей [48]. Wireshark

может захватывать и анализировать широкий спектр сетевых протоколов, включая TCP, UDP, HTTP и SSL, что делает его мощным инструментом для устранения неполадок в сети и анализа безопасности.

Недостатком Wireshark является то, что он требует ручного вмешательства для запуска и остановки захвата пакетов и не имеет встроенных функций автоматизации для повторяющихся задач. Инструмент плохо работает с большими сетями.

7. NeDi – это полностью бесплатное ПО с открытым исходным кодом. Для работы этот программный продукт использует веб-интерфейс [49]. Nedi может автоматически генерировать карты сети и диаграммы топологии, что упрощает понимание структуры сети и зависимостей.

Инструмент не кроссплатформенный, он не может обеспечивать такой же уровень поддержки для некоторых операционных систем и платформ. Возможности Nedi по мониторингу сети в реальном времени могут быть ограничены по сравнению со специализированными инструментами мониторинга сети.

8. Zabbix – универсальное решение для сетевого мониторинга с открытым исходным кодом, которое может быть сконфигурировано под отдельные сетевые модели [50]. Zabbix можно интегрировать с другими инструментами мониторинга сети, такими как Nagios, а также со сторонними приложениями, что упрощает встраивание в существующие сетевые среды. Данное приложение позволяет одновременно управлять сотнями сетевых узлов, что делает его крайне эффективным инструментом [51].

Из недостатков, у сканера нет версии для Windows, конфигурация Zabbix может быть сложной, что может затруднить настройку и использование

9. Total Network Monitor 2 (TNM2) – доступное и действенное программное решение для сетевого мониторинга, которое имеет идеальный баланс между удобством и функционалом [52]. Однако у инструмента только пробная версия бесплатная. TNM2 предлагает гибкие параметры отчетности,

включая настраиваемые отчеты и возможность экспорта данных в различных форматах.

TNM2 может не подходить для более крупных и сложных сетевых сред, так как может возникнуть сложность в управлении и обслуживании. TNM2 в первую очередь разработан для сетей на базе Windows и может быть совместим не со всеми операционными системами.

По результатам анализа инструментов для сканирования беспроводных точек доступа построена таблица сравнения (Таблица 4), где указаны плюсы и минусы инструментов. Исходя из таблицы можно сделать вывод что всем критериям удовлетворяет Kismet.

Таблица 4 – Сравнительная таблица инструментов сканирования

	Бесплатный	Сканирование больших сетей	Гибкость настроек	Отчеты	Кроссплатформенность	API
Network Olympus	-	+	+	+	-	-
Observium	+	-	+	+	+	-
Nagios	+	-	-	-	-	+
PRTG Network Monitor	-	+	+	+	-	-
Kismet	+	+	+	+	+	+
WireShark	+	-	+	+	+	+
NeDi	+	-	-	-	-	+
Zabbix	+	+	+	+	-	+
Total Network Monitor 2	-	-	+	+	-	-

Выводы по второй главе

Подводя итог материалу второй главы, можно сделать следующие краткие обобщенные выводы.

1. «DATAPK» – программный комплекс, предназначенный для оперативного мониторинга состояния информационной безопасности и контроля состояния защищенности производственных и технологических

комплексов. ПО возвращает определенные данные для проверки выполнимости меры.

2. Были проанализированы данные, которые возвращает «DATAPK», по итогам которых было выявлено какие меры ПО DATAPK имеет возможность автоматизировано проверить, по каким только возвращает необходимые данные и по каким не имеет необходимого функционала. Для мер УПД.14, АУД.2, АУД.5, ЗИС.2, ЗИС.6 необходимо выявлять уязвимости в сети, данный функционал отсутствует у ПО DATAPK. Также нет возможности обнаружить беспроводные точки доступа.

3. Для обнаружения уязвимости в сети были проанализированы десять инструментов, пять из которых являются отечественными. Был выбран Сканер-ВС, так как он соответствует всем требованиям: бесплатный, имеет открытый исходный код, умеет сканировать большие сети, кроссплатформенный.

4. Для обнаружения беспроводных точек доступа в сети были проанализированы девять инструментов. Был выбран сканер Kismet, так как он соответствует всем требованиям: бесплатный, имеет открытый исходный код, умеет сканировать большие сети, кроссплатформенный.

3. Проектирование системы

3.1 Архитектура системы

Обоснование выбора типа приложения.

Заказчик поставил перед нами задачу: разработать автоматизированную кроссплатформенную систему для проверки информационной безопасности на соответствие техническим мерам за два с половиной месяца, обрабатывающая большой объем данных.

В связи с данными требованиями, было решено разрабатывать веб-серверное приложение.

Веб-приложение не требует установки локально, установка происходит на удаленном сервере, к которому можно получить доступ через интернет. Все обновления происходят на сервере, доставляются пользователям сразу.

Веб-приложение кроссплатформенное, одинаково хорошо будет работать на любом устройстве, будь то стационарный компьютер, ноутбук, планшет или смартфон – ведь оно практически не зависит от «железа» или операционной системы.

Веб-приложение может обрабатывать несколько запросов одновременно, что позволяет эффективно доставлять контент большому количеству пользователей. Он также предоставляет функции безопасности, такие как контроль доступа и шифрование, для защиты конфиденциальной информации.

Обоснование выбора метода интеграции.

Для сбора данных с разных систем необходимо было выбрать метод интеграции. Требовался метод, обрабатывающий большие объемы запросов, с высоким уровнем безопасности, с наименьшими затратами и времени на разработку. В связи с этим был выбран метод интеграции API.

Интеграция API считается простым и эффективным способом интеграции различных программных систем, поскольку она обеспечивает

стандартизированный способ взаимодействия этих систем друг с другом. В API используются четко определенные протоколы и форматы, такие как REST и JSON, которые широко используются разработчиками моей команды.

API поддерживает кэширование, которое может значительно повысить производительность за счет уменьшения количества запросов к серверу. Кэширование также может помочь снизить нагрузку на сервер, сделав его более эффективным.

API обеспечивают большую гибкость с точки зрения поиска и обработки данных. Метод позволяет разработчикам извлекать только необходимые данные, что делает его более быстрым и эффективным.

API-интерфейсы разрабатываются с учетом требований безопасности, предоставляя такие функции, как аутентификация и авторизация, чтобы гарантировать, что только авторизованные пользователи или системы могут получить доступ к данным и функциям, предоставляемым API. Это помогает защититься от утечек данных и других угроз безопасности.

Обоснование выбора процесса развертывания

От заказчика было требование: в конце проведения аудита необходимо возвращать систему в исходное состояние, то есть слои промежуточного хранения данных должны быть пустыми. К слоям хранения относятся все инструменты заказчика, инструменты сканирования сети и беспроводных точек. Также было требование быстрого развертывания всех необходимых инструментов и обновление системы.

В связи с этими требованиями было принято решение использовать docker контейнеризацию для развертывания системы.

Docker позволяет разворачивать и настраивать несколько контейнеров одновременно одной командой. Приложения работают только внутри контейнеров и не имеют доступа к основной операционной системе.

Управление версиями контейнеров Docker легко интегрируется с конвейерами CI/CD, обеспечивая автоматическую сборку, тестирование и развертывание различных версий контейнеров.

Docker обеспечивает изоляцию на уровне процессов, сохраняя приложения и их зависимости изолированными друг от друга и от основной системы. Эта изоляция предотвращает взаимодействие приложений друг с другом чем повышает безопасность и снижает риск конфликтов или зависимостей.

Контейнеры легко останавливаются, перезапускаются и уничтожаются, вместе с этим удаляются все данные.

Контейнеры Docker легкие и имеют минимальные накладные расходы по сравнению с традиционными виртуальными машинами. Контейнеры совместно используют ядро и ресурсы основной операционной системы, что обеспечивает эффективное использование системных ресурсов. Несколько контейнеров могут работать одновременно на одном хосте без существенного снижения производительности.

Использование контейнеров позволяет перейти с монолита на микро сервисную архитектуру. За счет этого ускоряется разработка новой функциональности, поскольку нет опасений, что изменения в одной компоненте затронут всю остальную систему.

3.2 Описание системы

Наименование информационной системы: Мобильный комплекс (МК) – автоматизированная система для проведения аудита.

Описание: веб-серверное приложение для запуска сбора данных в активном и пассивном режимах со сторонних систем, формирует промежуточный отчет с результатами о выполнимости требований по каждой технической мере с возможностью редактирования, генерирует отчет в текстовом формате docx.

Предметом разработки является система с клиент-серверной архитектурой.

Основным назначением разрабатываемой системы является автоматизация процесса проведения аудита.

Основным назначением разрабатываемого веб-приложения является настройка профилей проверки, отображение данных, собранных со сторонних систем в отчете.

Основным назначением разрабатываемого серверного приложения является обеспечения веб-приложения необходимыми функциями для работы

Цель создания автоматизированной системы для проведения аудита Мобильного комплекса – увеличение скорости проведения аудита, уменьшение трудозатрат, минимизирование ошибок.

Задачами системы являются:

– Собрать данных со сторонних систем;

– Обработать собранных данных;

– Сделать выводы о выполнении меры;

– Сформировать промежуточный отчет с выводами о выполнении мер;

– Сгенерировать итоговый отчет в читабельном виде формата docx.

Функции системы являются:

– Сбор данных со сторонних систем для проверки мер по информационной безопасности;

– Автоматическая проверка на выполнение мер по информационной безопасности;

– Формирование отчета с результатами выполнения мер по информационной безопасности.

Функции веб-приложения являются:

– Возможность заполнения информации о текущей проверке;

– Добавление профилей проверки;

– Настройка профилей проверки;

– Запуск профиля проверки;

– Загрузка и выгрузка конфигурации профилей с пк;

– Редактирование профиля проверки до запуска;

– Удаление профиля проверки;

– Остановка работы профиля проверки в пассивном режиме;

– Просмотр времени сбора данных у профиля проверки;

– Импорт правил межсетевого экрана;

– Добавление координат беспроводных точек доступа;

– Остановка сканирования точек доступа;

– Просмотр информации о точках доступа;

– Просмотр карты, отображающую точки сбора трафика, координаты точек доступа;

– Просмотр информации, собранной системой, в виде отчета;

– Редактирование собранной системой информации;

– Выгрузка отчета в формате DOC\PDF;

– Сброс всех настроек профилей проверки.

Функции серверного приложения являются:

– Интеграции с системами:

  – DATAPK Audit;

  – DATAPK САМСИБ;

  – Kismet;

  – Сканер ВС;

– Анализ данных, собранных со сторонних систем;

– Проверка на выполнение меры на каждом ОЗ;

– Формирование отчета о выполнении мер.

3.3 Функциональные требования

Мобильный комплекс должен представлять собой систему для генерации отчета о выполнении мер на основе собранных данных, которая состоит из следующих подсистем:

– Серверная часть системы (бекэнд): программное обеспечение для сбора данных и проверки на выполнение меры, база данных;

– Клиентская сторона (фронтэнд): интерфейсы.

Функциональные требования серверного приложения:

1. В ПО «Серверное приложение» (Далее – «Сервер») должна быть реализована функция обработки запросов клиентского приложения.

2. На «Сервере» должно быть реализовано хранение следующих данных:

– настройки профилей;

– собранные данные из:

– DATAPK САМСИБ;

– DATAPK Audit;

– Kismet

– Сканера ВС;

– данные для промежуточного отчета.

3. На «Сервере» должна быть реализована возможность взаимодействия с системой ПО Kismet, а именно:

– Итеративная обработка файлов с копией сетевого трафика в базу данных;

– Сбор баз данных в одну с триангуляцией;

– Обработка данных из составленной базы данных;

– Построение карты на основе обработанных данных.

4. На «Сервере» должна быть реализована возможность взаимодействия с системой ПО DATAPK, а именно:

– Авторизация в системе;

– Получение следующих данных:

– Протоколов;

– Хостов;

– Сетевых интерфейсов;

– Типов хостов;

– Сканеров;

– Домашних сетей;

– Потоков данных;

– Собранных конфигураций;

– Потоки данных dpi;

– Экспорт и импорт правил одобрения потоков;

– Получение данных из kibana.

5. На «Сервере» должна быть реализована функция сбора данных в пассивном режиме.

6. На «Сервере» должна быть реализована возможность работы со сводным отчетом, а именно:

– Формирование сводного отчета по состоянию мер с указанием рекомендаций из базы данных;

– Генерация технического отчета по результатам промежуточного отчета;

– Перерасчет значения результата проверки после редактирования промежуточного отчета;

– Автосохранение отчета, после редактирования.

7. На «Сервере» должна быть реализована функция мастера завершения проверки.

Функциональные требования к клиентскому приложению:

1. В ПО “Клиентское приложение» (Далее – «Клиент») должна быть реализована возможность предварительной настройки профилей, а именно:

– Ввод информации о предстоящей проверке;

– Импорт и экспорт настроенных профилей;

– Добавление и настройка профиля;

– Добавление нескольких профилей по одному типу;

– Добавление профиля, работающего в активном режиме;

– Добавление профиля, работающего в пассивном режиме;

– Редактирование и удаления профиля до начала запуска профиля.

2. На «Клиенте» должна быть реализована работа с профилями, а именно:

– Запуск сканирования;

– Не должно быть возможности запустить несколько профилей одновременно;

– Отображение времени с момента запуска профиля.

3. На «Клиенте» должна быть реализована возможность работы с профилем, работающим в активном режиме, а именно:

– Ввод данных для профиля, работающего в активном режиме;

– Возможность ограничить сетевое взаимодействие.

4. На «Клиенте» должна быть реализована возможность работы с профилем, работающим в пассивном режиме, а именно:

– Ввод данных для профиля;

– Добавление нескольких диапазонов подсети в профиль;

– Отображение количества собранных данных по каждой подсети профиля;

– Обновление данных, собранных по каждой подсети профиля, раз в 10 секунд;

– Остановка сбора данных по профилю;

– Отображение предупреждения о малом количестве собранных данных по профилю.

5. На «Клиенте» должна быть реализована возможность работы с профилем сканирования, а именно:

– Ввод данных для профиля сканирования.

6. На «Клиенте» должна быть реализована возможность работы с модулем поиска беспроводных точек доступа, а именно:

– Ввод данных координат;

– Отображение количества найденных точек доступа по введенной координате;

– Отображение информации по найденным точкам доступа;

– Отображение карты с найденными точками.

7. На «Клиенте» должна быть реализована возможность работы со сводным отчетом в разрезе мер, а именно:

– Отображение информации о выполнении меры на всех ОЗ;

– Редактирование значения по выполнению меры;

– Отображение пометки о том, что значение было изменено вручную;

– Отображение информации о перво начальном и конечном состоянии меры;

– Перезапись отчета, случае изменения профилей;

– Выгрузка отчета в формате PDF/DOCX.

8. На «Клиенте» должна быть реализована возможность работы со сводным отчетом в разрезе ОЗ, а именно:

– Отображение информации о выполнении меры на каждом ОЗ;

– Редактирование значения по выполнению меры;

– Отображение пометки о том, что значение было изменено вручную;

– Отображение информации о перво начальном и конечном состоянии меры;

– Сортировки по названию ОЗ;

– Фильтрации по результату выполнения мер;

– Отображение описания метода проверки каждой меры;

– Отображение описания результата проверки каждой меры.

9. На «Клиенте» должна быть реализована функция очистки данных об аудите.

3.3 Не функциональные требования

1. Требуемый доступ к серверу: RDP или SSH.

2. Серверная платформа Windows Server 2018+ или UNIX-like.

3. Веб-сервер IIS или kestrel.

4. СУБД PostgreSQL не ниже 11 версии.

5. Net 6.0 не ниже версии 6.0.

6. Устойчивость к сетевым перегрузкам.

7. ПО должно сохранять работоспособность при увеличении количества пользователей в пределах, поддерживаемых вычислительной инфраструктурой.

8. Программа должна работать с входными данными, предусмотренными техническими требованиями в соответствии с алгоритмом функционирования, выдавать сообщения об ошибках при неверно заданных исходных данных и прочих нештатных ситуациях, поддерживать диалоговый режим в рамках предоставляемых пользователю возможностей.

9. Поддерживаемые браузеры и их минимальные версии:

- Chrome – 51
- Edge – 79
- Safari – 10
- Firefox – 54
- Яндекс – 51

10. Требования к надежности. Пользователю, работающему с МК базовой версии через веб-браузер, должен быть предоставлен непрерывный доступ к веб-приложению, расположенному по определённому URL-адресу. Веб-сервис не должен непредвиденно прерывать свою работу.

11. Требования к условиям эксплуатации. Эксплуатация МК базовой версии должна проводиться в соответствии с эксплуатационной документацией производителя.

12. Требования к маркировке и упаковке. Упаковка должна обеспечивать защиту от внешних воздействий и сохранность МК базовой версии при транспортировке и хранении.

13. МК базовой версии упаковывается в коробку, размеры и конструкция которой определяются документацией.

14. Требования к транспортированию и хранению. Транспортирование и хранение МК базовой версии производится согласно ГОСТ 21552–84. Транспортирование можно осуществлять всеми видами транспорта на любое расстояние в транспортной таре разработчика МК.

Архитектура информационной системы Мобильный комплекс микро сервисная, обернутая в докер контейнеры и состоит из веб-интерфейса, из которого пользователь инициализирует сбор данных, сервиса “DATAPK”, который собирает данные из системы ПО DATAPK, сервиса “Kismet”, который собирает данные из системы Kismet, сервиса “Сканер”, который собирает данные из системы Сканер ВС, сервис “Аудитор”, который обрабатывает все полученные данные и передает при необходимости в базу данных, сервис генерации отчета проверяет выполняется мера или нет на основании критериев оценки и генерирует отчет.

Схематично работу системы можно представить следующим образом (Рисунок 4).

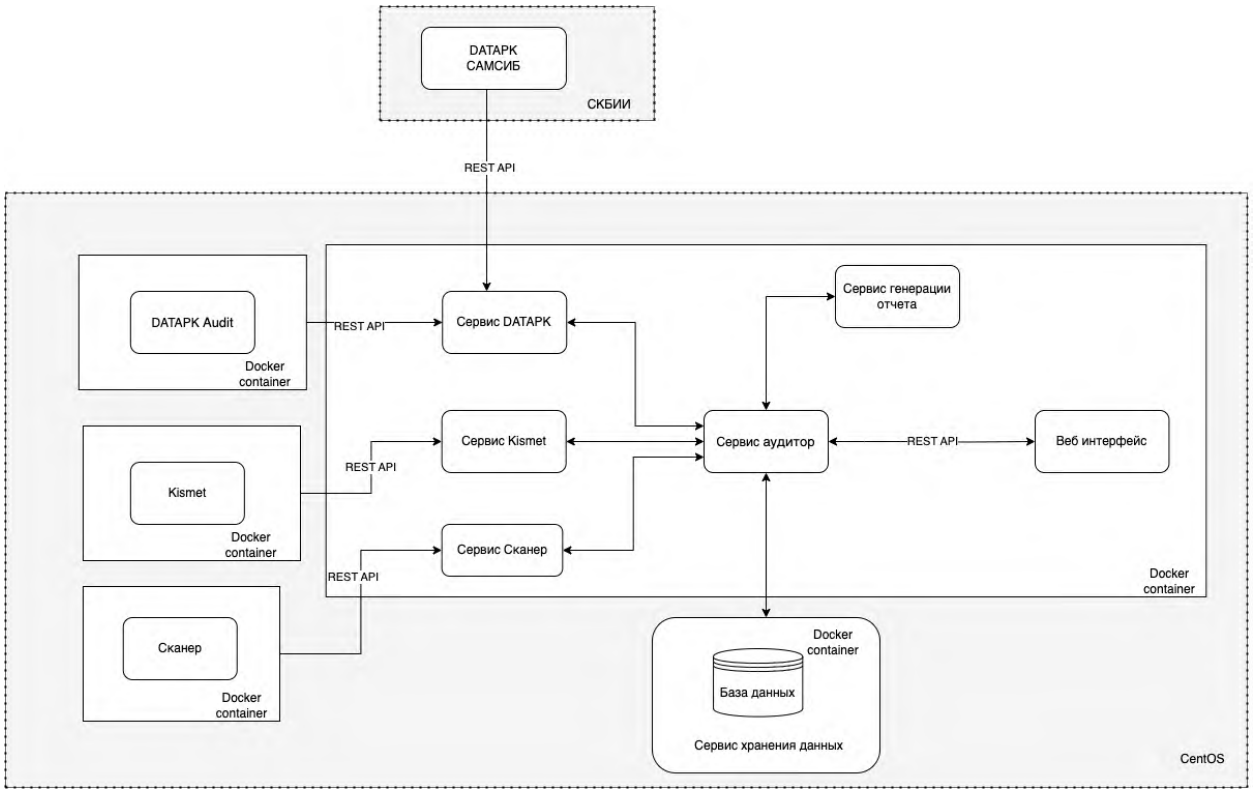

Рисунок 4 -Архитектура системы

Выводы по третьей главе

Подводя итог материалу третьей главы, можно сделать следующие краткие обобщенные выводы.

В связи с требованиями заказчика было решено разработать веб-серверное приложение, с микро сервисной архитектурой, обернутую в докер контейнеры, с интеграцией со сторонними системами посредствами метода API.

В главе описаны функциональные и не функциональные требования к системе. Полное техническое задание представлено в приложении А. Также были разработаны документы: пользовательский сценарий и шаблон технического отчета. Пользовательский сценарий описан в приложении Б. Шаблон технического отчета представлен в приложении Г.

ЗАКЛЮЧЕНИЕ

В рамках выполнения магистерской диссертации были разработаны критерии оценки соблюдения технических мер на основе данных, которые собирает инструмент ПО DATAPK, в соответствии с требованиями 187-ФЗ «О безопасности критической информационной инфраструктуры РФ».

Был проведен сравнительный анализ инструментов для сканирования сети для выявления уязвимостей и поиска беспроводных точек доступа. По результатам анализа инструментов для сканирования уязвимости был выбран Сканер-ВС, удовлетворяющий следующим условиям: он бесплатный, с открытым исходным кодом, кроссплатформенный и хорошо работает с большими сетями. Под эти же условия был выбран сканер Kismet для обнаружения беспроводных точек доступа.

Была спроектирована следующая архитектура системы с учетом требований заказчика: веб-серверное приложение, с микро сервисной архитектурой, обернутая в докер контейнеры, с интеграцией со сторонними системами посредствами метода API.

Результатом выпускной квалификационной работы стало разработанное техническое задание, сценарий использования и шаблон технического отчета. Функционал системы, следующий:

1. Сбор данных со сторонних систем для проверки мер по информационной безопасности;
2. Автоматическая проверка на выполнение мер по информационной безопасности;
3. Формирование отчета с результатами выполнения мер по информационной безопасности;
4. Возможность заполнения информации о текущей проверке;
5. Добавление профилей проверки;
6. Настройка профилей проверки;
7. Запуск профиля проверки;

8. Загрузка и выгрузка конфигурации профилей с пк;

9. Редактирование профиля проверки до запуска;

10. Удаление профиля проверки;

11. Остановка работы профиля проверки в пассивном режиме;

12. Просмотр времени сбора данных у профиля проверки;

13. Импорт правил межсетевого экрана;

14. Добавление координат беспроводных точек доступа;

15. Остановка сканирования точек доступа;

16. Просмотр информации о точках доступа;

17. Просмотр карты, отображающую точки сбора трафика, координаты точек доступа;

18. Просмотр информации, собранной системой, в виде отчета;

19. Редактирование собранной системой информации;

20. Выгрузка отчета в формате DOC\PDF;

21. Ретроспективный анализ;

22. Сброс всех настроек профилей проверки.

По техническому заданию была разработана система с использованием, которой процесс проведения аудита ускорился. Время, которое затрачивалось на одно предприятие, было от двух недель до месяца. Теперь время проведения аудита на сегменте предприятия занимает от двух до четырех часов, а на всем предприятии, в зависимости от количества сегментов, от 4 до 16 часов, то есть в среднем, два рабочих дня.

Теперь для проведения аудита есть возможность привлекать много других людей, которые знают информационную безопасность, но не умеют работать с ПО DATAPK, так как всю внутреннюю работу, анализ выполнения технических мер, система Мобильный комплекс взяла на себя. У аудитора есть возможность отредактировать результат, в случае если произошла ошибка и данные не были собраны.

Количество ошибок, связанных с человеческим фактором, свелись к минимуму, так как теперь ручная работа требуется только при возникновении ошибок сбора данных.

Теперь с помощью функционала ретроспективного анализа всегда можно автоматически сравнить два и более результата по проведению аудита за разные дни на одном предприятии и отследить динамику изменений соблюдения техническим мерам.

С помощью автоматизированной системы проведения аудита проверяются все существующие объекты защиты на выполнение техническим мерам, происходит обнаружение уязвимостей и беспроводных точек в сети, теперь можно гарантировать, что процесс оценки является всеобъемлющим и эффективным.

Результатом моей выпускной квалификационной работы стали, разработанные сценарий использования, шаблон технического отчета и техническое задание.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Безопасность объектов критической информационной инфраструктуры [Электронный ресурс] // Руслан Рахметов, Security Vision. – URL: https://www.securityvision.ru/blog/kii-chto-eto/ (дата обращения: 12.02.2023).

2. О безопасности критической информационной инфраструктуры Российской Федерации [Текст]: Федеральный закон от 26.07.2017 № 187-ФЗ // Российская газета. – 2017. – 31 июля.

3. Аудит безопасности критической инфраструктуры специальными информационными воздействиями. Монография [Электронный ресурс] // Макаренко С. И. – URL: https://sccs.intelgr.com/editors/Makarenko/makarenko-audit_ib_2018.pdf (дата обращения: 18.02.2023).

4. Астахов А. Введение в аудит информационной безопасности [Доклад] // GlobalTrust Solutions [Электронный ресурс] – URL: http://globaltrust.ru (дата обращения: 19.01.2018).

5. Аверичников В. И., Рытов М. Ю., Кувылкин А. В., Рудановский М. В. Аудит информационной безопасности органов исполнительной власти: учебное пособие. / В. И. Аверичников, М. Ю. Рытов, А. В. Кувылкин, М. В. Рудановский – Москва: Флинта, 2011. – 100 с.

6. Кульба В. В., Шелков А. Б., Гладков Ю. М., Павельев С. В. Мониторинг и аудит информационной безопасности автоматизированных систем / В. В. Кульба, А.Б. Шелков, Ю. М. Гладков, С. В. Павельев. – Москва: ИПУ им. В. А. Трапезникова РАН, 2009. – 94 с.

7. Приказ ФСТЭК № 239: правовой щит для критической инфраструктуры [Электронный ресурс] // Cyber Media. – URL: https://securitymedia.org/info/prikaz-fstek-239-pravovoy-shchit-dlya-kriticheskoy-infrastruktury.html (дата обращения: 01.03.2023).

8. ФСТЭК №31 И №239 [Электронный ресурс] // Сфера – URL: http://versiondog.ru/fstek-no31-i-no239 (дата обращения: 06.03.2023).

9. SWOT-анализ – определение и 5 шагов для профессионального SWOT-анализа [Электронный ресурс] // MoreThanDigital – URL: https://morethandigital.info/ru/swot-analiz-opredelenie-i-5-shagov-dlja-professionalnogo-swot-analiza/ (дата обращения: 10.03.2023).

10. Программно-аппаратный комплекс DATAPK – [Электронный ресурс] // Wikipedia – URL: https://ru.wikipedia.org/wiki/_DATAPK (дата обращения: 15.03.2023).

11. Решения по защите АСУ ТП [Электронный ресурс] // Комерсантъ – URL: https://www.kommersant.ru/doc/2882393 (дата обращения: 17.03.2023).

12. ФСТЭК России сертифицировала систему мониторинга защиты АСУ ТП DATAPK [Электронный ресурс] // Server news logo – URL: https://servernews.ru/952909 (дата обращения: 18.03.2023).

13. Программный комплекс оперативного мониторинга состояния информационной безопасности и контроля состояния защищенности производственно-технологических комплексов «DATAPK» – [Электронный ресурс] // РЕЕСТР ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ – URL: https://reestr.digital.gov.ru/reestr/306082/ (дата обращения: 20.03.2023).

14. Обзор DATAPK – комплекса оперативного мониторинга и контроля защищённости АСУ ТП – [Электронный ресурс] // Anti-malware – URL: https://www.anti-malware.ru/reviews/PAK-DATAPK (дата обращения: 20.03.2023).

15. Программный комплекс оперативного мониторинга состояния информационной безопасности и контроля состояния защищенности производственно-технологических комплексов «DATAPK» [Электронный ресурс] // Цифровой маркетплейс – URL: https://platforms.su/platform/5170#:~:text=DATAPK (дата обращения: 20.03.2023).

16. DATAPK [Электронный ресурс] – URL: https://www.ussc.ru/upload/files/DATAPK.pdf (дата обращения: 20.03.2023).

17. Анализ безопасности беспроводных (WI-FI) сетей [Электронный ресурс] // УЦСБ – URL: https://www.ussc.ru/news/novosti/analiz_bezopasnosti_besprovodnykh_wi_fi_setey/ (дата обращения: 25.03.2023).

18. Предложения по защите беспроводных сетей [Электронный ресурс] // CyberLeninka – URL: https://cyberleninka.ru/article/n/predlozheniya-po-zaschite-besprovodnyh-setey-peredachi-dannyh-ot-kompyuternyh-atak-napravlennyh-na-podmenu-doverennogo-polzovatelya (дата обращения: 25.03.2023).

19. Обнаружение неавторизованных беспроводных точек доступа [Электронный ресурс] // ics группа компаний – URL: https://www.icsgroup.ru/library/publications/locating_rogue_wireless_access_points/ (дата обращения: 25.03.2023).

20. Александр Астахов. Уязвимости информационной безопасности / Александр Астахов [Электронный ресурс] – URL: http://xn----7sbab7afcqes2bn.xn--p1ai/content/uyazvimosti-informacionnoy-bezopasnosti (дата обращения: 02.04.2023).

21. Сканеры уязвимостей [Электронный ресурс] // Anti-malware – URL: https://www.anti-malware.ru/analytics/Market_Analysis/Vulnerability-scanners-global-and-Russian-markets (дата обращения: 02.04.2023).

22. Сканеры уязвимостей [Электронный ресурс] // Макхост – URL: https://mchost.ru/articles/chto-takoe-skaner-uyazvimostej/ (дата обращения: 02.04.2023).

23. MaxPatrol 8 [Электронный ресурс] // CopmuWay – URL: https://www.compuway.ru/productline/security/scr/maxpatrol/ (дата обращения: 06.04.2023).

24. Обзор MaxPatrol 8 [Электронный ресурс] // Picktech – URL: https://picktech.ru/product/maxpatrol-8/ (дата обращения: 06.04.2023).

25. RedCheck [Электронный ресурс] // Алтэкс софт – URL: https://www.altx-soft.ru/catalog/redcheck/redcheck/ (дата обращения: 10.04.2023).

26. Сканер безопасности RedCheck [Электронный ресурс] // infotrust – URL:https://www.infotrust.pro/about/news/18-products/security-management/343-redcheck (дата обращения: 10.04.2023).

27. ScanOVAL [Электронный ресурс] // securitylab – URL: https://www.securitylab.ru/software/495875.php (дата обращения: 10.04.2023).

28. ScanOVAL для Linux [Электронный ресурс] // servernews – URL: https://servernews.ru/1003448 (дата обращения: 10.04.2023).

29. Сканер уязвимостей XSpider 7 [Электронный ресурс] // ixbt – URL: https://www.ixbt.com/soft/xspider7.shtml (дата обращения: 12.04.2023).

30. XSpider – профессиональный сканер уязвимостей [Электронный ресурс] // allsoft – URL: https://allsoft.ru/software/vendors/positive-technologies/positive-technologies-xspider-/ (дата обращения: 12.04.2023).

31. Сканер-ВС [Электронный ресурс] // Эшелон – URL: https://npo-echelon.ru/production/65/4291 (дата обращения: 12.04.2023).

32. Установка OpenVAS – сканер оценки уязвимостей [Электронный ресурс] // SETIWIK – URL: https://setiwik.ru/ustanovka-openvas-skaner-otsenki-uyazvimostey/ (дата обращения: 13.04.2023).

33. Nmap: Сканирование портов для обнаружения служб и уязвимостей [Электронный ресурс] // General Software – URL: https://g-soft.info/articles/8446/nmap-skanirovanie-portov-dlya-obnaruzheniya-sluzhb-i-uyazvimostey/ (дата обращения: 13.04.2023).

34. Nmap – как сканировать, как обнаружить уязвимость и как пользоваться сканером? [Электронный ресурс] // NIBBLE – URL: https://nibbl.ru/hacker/nmap-kak-skanirovat-kak-obnaruzhit-uyazvimost-i-kak-polzovatsya-skanerom.html (дата обращения: 13.04.2023).

35. Сканер F-Secure Online Scanner [Электронный ресурс] // comss – URL: https://www.comss.ru/page.php?id=1349 (дата обращения: 16.04.2023).

36. Сканер F-Secure Radar [Электронный ресурс] // securitylab – URL: https://www.securitylab.ru/software/517034.php (дата обращения: 16.04.2023).

37. Сканер-ВС [Электронный ресурс] // anti-malware – URL: https://www.anti-malware.ru/products/Scanner-VS (дата обращения: 16.04.2023).

38. Чем RustScan лучше Nmap? [Электронный ресурс] // spy-soft.net – URL: https://spy-soft.net/install-and-use-rustscan-kali-linux/ (дата обращения: 16.04.2023).

39. Flan Scan [Электронный ресурс] // $ information Security Squad - URL: https://itsecforu.ru/2021/03/25/%F0%9F%96%A7flan-scan (дата обращения: 17.04.2023).

40. Flan Scan, сканер уязвимостей [Электронный ресурс] // Убунлог – URL: https://ubunlog.com/ru/flan-scan-el-escaner-de-vulnerabilidades-de-cloudflare/ (дата обращения: 17.04.2023).

41. Топ 10 лучших программ для мониторинга сети в 2023 [Электронный ресурс] // SoftinventiveLab – URL: https://www.softinventive.ru/best-network-monitoring-tools (дата обращения: 20.04.2023).

42. Network Olympus [Электронный ресурс] // allsoft – URL: https://allsoft.ru/software/vendors/softinventive-lab/network-olympus/ (дата обращения: 20.04.2023).

43. Observium [Электронный ресурс] // observium – URL: https://www.observium.org/ (дата обращения: 25.04.2023).

44. Безопасность систем мониторинга: Nagios [Электронный ресурс] // Хабр – URL: https://habr.com/ru/companies/dsec/articles/346966/ (дата обращения: 25.04.2023).

45. PRTG Network Monitor [Электронный ресурс] // wlan-soft.com – URL: https://wlan-soft.com/25-prtg.html (дата обращения: 27.04.2023).

46. PRTG Network Monitor [Электронный ресурс] // Paessler – The Monitoring Experts – URL: https://www.paessler.com/ru/ip_monitoring (дата обращения: 27.04.2023).

47. Kismet [Электронный ресурс] // Инструменты Kali Linux – URL: https://kali.tools/?p=1118 (дата обращения: 27.04.2023).

48. Руководство и шпаргалка по Wireshark [Электронный ресурс] // Хабр – URL: https://habr.com/ru/articles/436226/ (дата обращения: 30.04.2023).

49. NeDi сканер [Электронный ресурс] // NeDi – URL: https://www.nedi.ch/ (дата обращения: 30.04.2023).

50. Zabbix как сканер безопасности [Электронный ресурс] // Хабр – URL: https://habr.com/ru/companies/vulners/articles/416137/ (дата обращения: 02.05.2023).

51. Zabbix [Электронный ресурс] // pvsm – URL: https://www.pvsm.ru/informatsionnaya-bezopasnost/285000 (дата обращения: 02.05.2023).

52. Total Network Monitor 2 [Электронный ресурс] // SoftinventiveLab – URL: https://www.softinventive.ru/total-network-monitor (дата обращения: 10.05.2023).

53. Алферьева Т. И., Васина В. Н., Шадрин Д.Б. Оформление курсовых и дипломных проектов [Текст]: методические указания для студентов технических специальностей / составители Т.И. Алферьева, В.Н. Васина, Д.Б. Шадрин – Екатеринбург: ГОУ ВПО «УрФУ-УПИ», 2019. -78 с.

ПРИЛОЖЕНИЕ А

Техническое задание

А 1. Общие требования

Предметом разработки является система с клиент-серверной архитектурой

Основным назначением разрабатываемой системы является автоматизация процесса проведения аудита.

Основным назначением разрабатываемого веб-приложения является настройка профилей проверки, отображение данных, собранных со сторонних систем в отчете.

Основным назначением разрабатываемого серверного приложения является обеспечения веб-приложения необходимыми функциями для работы

А 2. Назначение разработки

Модернизация МК осуществляется с целью автоматизации проводимых Службой проверок выполнения предприятия, являющихся субъектами КИИ, требований, установленных следующими нормативными правовыми актами Российской Федерации, а также локальными нормативными актами:

– Федеральный закон Российской Федерации от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (далее – ФЗ №187);

– Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (далее – Приказ ФСТЭК №239);

– Методические рекомендации по подготовке и сопровождению мероприятий по государственному контролю в области обеспечения

безопасности значимых объектов критической информационной инфраструктуры;

– Временные рекомендации по проведению проверок соблюдения требований безопасности значимых объектов критической информационной инфраструктуры.

А 3. Функции системы

Функции системы являются:

– Сбор данных со сторонних систем для проверки мер по информационной безопасности;

– Автоматическая проверка на выполнение мер по информационной безопасности;

– Формирование отчета с результатами выполнения мер по информационной безопасности.

А 4. Функции веб-приложения

Функции веб-приложения являются:

– Возможность заполнения информации о текущей проверке;

– Добавление профилей проверки;

– Настройка профилей проверки;

– Запуск профиля проверки;

– Загрузка и выгрузка конфигурации профилей с пк;

– Редактирование профиля проверки до запуска;

– Удаление профиля проверки;

– Остановка работы профиля проверки в пассивном режиме;

– Просмотр времени сбора данных у профиля проверки;

Техническое задание

– Импорт правил межсетевого экрана;

– Добавление координат беспроводных точек доступа;

– Остановка сканирования точек доступа;

– Просмотр информации о точках доступа;

– Просмотр карты, отображающую точки сбора трафика, координаты точек доступа;

– Просмотр информации, собранной системой, в виде отчета;

– Редактирование собранной системой информации;

– Выгрузка отчета в формате DOC\PDF;

– Сброс всех настроек профилей проверки.

А 5. Функции серверного приложения

Функции серверного приложения являются:

– Интеграции с системами:

  – DATAPK Audit;

  – DATAPK САМСИБ;

  – Kismet;

  – Сканер ВС;

– Анализ данных, собранных со сторонних систем;

– Проверка на выполнение меры на каждом ОЗ;

– Формирование отчета о выполнении мер.

А 6. Функциональные требования

Функциональные требования серверного приложения:

Продолжение ПРИЛОЖЕНИЯ А

Техническое задание

1. В ПО «Серверное приложение» (Далее – «Сервер») должна быть реализована функция обработки запросов клиентского приложения.

2. На «Сервере» должно быть реализовано хранение следующих данных:

- настройки профилей;
- собранные данные из:
- DATAPK САМСИБ;
- DATAPK Audit;
- Kismet
- Сканера-ВС;
- данные для промежуточного отчета.

3. На «Сервере» должна быть реализована возможность взаимодействия с системой ПО Kismet, а именно:

- итеративная обработка файлов с копией сетевого трафика в базу данных;
- сбор баз данных в одну с триангуляцией;
- обработка данных из составленной базы данных;
- построение карты на основе обработанных данных.

4. На «Сервере» должна быть реализована возможность взаимодействия с системой ПО DATAPK, а именно:

- авторизация в системе;
- получение следующих данных:
- протоколов;
- хостов;
- сетевых интерфейсов;
- типов хостов;
- сканеров;

– домашних сетей;

– потоков данных;

– собранных конфигураций;

– потоки данных dpi;

– экспорт и импорт правил одобрения потоков;

– получение данных из kibana.

5. На «Сервере» должна быть реализована функция сбора данных в пассивном режиме.

6. На «Сервере» должна быть реализована возможность работы со сводным отчетом, а именно:

– формирование сводного отчета по состоянию мер с указанием рекомендаций из базы данных;

– генерация технического отчета по результатам промежуточного отчета;

– перерасчет значения результата проверки после редактирования промежуточного отчета;

– автосохранение отчета, после редактирования.

7. На «Сервере» должна быть реализована функция мастера завершения проверки.

Функциональные требования к клиентскому приложению:

10. В ПО “Клиентское приложение» (Далее – «Клиент») должна быть реализована возможность предварительной настройки профилей, а именно:

– Ввод информации о предстоящей проверке;

– Импорт и экспорт настроенных профилей;

– Добавление и настройка профиля;

– Добавление нескольких профилей по одному типу;

– Добавление профиля, работающего в активном режиме;

– Добавление профиля, работающего в пассивном режиме;

– Редактирование и удаления профиля до начала запуска профиля.

11. На «Клиенте» должна быть реализована работа с профилями, а именно:

– Запуск сканирования;

– Не должно быть возможности запустить несколько профилей одновременно;

– Отображение времени с момента запуска профиля.

12. На «Клиенте» должна быть реализована возможность работы с профилем, работающим в активном режиме, а именно:

– Ввод данных для профиля, работающего в активном режиме;

– Возможность ограничить сетевое взаимодействие.

13. На «Клиенте» должна быть реализована возможность работы с профилем, работающим в пассивном режиме, а именно:

– Ввод данных для профиля;

– Добавление нескольких диапазонов подсети в профиль;

– Отображение количества собранных данных по каждой подсети профиля;

– Обновление данных, собранных по каждой подсети профиля, раз в 10 секунд;

– Остановка сбора данных по профилю;

– Отображение предупреждения о малом количестве собранных данных по профилю.

14. На «Клиенте» должна быть реализована возможность работы с профилем сканирования, а именно:

– Ввод данных для профиля сканирования.

Техническое задание

15. На «Клиенте» должна быть реализована возможность работы с модулем поиска беспроводных точек доступа, а именно:

– Ввод данных координат;

– Отображение количества найденных точек доступа по введенной координате;

– Отображение информации по найденным точкам доступа;

– Отображение карты с найденными точками.

16. На «Клиенте» должна быть реализована возможность работы со сводным отчетом в разрезе мер, а именно:

– Отображение информации о выполнении меры на всех ОЗ;

– Редактирование значения по выполнению меры;

– Отображение пометки о том, что значение было изменено вручную;

– Отображение информации о перво начальном и конечном состоянии меры;

– Перезапись отчета, случае изменения профилей;

– Выгрузка отчета в формате PDF/DOCX.

17. На «Клиенте» должна быть реализована возможность работы со сводным отчетом в разрезе ОЗ, а именно:

– Отображение информации о выполнении меры на каждом ОЗ;

– Редактирование значения по выполнению меры;

– Отображение пометки о том, что значение было изменено вручную;

– Отображение информации о перво начальном и конечном состоянии меры;

– Сортировки по названию ОЗ;

– Фильтрации по результату выполнения мер;

– Отображение описания метода проверки каждой меры;

– Отображение описания результата проверки каждой меры.

18. На «Клиенте» должна быть реализована функция очистки данных об аудите.

А 7. Взаимодействие с сервисами

А 7.1. Взаимодействие с DATAPK

Запрашиваемые данные представлены в таблице А.1

Таблица А.1 – Запрашиваемые данные с DATAPK

Требуемые данные	**Функция API**
Идентификаторы ОЗ сети	{base_url}/api/v1/api/hosts
Информация по выполнению меры ИАФ.1 проверяемого ОЗ	{base_url}/api/v1/host_data_collector/collected_configs?host_ids=<идентификаторы проверяемых ОЗ>&last_only=true&search_text=ИАФ.1
Сетевые интерфейсы сети	{base_url}/api/v1/api/host_interfaces
Идентификаторы сканеров для меры УПД.4	{base_url}/api/v1/host_data_collector/scanners?name_search=Список пользователей и их группы
Список пользователей и их групп с заданного ОЗ	{base_url}/api/v1/host_data_collector/collected_configs?host_idss=<...>&scanner_ids=<...>
id проверок	{base_url}/api/v1/host_data_collector/oval/assessments?host_ids=<...>&search=Приказ ФСТЭК 239
Информация по выполнению меры УПД.6 проверяемого ОЗ	{base_url}/api/v1/host_data_collector/oval/assessments/<.id проверки.>/summary?title_search_term=УПД.6 Ограничение неуспешных попыток
Информация по выполнению меры УПД.10 проверяемого ОЗ	{base_url}/api/v1/host_data_collector/oval/assessments/<.id..>/summary?title_search_term=УПД.10
id сканеров “Установленное ПО”	{base_url}/api/v1/host_data_collector/collected_configs?host_ids=<...>&last_only=true&scanner_id=<...>"

Техническое задание

Отправляемые данные представлены в таблице А.2

Таблица А.2 – Отправляемые данные в DATAPK

Название данных	Ответ
Диапазоны домашних подсетей	Статус запроса: • 200 • 201 • 500 • 400 • 401
IP-адрес МК	Статус запроса: • 200 • 201 • 500 • 400 • 401
IP-адрес Datapk ОКИИ	Статус запроса: • 200 • 201 • 500 • 400 • 401
Логин и пароль Datapk ОКИИ	Статус запроса: • 200 • 201 • 500 • 400 • 401
IP-адрес и MAC-адрес межсетевого экрана	Статус запроса: • 200 • 201 • 500 • 400 • 401

А 7.2. Взаимодействие с Kismet

Запрашиваемые данные:

1. Информация о найденных точках:
   - Название сети;
   - MAC адрес;

– Encrypt;

– Канал;

– Manufacture;

– Тип устройства;

– Частота работы устройства;

– Набор стандартов связи;

– Общее количество пакетов;

– Bssid.

2. Карта с расположением точек.

Отправляемые данные представлены в таблице А.3

Таблица А.3 – Отправляемые данные в Kismet

Название данных	Ответ
Координаты точек	Статус запроса: • 200 • 201 • 500 • 400

А 7.3. Взаимодействие со сканером Сканер-ВС

Запрашиваемые данные:

1. Информация о найденных уязвимостей:

– Название ОЗ;

– IP адрес ОЗ.

– Мас адрес ОЗ.

– Название уязвимости;

– Уровень критичности уязвимости:

– Высокий;

– Средний;

– Низкий.

Отправляемые данные представлены в таблице А.4

Таблица А.4 – Отправляемые данные в Сканер-ВС

Название данных	Ответ
Диапазоны подсетей	Статус запроса: • 200 • 500 • 400

А 8. Требования к режиму работы

МК базовой версии должен работать в следующих режимах:

1. Пассивный режим работы для сбора копии трафика сети Объектов КИИ без активного взаимодействия с компонентами Объектов КИИ, подключение МК базовой версии должно осуществляться к SPAN-порту коммутатора Объектов КИИ;

2. Режим подключения к Datapk Объекта КИИ (САМСИБ), подключение МК базовой версии должно осуществляться к порту передачи данных коммутатора САМСИБ, либо напрямую в Datapk Объекта КИИ.

3. Активный режим работы для сканирования защищенности Объектов КИИ в реальном времени, подключение МК базовой версии должно осуществляться к порту передачи данных коммутатора Объектов КИИ.

А 9. Требования к составу и параметрам технических и программных средств

А 9.1. Требования к техническим средствам

В состав МК базовой версии должны входить следующие технические средства:

Продолжение ПРИЛОЖЕНИЯ А

Техническое задание

1. Ноутбук;

2. Ответвитель данных ЛВС с однонаправленным шлюзом передачи данных ОД ОШПД «СПРУТ100» (ТАР);

3. Съемный носитель информации.

Характеристики ноутбука МК базовой версии должны быть не ниже параметров, представленных в таблице А.5

Таблица А.5 – Характеристики ноутбука МК базовой версии

Процессор	Уровень производительности	i5
	Частота	2.4 ГГц
	Количество ядер	4
Оперативная память	Объем	16ГБ
	Тип	DDR4
	Частота	3200 МГц
Накопитель	Объем	512 ГБ
	Тип	SSD
Ethernet модуль	Поддерживаемая скорость	До 1 Гбит/с
Wi-Fi модуль	Поддержка стандартов	802.11 a/b/g/n/ac
	Поддержка режима RFMON	есть

Съемный носитель информации должен хранить копии трафика и истории проверок в течение нескольких проверок подряд (рекомендуемый параметр – не более 10 Объектов КИИ).

Характеристики съемного носителя информации должны быть не ниже параметров, представленных в таблице А.6.

Таблица А.6 – Характеристики съемного носителя информации

Объем	2 ТБ
Тип	HDD
Форм-фактор	2,5"
Интерфейс подключения	USB 3.0
Защита от внешнего воздействия	Защита от ударов Резиновый/силиконовый корпус

Техническое задание

А 9.2. Требования к программному обеспечению

На ноутбуке должны быть установлены следующие компоненты:

1. РЕД ОС;
2. CL DATAPK Audit;
3. Программное обеспечение (ПО) Docker;
4. Docker-compose;
5. Средство сканирования защищенности;
6. ПО для просмотра таблиц;
7. Компонент формирования отчета проведенной проверки;
8. ПО для обнаружения беспроводных точек доступа;
9. Веб-приложение;
10. Браузеры: Google Chrome версии 88 и выше / Mozilla Firefox версии 84 и выше.

А 9.3. Требования к информационной и программной совместимости

МК базовой версии должен предусматривать следующие компоненты, обеспечивающие информационную и программную совместимость:

1. API для взаимодействия веб-приложения с CL DATAPK Audit;
2. Модуль для загрузки данных со сканера защищенности;
3. Модуль для загрузки данных с САМСИБ;
4. Модуль для загрузки данных с ПО для обнаружения беспроводных точек доступа;
5. Протокол HTTPS для взаимодействия с веб-сервисом.

Формат данных для загрузки в МК базовой версии должен быть уточнен на этапе технорабочего проекта.

А 9.4. Требования к надежности

Пользователю, работающему с МК базовой версии через веб-браузер, должен быть предоставлен непрерывный доступ к веб-приложению, расположенному по определённому URL-адресу. Веб-сервис не должен непредвиденно прерывать свою работу.

А 9.5. Требования к условиям эксплуатации

Эксплуатация МК базовой версии должна проводиться в соответствии с эксплуатационной документацией производителя.

А 9.6. Требования к маркировке и упаковке

Упаковка должна обеспечивать защиту от внешних воздействий и сохранность МК базовой версии при транспортировке и хранении.

МК базовой версии упаковывается в коробку, размеры и конструкция которой определяются документацией.

А 9.7. Требования к транспортированию и хранению

Транспортирование и хранение МК базовой версии производится согласно ГОСТ 21552–84.

Транспортирование можно осуществлять всеми видами транспорта на любое расстояние в транспортной таре разработчика МК.

ПРИЛОЖЕНИЕ Б

Сценарий использования

Б 1. Общие положения

Данный документ содержит описание пользовательского сценария работы веб-приложения в рамках проекта «Мобильный комплекс оперативного мониторинга обеспечения безопасности ОКИИ» базовой версии.

Б 2. Установочная настройка

Перед запуском веб-приложения пользователь соединяет патч-кордом ноутбук мобильного комплекса (далее – МК) и SPAN/RSPAN порт коммутатора, а также аутентифицируется под своей учетной записью, происходит автозапуск браузера со стартовой страницей веб-приложения.

Во время загрузки поднимаются все контейнеры и зависимости, необходимые для работы приложения.

Далее пользователь вводит краткую информацию о текущей проверке:

- Наименование ОКИИ;
- Дата проверки;
- ФИО проверяющего.

Открывается мастер первоначальной настройки. Пользователь выбирает профиль проверки для настройки.

Профиль проверки в пассивном режиме CL Datapk Audit состоит из:

- Диапазоны домашних подсетей.

Профиль проверки в режиме подключения CL Datapk Audit к Datapk ОКИИ состоит из:

- Диапазоны домашних подсетей;
- IP-адрес МК;

Сценарий использования

– IP-адрес Datapk ОКИИ;

– Логин пароль Datapk ОКИИ;

– Галочка «Ограничить сетевое взаимодействие».

Профиль проверки сканера (в случае нескольких сегментов необходимо настроить IP-адрес для нового сегмента) состоит из:

– Диапазоны домашних подсетей;

– IP-адрес МК.

Профиль проверки беспроводных точек доступа состоит из:

– Координаты точки сбора трафика.

После ввода всех необходимых данных в профиле проверки пользователь нажимает на кнопку «Сохранить», выводится короткое (по времени) уведомление «Профили настроены».

Пользователь выбирает из выпадающего списка необходимый профиль и нажимает «Загрузить профиль», выходит уведомление «Мобильный комплекс настроен и готов к работе».

Б 3. Работа с профилями

Б 3.1 Работа с CL Datapk Audit

CL Datapk Audit работает в пассивном режиме с момента подключения в SPAN – порт, получает копию трафика сети ОКИИ, в процессе выводится надпись «Осуществляется сбор трафика» и отображение в счетчике кол-ва пакетов/кол-ва созданных потоков/кол-ва ОЗ(объект защиты).

Пользователь останавливает сбор копии трафика после 1ч. (в идеальном случае – через сутки) выполнения проверки, на экран выдается сообщение «Сбор копии трафика завершен».

Сценарий использования

Осуществляется выход в главное меню, где пользователь снова выбирает профиль проверки и нажимает «Загрузить профиль». Процесс повторяется для всех диапазонов домашней сети. Предварительно пользователь меняет подключение МК к SPAN-порту следующей сети.

Б 3.2 Работа с CL Datapk Audit

Пользователь выбирает требуемый профиль проверки и нажимает «Загрузить профиль». Запускает CL Datapk Audit в активном режиме для подключения к Datapk ОКИИ. Для этого он переключает патч-корд в активный порт коммутатора ОКИИ, и запускает сбор данных. В процессе выводится надпись «Осуществляется сбор данных». Когда все данные будут получены, появляется уведомление «Данные получены» либо «Ошибка».

Б 3.3 Работа со сканером Сканер-ВС

Для работы со сканером пользователь выбирает требуемый профиль проверки и нажимает «Загрузить профиль», переключает патч-корд в активный порт коммутатора ОКИИ, запускает сканирование. Выводится сообщение «Сканирование запущено». По окончанию сканирования появляется уведомление «Сканирование завершено».

Б 3.4 Работа со сканером Kismet

Для работы с модулем пользователь запускает его, вводит координаты точки сбора трафика в соответствующее поле, нажимает «Запустить сканирование», получает информацию о точках доступа в этой координате. Пользователь нажимает «Выключить сканер», меняет местоположение и

нажимает кнопку добавления новой точки снова вводит координаты в поле, нажимает «Запустить сканирование» – повторяет для требуемого количества точек сбора трафика. Нажимает «Сформировать карту».

Б 4. Технический отчет

При нажатии пользователем на кнопку «Сгенерировать технический отчет» технический отчет составляется автоматически из данных, полученных в разделе 3 и включает в себя оценку реализации меры (выполняется/выполняется частично/не выполняется). Правила обработки данных по принятию решения реализации той или иной меры приведены в Приложении В «Правила обработки МК». Шаблон технического отчета приведен в Приложении Г «Технический отчет».

После того, как отчет сгенерирован пользователю выводится уведомление, предлагающее проверить и утвердить технический отчет. На данном этапе имеется возможность изменить оценку реализации меры (выполняется/выполняется частично/не выполняется).

После того, как отчет утвержден пользователь может загрузить отчет в двух форматах (DOC/PDF) по кнопке «Экспорт технического отчета».

Б 5. Модуль ретроспективного анализа проверок

При необходимости сравнить полученный технический отчет с отчетом по предыдущей проверке пользователь нажимает кнопку «Загрузить технический отчет», выбирает интересующей его отчет проверки и нажимает «Запустить ретроспективный анализ», по итогу выводится сравнительный отчет по изменениям в реализации требований безопасности ОКИИ.

ПРИЛОЖЕНИЕ В

Критерий оценки соблюдения мер

Мера	Метод проверки	Критерий выполнения	Критерий невыполнения
ИАФ.1	Проверка отсутствия возможности беспарольного входа на конечных ОЗ.	Параметр DefaultPassword отсутствует	Параметр DefaultPassword присутствует
ИАФ.2	Автоматизированное получение информации об ОЗиз копии сетевого трафика.	Все найденные ОЗотражены и в DATAPK ОКИИ.	Существует хотя бы одно устройство, найденное в Audit, которого нет в Самсибе.
ИАФ.3	Проверка ОЗна установленную ОС семейства Windows, Linux	ОС установлена	ОС не установлена
ИАФ.4	Проверка конфигурации на наличие параметров аутентификации.	Все параметры настроены	Хотя бы один параметр не настроен
ИАФ.5	Проверка конфигурации на наличие параметров аутентификации.	Все параметры настроены	Хотя бы один параметр не настроен
ИАФ.7	Проверка конфигурации на наличие параметров защиты трафика аутентификации.	Все параметры настроены	Хотя бы один параметр не настроен
УПД.1	Проверка ОЗ на установленную ОС семейства Windows, Linux	ОС установлена	ОС не установлена
УПД.4	Проверка реализации модели управления доступом на конечных ОЗ.	Присутствуют различные роли/группы на конечных ОЗ.	Отсутствуют различные роли/группы на конечных ОЗ.

Продолжение ПРИЛОЖЕНИЯ В

Критерий оценки соблюдения мер

Мера	Метод проверки	Критерий выполнения	Критерий невыполнения
УПД.4	Проверка реализации модели управления доступом на конечных ОЗ.	Присутствуют различные роли/группы на конечных ОЗ.	Отсутствуют различные роли/группы на конечных ОЗ.
УПД.7	Проверка конфигурации на наличие параметров оповещения пользователей.	Все параметры настроены	Хотя бы один параметр не настроен
УПД.8	Проверка конфигурации на наличие параметров оповещения пользователей.	Все параметры настроены	Хотя бы один параметр не настроен
УПД.9	Проверка конфигурации на наличие параметров ограничения сеансов.	Все параметры настроены	Хотя бы один параметр не настроен
УПД.6	Проверка наличия политик по ограничению неуспешных попыток аутентификации в систему.	Присутствуют.	Отсутствуют.
УПД.10	Проверка конфигурации на наличие параметра блокирования сеанса при неактивности.	Присутствуют.	Отсутствуют.
УПД.11	Проверка конфигурации на наличие параметров аутентификации.	Все параметры настроены	Хотя бы один параметр не настроен
УПД.13	Проверка конфигурации на наличие параметров защиты удаленного доступа.	Все параметры настроены	Хотя бы один параметр не настроен

Продолжение ПРИЛОЖЕНИЯ В

Критерий оценки соблюдения мер

Мера	Метод проверки	Критерий выполнения	Критерий невыполнения
УПД.14	Автоматизированное получение информационных потоков из копии трафика во внешние сети	В сегменте нет внешних неодобренных информационных потоков по отношению к данному сегменту	В сегменте найден хотя бы один неодобренный поток, который является внешним по отношению к данному сегменту. В сегменте найден хотя бы один одобренный поток, который является внешним по отношению к данному сегменту и источник находится вне данного сегмента.
АУД.1	Получение информации об установленном ПО	Присутствуют данные.	Отсутствуют данные.
АУД.3	Автоматизированный анализ копии сетевого трафика на предмет наличия сообщений протокола синхронизации времени (NTP) от зафиксированных ОЗ.	В копии трафика отражено получение времени по протоколу NTP. Существует утвержденный список устройств, не поддерживающих поддержку протокола NTP, в которых время задается на этапе настройки.	В копии трафика было найдено устройство, которое не получает время по протоколу NTP, не находящееся в перечне устройств, не поддерживающих данный протокол.

Продолжение ПРИЛОЖЕНИЯ В

Критерий оценки соблюдения мер

Мера	Метод проверки	Критерий выполнения	Критерий невыполнения
АУД.4	Анализ копии сетевого трафика на предмет наличия Syslog и WinRM. Автоматизированный анализ наличия стандартов регистрации и передачи событий безопасности.	В копиях трафика между DATAPK ОКИИ и ОЗСL DATAPK Audit регистрирует потоки данных по протоколам syslog, WinRM.	В копиях трафика между DATAPK ОКИИ и ОЗСL DATAPK Audit отсутствуют потоки данных по протоколам syslog, WinRM.
АУД.5	Получение с DATAPK САМСИБ Объекта информации о статусе наблюдаемых информационных потоков.	В сегменте все потоки являются одобренными.	В сегменте существует хотя бы один неодобренный поток.
АУД.7	Автоматизированный анализ копии сетевого трафика на предмет наличия Syslog и WinRM. Автоматизированный анализ наличия стандартов регистрации и передачи событий безопасности.	В копиях траффика DATAPK ОКИИ и CL DATAPK Audit присутствуют события syslog, WinRM.	В копиях траффика DATAPK ОКИИ и CL DATAPK Audit отсутствуют события syslog, WinRM.
ЗИС.2	Получение информации о правилах МЭ, автоматизированное получение информационных потоков из копии трафика, сличение полученных потоков с предоставленными правилами МЭ.	В сегменте нет информационных потоков, не подходящих под критерии правил сегментирующего МЭ.	В сегменте найден хотя бы один поток, не подходящий под критерии правил сегментирующего МЭ.

Продолжение ПРИЛОЖЕНИЯ В

Критерий оценки соблюдения мер

Мера	Метод проверки	Критерий выполнения	Критерий невыполнения
ЗИС.6	Получение с DATAPK САМСИБ Объекта информации о статусе наблюдаемых информационных потоков.	В сегменте все потоки являются одобренными.	В сегменте существует хотя бы один неодобренный поток.
ЗИС.7	Проверка конфигурации на наличие установленного ПО.	Установлено ПО	Не установлено ПО
ЗИС.8	Получение информации о наличии в ОЗ, обнаруженных МК базовой версии, МЭ. Получение структурной схемы сети ОКИИ. Сравнение данных об МЭ, полученных МК базовой версии, и имеющихся на схеме (IP-адрес, модель).	Данные о МЭ от ЭО соответствуют данным из CL DATAPK Audit.	Данные о МЭ от ЭО не соответствуют данным из CL DATAPK Audit.
ЗНИ.5	Проверка конфигурации на наличие параметров.	Все параметры настроены	Хотя бы один параметр не настроен
ОПО.4	Автоматизированный анализ копии сетевого трафика на предмет наличия пакетов попадающих под сигнатуры уязвимых версий ПО	Все найденные уязвимости отражены в данных от ЭО и не признаны критичными.	Существует хотя бы одна уязвимость, которая не отражена в отчете об уязвимостях.

Продолжение ПРИЛОЖЕНИЯ В

Критерий оценки соблюдения мер

Мера	Метод проверки	Критерий выполнения	Критерий невыполнения
АВЗ.1	Автоматизированный анализ копии сетевого трафика на предмет наличия протокола KSC. Автоматизированный анализ наличия протоколов антивирусных систем.	От каждого АРМ и сервера зафиксирован трафик антивирусных систем.	Хотя бы от одного устройства, на котором должен быть агент антивирусной системы, не зафиксирован трафик АЗ.
АВЗ.4	Проверка конфигурации на наличие обновлений.	Базы обновлены.	Базы не актуальны.
Защита беспроводных соединений	Автоматизированный анализ радиочастот диапазона работы Wi-Fi в 3 различных географических координатах ОКИИ.	Беспроводных точек доступа не зафиксировано.	Зафиксирована хотя бы одна точка доступа.

ПРИЛОЖЕНИЕ Г

Шаблон технического отчета

Наименование ОКИИ

КС 11111

Дата проверки

06.03.2023

Группа проверки

Иванов И. И., начальник отдела

Петров П. П., зам. начальника отдела

Сидоров И. И., главный специалист

В данном отчете приведены результаты оперативного мониторинга, проведенного с помощью мобильного комплекса оперативного мониторинга (МК) на соответствие объекта критической информационной инфраструктуры (ОКИИ) требованиям, установленным следующими нормативными правовыми актами Российской Федерации:

– Федеральный закон Российской Федерации от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

– Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (далее – Приказ ФСТЭК №239).

Данный отчет проверен и утвержден

Иванов И. И., начальник отдела

Продолжение ПРИЛОЖЕНИЯ Г

Шаблон технического отчета

Г 1. Общие сведения

В рамках проведения оперативного мониторинга обеспечения безопасности проведены следующие мероприятия:

1. Автоматизированный сбор и анализ трафика сети ОКИИ.
2. Автоматизированный сбор информации с DATAPK, входящего в состав САМСИБ ОКИИ, с целью получения информации о текущем состоянии реализации мер приказа ФСТЭК № 239.
3. Сканирование сети ОКИИ и анализ защищенности.
4. Автоматизированный сбор и анализ Wi-Fi трафика ОКИИ.

Г 2. Информация о проверяемых сегментах

На проверяемом ОКИИ два сетевых сегмента:

– Сегмент сети ОКИИ с адресацией 192.*.*. */24 (далее – Сегмент 192). Полностью изолированный сегмент. Сбор копии трафика для Сегмента 192 осуществлялся в течение 1 часа. Сканирование Сегмента 192 осуществлялось в течение 1 часа

– Сегмент сети ОКИИ с адресацией 10.*.*. */26 (далее – Сегмент 10). Сегмент имеет доступ из внешний сетей через сегментирующий межсетевой экран (далее – МЭ). Сбор копии трафика для Сегмента 10 осуществлялся в течение 1,5 часа. Сканирование Сегмента 10 осуществлялось в течение 1,5 часа.

Г 3. Методы проверок и результаты

Далее приведены методы и результаты проверок в рамках оперативного мониторинга обеспечения безопасности ОКИИ.

Продолжение ПРИЛОЖЕНИЯ Г

Шаблон технического отчета

Г 3.1 ИАФ.1 «Идентификация и аутентификация пользователей и инициируемых ими процессов»

ВЫПОЛНЯЕТСЯ ЧАСТИЧНО

Метод проверки

Анализ конфигурации Объекта защиты (далее – ОЗ), полученной от DATAPK САМСИБ ОКИИ, на наличие логина пользователя и парольной политики, запрещающей вход без ввода пароля.

Критерий успешности: default password выключен или отсутствует, минимальная длина пароля больше нуля.

Результат

В Сегменте 192 зафиксировано 43 ОЗ, из них проверено автоматически 39:

- 35 ОЗ выполнены требования;
- 2 ОЗ не выполнены требования;
- На 4 ОЗ автоматическая проверка данной меры не реализуется.

Г 3.2 ИАФ.2 «Идентификация и аутентификация устройств»

ВЫПОЛНЯЕТСЯ ЧАСТИЧНО

Метод проверки

Сравнение информации об ОЗ, полученной МК из копии сетевого трафика ОКИИ с информацией об ОЗ, полученной от DATAPK САМСИБ ОКИИ.

Критерий успешности: все ОЗ, обнаруженные МК, зарегистрированы в DATAPK САМСИБ ОКИИ; в DATAPK САМСИБ ОКИИ отсутствуют неизвестные ОЗ.

Результат

В Сегменте 192 зафиксировано 43 ОЗ, из них:

– 36 ОЗ зарегистрированы в DATAPK САМСИБ ОКИИ:

– Для 36 ОЗ уникальные связки IP-MAC соответствуют связкам, зафиксированным в МК. 2 ОЗ подключены к сегменту сети при помощи 2 сетевых интерфейсов;

– Для 1 ОЗ уникальные связки IP-MAC не соответствуют связкам, зафиксированным в МК;

– 1 ОЗ является неизвестным ОЗ в DATAPK САМСИБ ОКИИ;

– 6 ОЗ не зарегистрированы в DATAPK САМСИБ ОКИИ:

– 6 ОЗ с уникальными связками IP-MAC;

– 2 ОЗ подключены к сегменту сети при помощи 2 сетевых интерфейсов.

Г 3.3 ИАФ.4 «Управление средствами аутентификации»

ВЫПОЛНЯЕТСЯ ЧАСТИЧНО

Метод проверки

Анализ конфигурации ОЗ, полученной от DATAPK САМСИБ ОКИИ, на наличие настроенных параметров парольной политики.

Критерий успешности: на всех ОЗ настроена парольная политика с указанными параметрами аутентификации – минимальная длина пароля: 6; максимальный срок действия пароля: 90 дн.; минимальный

срок действия пароля: 2 дн.; пароль должен отвечать требованиям сложности: вкл.; требовать не повторяемости паролей: 5.; хранить пароли, используя обратимое шифрование: отключен.

Результат:

В Сегменте 192 зафиксировано 43 ОЗ, из них проверено автоматически 39:

– На 33 ОЗ настроена парольная политика с указанными параметрами аутентификации;

– На 2 ОЗ настроена парольная политика, параметры аутентификации не совпадают с указанными;

– На 4 ОЗ не настроена парольная политика;

– На 4 ОЗ автоматическая проверка данной меры не реализуется.

Г 3.4 ИАФ.7 «Защита аутентификационной информации при передаче»

ВЫПОЛНЯЕТСЯ ЧАСТИЧНО

Метод проверки

Анализ конфигурации ОЗ, полученной от DATAPK САМСИБ ОКИИ, на наличие параметров защиты трафика аутентификации.

Критерий успешности: на всех ОЗ настроены параметры защиты трафика аутентификации.

Результат

В Сегменте 192 зафиксировано 43 ОЗ, из них проверено автоматически 39:

– 35 ОЗ настроены шифрование паролей при передаче и включен NTLM 2.0;

– 4 ОЗ не настроено шифрование паролей при передаче или не включен NTLM 2.0;

– На 4 ОЗ автоматическая проверка данной меры не реализуется.

Г 3.5 УПД.4 «Разделение полномочий (ролей) пользователей»

ВЫПОЛНЯЕТСЯ ЧАСТИЧНО

Метод проверки

Анализ конфигурации ОЗ, полученной от DATAPK САМСИБ ОКИИ, на наличие ролевой модели в политике управления доступом.

Критерий успешности: на ОЗ присутствуют, как минимум, две разные группы -«пользователи» и «администраторы», пользователи распределены по разным группам.

Результат

В Сегменте 192 зафиксировано 43 ОЗ, из них проверено автоматически 39:

– 35 ОЗ с разными группами, пользователи распределены по группам;

– 2 ОЗ с разными группами, пользователи не распределены по группам;

– 2 ОЗ без ролевой модели (нет групп, либо одна общая);

– На 4 ОЗ автоматическая проверка данной меры не реализуется.

Г 3.6 УПД.6 «Ограничение неуспешных попыток доступа в автоматизированную систему управления (доступа к системе)»

Шаблон технического отчета

ВЫПОЛНЯЕТСЯ ЧАСТИЧНО

Метод проверки

Анализ конфигурации ОЗ, полученной от DATAPK САМСИБ ОКИИ, на наличие политики УЗ, ограничивающей число неуспешных попыток входа в систему.

Критерий успешности: на ОЗ установлено ограничение на количество попыток входа в систему, параметр порогового значения блокировки учетной записи задан больше 3.

Результат

В Сегменте 192 зафиксировано 43 ОЗ, из них проверено автоматически 39:

– На 34 ОЗ количество попыток входа в систему ограничено, параметр порогового значения блокировки учетной записи больше 3;

– На 5 ОЗ количество попыток входа в систему не ограничено, параметр порогового значения блокировки учетной записи равен 3;

– На 4 ОЗ автоматическая проверка данной меры не реализуется.

Г 3.7 УПД.10 «Блокирование сеанса доступа пользователя при неактивности»

ВЫПОЛНЯЕТСЯ ЧАСТИЧНО

Метод проверки

Анализ конфигурации ОЗ, полученной от DATAPK САМСИБ ОКИИ, на наличие политики блокирования сеанса доступа пользователя при неактивности.

Шаблон технического отчета

Критерий успешности: на ОЗ настроено блокирование сеанса доступа пользователя при неактивности.

Результат

В Сегменте 192 зафиксировано 43 ОЗ, из них проверено автоматически 39:

– На 33 ОЗ настроено блокирование сеанса доступа пользователя при неактивности;

– На 2 ОЗ не настроено блокирование сеанса доступа пользователя при неактивности;

– На 2 ОЗ автоматическая проверка данной меры не реализуется.

Г 3.8 УПД.11 «Управление действиями пользователей до идентификации и аутентификации»

ВЫПОЛНЯЕТСЯ ЧАСТИЧНО

Метод проверки

Анализ конфигурации Объекта защиты (далее – ОЗ), полученной от DATAPK САМСИБ ОКИИ, на наличие логина пользователя и парольной политики, запрещающей вход без ввода пароля.

Критерий успешности: default password выключен или отсутствует, минимальная длина пароля больше нуля.

Результат

В Сегменте 192 зафиксировано 43 ОЗ, из них проверено автоматически 39:

– 35 ОЗ с выключенным default password и minimalPasswordLength больше нуля;

– 2 ОЗ с выключенным default password и minimalPasswordLength равным нулю;

– 2 ОЗ с включенным default password и minimalPasswordLength больше нуля;

– На 4 ОЗ автоматическая проверка данной меры не реализуется.

Г 3.9 УПД.14 «Контроль доступа из внешних информационных (автоматизированных) систем»

ВЫПОЛНЯЕТСЯ ЧАСТИЧНО

Метод проверки

Анализ информации об ОЗ, полученной МК из копии сетевого трафика ОКИИ, на наличие внешних информационных потоков. Проверка легитимности данных потоков по правилам политики, полученным с межсетевого экрана (далее – МЭ) ОКИИ.

Анализ информации, полученной при попытке активного сканирования сети ОКИИ из внешней сети, за МЭ ОКИИ.

Критерий успешности: все обнаруженные МК внешние информационные потоки являются легитимными; в отчете сканирования защищенности успешных подключений к сети ОКИИ нет, все подключения к сети ОКИИ заблокированы МЭ ОКИИ.

Результат

В Сегменте 192 зафиксировано 10 внешних информационных потоков. Из них:

– 8 потоков предусмотрены правилами политики МЭ, являются легитимными;

– 2 потока не предусмотрены правилами политики МЭ, являются нелегитимными;

– В отчете сканирования защищенности зафиксировано 5 успешных подключений.

Г 3.10 АУД.1 «Инвентаризация информационных ресурсов»

ВЫПОЛНЯЕТСЯ ЧАСТИЧНО

Метод проверки

Анализ информации об ОЗ, полученной от DATAPK САМСИБ ОКИИ, на наличие перечня установленного ПО, ОС и настроенных сервисов ОЗ.

Критерий успешности: со всех зарегистрированных в МК ОЗ получен перечень сервисов ПО и ОС.

Результат

В Сегменте 192 зафиксировано 43 ОЗ, из них проверено автоматически 37:

– По 35 ОЗ информация об установленном ПО получена;

– По 2 ОЗ информация об установленном ПО не получена;

– По 35 ОЗ информация об установленной ОС получена;

– По 2 ОЗ информация об установленной ОС не получена;

– По 35 ОЗ информация о сервисах получена;

– По 2 ОЗ информация о сервисах не получена;

– На 6 ОЗ автоматическая проверка данной меры не реализуется.

Г 3.11 АУД.2 «Анализ уязвимостей и их устранение»

Шаблон технического отчета

ВЫПОЛНЯЕТСЯ ЧАСТИЧНО

Метод проверки

Анализ информации об ОЗ, полученной МК из копии сетевого трафика ОКИИ, а также при активном сканировании сети ОКИИ, на предмет наличия уязвимости в ПО ОЗ.

Критерий успешности: на ОЗ нет ПО, подверженного критичной уязвимости.

Результат

В Сегменте 192 зафиксировано 43 ОЗ, из них проверено автоматически 39:

– На 30 ОЗ уязвимости не обнаружены;

– На 9 ОЗ обнаружено 19 уязвимостей:

– С высоким уровнем критичности 9;

– Со средним уровнем критичности 0;

– С низким уровнем критичности 10;

– На 4 ОЗ автоматическая проверка данной меры не реализуется.

Г 3.12 АУД.3 «Генерирование временных меток и (или) синхронизация системного времени»

ВЫПОЛНЯЕТСЯ ЧАСТИЧНО

Метод проверки

Анализ информации об ОЗ, полученной МК из копии сетевого трафика ОКИИ, на наличие протокола синхронизации времени (NTP).

Критерий успешности: со всех ОЗ зафиксированы сообщения NTP в трафике.

Результат

В Сегменте 192 зафиксировано 43 ОЗ, из них проверено автоматически 39:

– От 35 ОЗ сообщения NTP зафиксированы в трафике;

– От 4 ОЗ сообщения NTP не зафиксированы в трафике;

– На 4 ОЗ автоматическая проверка данной меры не реализуется.

Г 3.13 АУД.4 «Регистрация событий безопасности»

ВЫПОЛНЯЕТСЯ ЧАСТИЧНО

Метод проверки

Анализ информации об ОЗ, полученной из копии сетевого трафика ОКИИ, на наличие стандартов регистрации и передачи событий безопасности (syslog, WinRM).

Анализ информации об ОЗ, полученной от DATAPK САМСИБ ОКИИ, на наличие настроек политики аудита безопасности в ОЗ.

Критерий успешности: на ОЗ настроен аудит событий; со всех ОЗ зафиксированы сообщения syslog либо WinRM в трафике.

Результат

В Сегменте 192 зарегистрировано 43 ОЗ, из них проверено автоматически 39:

– На 35 ОЗ политика аудита событий ИБ настроена;

– На 4 ОЗ политика аудита событий ИБ не настроена;

– От 35 ОЗ зафиксированы сообщения syslog в трафике;

– От 0 ОЗ зафиксированы сообщения WinRM в трафике;

– От 4 ОЗ не зафиксированы сообщения syslog в трафике;

– От 0 ОЗ не зафиксированы сообщения WinRM в трафике;

– На 4 ОЗ автоматическая проверка данной меры не реализуется.

Г 3.14 АУД.5 «Контроль и анализ сетевого трафика»

ВЫПОЛНЯЕТСЯ ЧАСТИЧНО

Метод проверки

Анализ информации об ОЗ, полученной от DATAPK САМСИБ ОКИИ, на наличие статусов информационных потоков сети ОКИИ, а также следов контроля информационных потоков сети ОКИИ.

Критерий успешности: зафиксированные в МК информационные потоки присутствуют в DATAPK САМСИБ ОКИИ, есть контролирующее разделение потоков на одобренные/неодобренные.

Результат

В Сегменте 192 зафиксировано 43 информационных потока, из них:

– 30 потоков в DATAPK САМСИБ ОКИИ находятся в статусе «одобренный»;

– 2 потока в DATAPK САМСИБ ОКИИ находятся в статусе «неодобренный»;

– 11 потоков не зафиксированы в DATAPK САМСИБ ОКИИ.

Г 3.15 АУД.7 «Мониторинг безопасности»

ВЫПОЛНЯЕТСЯ ЧАСТИЧНО

Шаблон технического отчета

Метод проверки

Анализ информации об ОЗ, полученной из копии сетевого трафика ОКИИ, на наличие стандартов регистрации и передачи событий безопасности (syslog, WinRM).

Анализ информации об ОЗ, полученной от DATAPK САМСИБ ОКИИ, на наличие настроек политики аудита безопасности в ОЗ.

Критерий успешности: на ОЗ настроен аудит событий; со всех ОЗ зафиксированы сообщения syslog либо WinRM в трафике.

Результат

В Сегменте 192 зарегистрировано 43 ОЗ, из них проверено автоматически 39:

- На 35 ОЗ политика аудита событий ИБ настроена;
- На 4 ОЗ политика аудита событий ИБ не настроена;
- От 35 ОЗ зафиксированы сообщения syslog в трафике;
- От 0 ОЗ зафиксированы сообщения WinRM в трафике;
- От 4 ОЗ не зафиксированы сообщения syslog в трафике;
- От 0 ОЗ не зафиксированы сообщения WinRM в трафике;
- На 4 ОЗ автоматическая проверка данной меры не реализуется.

Г3.16 ЗИС.2 «Защита периметра информационной (автоматизированной) системы»

НЕ ВЫПОЛНЯЕТСЯ

Метод проверки

Анализ информации об ОЗ, полученной МК из копии сетевого трафика ОКИИ, на наличие внешних информационных потоков.

Шаблон технического отчета

Проверка легитимности данных потоков по правилам политики, полученным с межсетевого экрана (далее – МЭ) ОКИИ.

Анализ информации, полученной при попытке активного сканирования сети ОКИИ из внешней сети, за МЭ ОКИИ.

Критерий успешности: все обнаруженные МК внешние информационные потоки являются легитимными; в отчете сканирования защищенности успешных подключений к сети ОКИИ нет, все подключения к сети ОКИИ заблокированы МЭ ОКИИ.

Результат

В Сегменте 192 зафиксировано 10 внешних информационных потоков. Из них:

– 8 потоков предусмотрены правилами политики МЭ, являются легитимными;

– 2 потока не предусмотрены правилами политики МЭ, являются нелегитимными;

– В отчете сканирования защищенности зафиксировано 5 успешных подключений.

Г 3.17 ЗИС.6 «Управление сетевыми потоками»

ВЫПОЛНЯЕТСЯ ЧАСТИЧНО

Метод проверки

Анализ информации об ОЗ, полученной от DATAPK САМСИБ ОКИИ, на предмет статусов информационных потоков сети ОКИИ.

Критерий успешности: все потоки, зарегистрированные в DATAPK САМСИБ ОКИИ, являются одобренными.

Шаблон технического отчета

Результат

В Сегменте 192 зафиксировано 43 информационных потока, из них:

– 30 потоков в DATAPK САМСИБ ОКИИ находятся в статусе «одобренный»;

– 2 потока в DATAPK САМСИБ ОКИИ находятся в статусе «неодобренный».

Г3.18 ЗИС.8 «Сокрытие архитектуры и конфигурации информационной (автоматизированной) системы»

ВЫПОЛНЯЕТСЯ

Метод проверки

Сравнение данных об МЭ, полученных МК, с предоставленным IP-адресом МЭ ОКИИ.

Критерий успешности: все зарегистрированные в МК МЭ соответствуют предоставленным параметрам МЭ ОКИИ.

Результат

В МК зарегистрировано 2 МЭ:

– 1 МЭ соответствует предоставленным параметрам МЭ ОКИИ;

– 1 МЭ не соответствует предоставленным параметрам МЭ ОКИИ.

Г3.19 ОПО.4 «Установка обновлений программного обеспечения»

Шаблон технического отчета

ВЫПОЛНЯЕТСЯ ЧАСТИЧНО

Метод проверки

Анализ информации об ОЗ, полученной от DATAPK САМСИБ ОКИИ, на актуальность обновления установленной ОС.

Критерий успешности: на всех ОЗ установлена обновленная версия ОС, дата обновления ОС не более 2 месяцев.

Результат

В Сегменте 192 зафиксировано 43 ОЗ, из них проверено автоматически 39:

– На 30 ОЗ дата обновления ОС не более 2 месяцев;

– На 9 ОЗ дата обновления ОС более 2 месяцев;

– На 4 ОЗ автоматическая проверка данной меры не реализуется.

Г 3.20 АВЗ.1 «Реализация антивирусной защиты»

ВЫПОЛНЯЕТСЯ ЧАСТИЧНО

Метод проверки

Анализ информации об ОЗ, полученной от DATAPK САМСИБ ОКИИ, на наличие установленного средства антивирусной защиты (САЗ) Kaspersky Endpoint Security на ОЗ.

Критерий успешности: на ОЗ установлено САЗ.

Результат

В Сегменте 192 зафиксировано 43 ОЗ, из них проверено автоматически 39:

– На 37 ОЗ установлено САЗ;

– На 2 ОЗ не установлено САЗ;

– На 4 ОЗ автоматическая проверка данной меры не реализуется.

Г 3.21 АВЗ.4 «Обновление базы данных признаков вредоносных компьютерных программ»

ВЫПОЛНЯЕТСЯ ЧАСТИЧНО

Метод проверки

Анализ информации об ОЗ, полученной от DATAPK САМСИБ ОКИИ, на наличие актуальных баз данных САЗ на ОЗ.

Анализ информации об ОЗ, полученной из копии сетевого трафика ОКИИ, на наличие протокола KSC.

Критерий успешности: со всех ОЗ зафиксированы сообщения KSC в трафике, базы данных САЗ обновлены.

Результат

В Сегменте 192 зафиксировано 43 ОЗ, из них проверено автоматически 39:

– На 35 ОЗ базы данных САЗ обновлены менее 14 дней назад;

– На 2 ОЗ базы данных САЗ обновлены более 14 дней назад;

– С 37 ОЗ зафиксированы сообщения KSC в трафике;

– С 2 ОЗ не зафиксированы сообщения KSC в трафике.

– На 4 ОЗ автоматическая проверка данной меры не реализуется.

Г 3.21 Обнаружение беспроводных точек доступа

ОБНАРУЖЕНЫ 2 БЕСПРОВОДНЫЕ ТОЧКИ ДОСТУПА

Метод проверки

Продолжение ПРИЛОЖЕНИЯ Г

Шаблон технического отчета

Анализ радиочастот диапазона работы Wi-Fi в 3 различных географических координатах ОКИИ.

Результат

На ОКИИ зафиксированы 2 беспроводных точки доступа.

Информация об обнаруженных точках доступа:

- точка 1:
  - mac: AE:1A: 06:9D:C0:DA;
  - essid: poco;
  - encrypt: WPA2-PSK;
  - channel: 6 (2432000);
  - packets: 223;
  - manufacture: Apple, Inc.
- точка 2:
  - mac: 3E:0B: 5A:3B:77:47;
  - essid: realme C3;
  - encrypt: WPA2-PSK;
  - channel: 1 (2412000);
  - packets: 79;
  - manufacture: MediaTek Inc.

Зафиксированное расположение точек доступа приведено на рисунке 5.

Рисунок 5 – Географическое положение зафиксированных беспроводных точек доступа