**ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА**

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«Петербургский государственный университет путей сообщения**

**Императора Александра I»**

**(ФГБОУ ВО ПГУПС)**

Факультет «Автоматизация и интеллектуальные технологии»

Кафедра «Информатика и информационная безопасность»

Специальность 10.05.03 «Информационная безопасность автоматизированных систем»

Специализация «Информационная безопасность автоматизированных систем на транспорте»

**Курсовой проект**

по дисциплине

«Комплексное обеспечение информационной безопасности автоматизированных систем»

на тему: «Разработка модели комплексной системы информационной безопасности автоматизированной системы критического применения»

Форма обучения – очная

|  |  |  |
| --- | --- | --- |
| **Выполнил обучающийся**  Курс 5  Группа КИБ-012 | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  подпись, дата | Г.Е. Груздев |
|  |  |  |
| **Руководитель** | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  подпись, дата | А.А. Корниенко |

Санкт-Петербург

2024

**ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА**

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«Петербургский государственный университет путей сообщения**

**Императора Александра I»**

**(ФГБОУ ВО ПГУПС)**

Факультет «Автоматизация и интеллектуальные технологии»

Кафедра «Информатика и информационная безопасность»

Специальность 10.05.03 «Информационная безопасность автоматизированных систем»

Специализация «Информационная безопасность автоматизированных систем на транспорте»

**Оценочный лист на курсовой проект**

по дисциплине

«Информационная безопасность автоматизированных транспортных систем»

Груздев Георгий Евгеньевич

Тема: «Разработка системы обеспечения информационной безопасности (подсистемы защиты информации) автоматизированной системы (АС) или корпоративной информационной системы (КИС)»

**Оценка курсовой работы**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№**  **п/п** | **Материалы необходимые для оценки знаний, умений**  **и навыков** | **Показатель**  **оценивания** | **Шкала оценивания** | **Полученная оценка** |
| 1 | Пояснительная записка к курсовому проекту | Соответствие исходных данных выданному заданию | 0 – 5 |  |
| Проведение полного анализа поставленной проблемы | 0 – 15 |  |
| Обоснованность принятых технических, технологических, организационных решений, подтвержденная соответствующим анализом | 0 – 15 |  |
| Использование современных методов проектирования и разработки | 0 – 5 |  |
| Итого максимальное количество баллов по п. 1 | | | 0 – 40 |  |
| 2 | Разработанная подсистема защиты | Соответствие поставленной задаче | 0 – 10 |  |
| Соответствие пояснительной записке | 0 – 5 |  |
| Соответствие требованиям НД | 0 – 5 |  |
| Использование современных средств и методов защиты | 0 – 10 |  |
| Итого максимальное количество баллов по п. 2 | | | 0 – 30 |  |
| **ИТОГО максимальное количество баллов** | | | 0 – 70 |  |

Заключение: рецензируемая курсовая работа соответствует требованиям основной образовательной программы специальности 10.05.03 «Информационная безопасность автоматизированных систем» (специализация «Информационная безопасность автоматизированных систем на транспорте»).

Итоговая оценка –

Руководитель \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А. А. Корниенко «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 2024 г.

[ВВЕДЕНИЕ 5](#_Toc154401010)

[1 Характеристика АС (КИС) как объекта информационной безопасности, определение требования и анализ мер и средств защиты 6](#_Toc154401011)

[1.1 Анализ особенностей построения и функционирования WAZUH, определение защищаемых информационных ресурсов - информации и информационной инфраструктуры, классификация 6](#_Toc154401012)

[1.1.1 Определение защищаемых информационных ресурсов 8](#_Toc154401013)

[1.1.2 Классификация и категорирование 9](#_Toc154401014)

[1.2 Определение угроз информационной безопасности, оценка возможностей внешних и внутренних нарушителей и анализ возможных уязвимостей, построение модели актуальных угроз информационным ресурсам АС 11](#_Toc154401015)

[1.3 Определение требований к системе или подсистеме (мерам и средствам) защиты информации в соответствии со стандартами ФСТЭК России 14](#_Toc154401016)

[1.4 Анализ существующих мер и средств защиты АСУТ 26](#_Toc154401017)

[2 Организационные меры защиты АС 27](#_Toc154401018)

[2.1 Порядок доступа к защищаемым ресурсам и безопасного обращения с ними 27](#_Toc154401019)

[2.2 Порядок работы с конфиденциальной информацией 27](#_Toc154401020)

[2.3 Организация администрирования (службы) информационной безопасности 28](#_Toc154401021)

[2.4 Общие права и обязанности персонала 29](#_Toc154401022)

[2.5 Меры по реагированию на нарушения информационной безопасности 30](#_Toc154401023)

[2.6 Ответственность за нарушение режима безопасности 31](#_Toc154401024)

[2.7 Организационно-распорядительные документы 31](#_Toc154401025)

[3 Программно-технические меры защиты АСУ 33](#_Toc154401026)

[3.1 Принципы применения программно-технических мер защиты 33](#_Toc154401027)

[3.2 Физическая защита АС 34](#_Toc154401028)

[3.3 Предложения по применению дополнительных средств программно-аппаратной защиты информационных ресурсов 35](#_Toc154401029)

[3.4 Обобщенная архитектура системы защиты информации 37](#_Toc154401030)

[ЗАКЛЮЧЕНИЕ 38](#_Toc154401031)

[Список литературы 39](#_Toc154401032)

# ВВЕДЕНИЕ

Актуальность темы курсовой работы обусловлена тем, что для информации, обрабатываемой в любой автоматизированной системе управления, должна обеспечиваться конфиденциальность, целостность и доступность. В рассматриваемой системе обрабатывается информация разных видов, в том числе, персональные данные, данные составляющие коммерческую тайну и нарушение хотя бы одного из свойств (конфиденциальности, целостности или доступность) информации может привести к материальным и репутационным потерям.

Предметом исследования является процесс обеспечения безопасности информационных систем, поддержания конфиденциальности, целостности и доступности данных в условиях потенциальных компьютерных инцидентов. Исследуется эффективность передачи сигналов об угрозах, оперативность реакции на них, а также механизмы обеспечения конфиденциальности при передаче и обработке информации в рамках системы Wazuh.

Цель исследования заключается в разработке и совершенствовании методов, алгоритмов и технологий, обеспечивающих высокий уровень безопасности информационных ресурсов, а также оперативное и эффективное реагирование на возможные угрозы, с сохранением конфиденциальности, целостности и доступности передаваемой информации в рамках Wazuh.

Задачи курсовой работы:

1. Провести анализ архитектуры и функциональных возможностей системы управления, мониторинга и реагирования на компьютерные инциденты Wazuh.
2. Классифицировать или категорировать Wazuh в соответствии с нормативными документами, определяя их основные характеристики и функциональные аспекты.
3. Определить угрозы безопасности информации для Wazuh в соответствии с нормативными документами, выявив потенциальные уязвимости и риски.
4. Идентифицировать угрозы безопасности информации для Wazuh на основе оценки возможностей внешних и внутренних нарушителей, анализа уязвимостей системы, возможных методов атак, и последствий нарушения безопасности информации. Разработать модель актуальных угроз безопасности информации для Wazuh.
5. Определить требования к системе (мерам и средствам) защиты информации в рамках Wazuh, учитывая особенности функционирования и специфику системы.
6. Изучить и проанализировать существующие организационные и технические меры и средства защиты информации, применяемые в Wazuh, оценить их соответствие необходимому уровню защищенности и предложить возможные улучшения.

# Характеристика АС (КИС) как объекта информационной безопасности, определение требования и анализ мер и средств защиты

## Анализ особенностей построения и функционирования Wazuh, определение защищаемых информационных ресурсов - информации и информационной инфраструктуры, классификация

Система управления, мониторинга и реагирования на компьютерные инциденты (WAZUH) играет ключевую роль в информационно-управляющей структуре организации. Работа системы направлена на:

* + Оперативное реагирование на компьютерные инциденты, обеспечение контроля за обнаружением и устранением угроз в реальном времени.
  + Мониторинг и анализ безопасности информационных ресурсов с целью обеспечения конфиденциальности, целостности и доступности данных.
  + Комплексное обеспечение мер по предотвращению атак, включая контроль за соблюдением политик безопасности, обновлением программного обеспечения и обучением персонала.
  + Автоматизация процессов анализа и реагирования на инциденты, включая моментальное уведомление ответственных лиц и принятие необходимых мер по восстановлению безопасности.
  + Обеспечение взаимодействия с другими системами безопасности и мониторинга, например, системой автоматической идентификации угроз (САИУ).
  + Генерация автоматизированной отчетности по инцидентам, обзорам безопасности и эффективности мер по защите информационных ресурсов.
  + Синхронизация с автоматизированной системой управления информационной безопасностью и другими инструментами, обеспечивая единый стандарт безопасности в организации.

Цели реализуются через внедрение единой компьютерной информационно-управляющей системы на предприятиях, где в фокусе находится система управления, мониторинга и реагирования на компьютерные инциденты (Wazuh). Этот переход также включает в себя переход на безбумажную технологию работы, автоматическое формирование отчетных форм, а также автоматизированный анализ, поддержку и контроль принимаемых решений в области информационной безопасности.

Wazuh обеспечивает автоматическое выявление и оперативное устранение причин, связанных с компьютерными инцидентами, гарантируя эффективное реагирование на потенциальные угрозы и минимизацию последствий. Система включает в себя комплексы технического диагностирования, предоставляющие возможность оперативно выявлять и анализировать инциденты, а также расшифровывать информацию, поступающую из различных источников, для более точного определения характера и происхождения угроз.

Системы, взаимодействующие с Wazuh*:*

1. ПК Сбора информации об уязвимостях
2. Подсистема управления событиями ИБ
3. Система пересылки события ИБ
4. ПК Хранилище данных

Система включает в себя:

1. **Модуль обнаружения инцидентов:**
   * Отслеживание аномалий и подозрительной активности в сети.
2. **Модуль исследования инцидентов:**
   * Анализ данных о инцидентах для выявления корневых причин и масштаба инцидентов.
3. **Модуль контроля доступа:**
   * Управление доступом к данным и ресурсам в период реагирования на инциденты.
4. **Модуль контроля сетевого трафика:**
   * Мониторинг и анализ сетевого трафика для выявления необычных паттернов.
5. **Модуль управления событиями:**
   * Сбор, агрегация и управление событиями в ходе инцидентов.
6. **Модуль коммуникации и согласования:**
   * Средства коммуникации и координации действий персонала в процессе реагирования на инциденты.
7. **Модуль восстановления:**
   * Планирование и реализация мер по восстановлению после завершения инцидента.
8. **Модуль управления данными инцидентов:**
   * Система для хранения, анализа и обработки данных о прошлых инцидентах.
9. **Модуль обучения и обучаемости:**
   * Обучение персонала по процедурам реагирования и обновление знаний в соответствии с изменениями в угрозах.
10. **Модуль отчетности:**
    * Подготовка отчетов и аналитики по проведенным мероприятиям по реагированию на инциденты.

### Определение защищаемых информационных ресурсов

1. Защищаемой информацией в подсистеме управления, мониторинга и реагирования на компьютерные инциденты Wazuh являются:

* Персональные данные пользователей системы: включает в себя личные данные сотрудников, поддерживающих и обслуживающих Wazuh.

1. Системные сообщения и логи:

* Информация, представляющая служебные сообщения и данные, передаваемые между компонентами системы.

1. Данные от датчиков и мониторов:

* Сведения, получаемые от различных датчиков, используемых в рамках Wazuh для мониторинга и контроля различных параметров.

1. Рабочие отчеты и аналитика:

* Информация, создаваемая системой в процессе работы, включая отчеты, аналитическую информацию и другие документы, связанные с оперативной деятельностью.

1. Данные о пользователях системы:

* Включают в себя информацию о пользователях Wazuh, их ролях и уровнях доступа.

Защищаемой информационной инфраструктурой в Wazuh являются:

1. **Рабочие места и станции операторов:**

Компьютерные рабочие места операторов и других пользователей системы.

1. **Каналы связи и сетевое оборудование:**

Инфраструктура сетевого взаимодействия, включая коммуникационные каналы и сетевое оборудование.

1. **Программное обеспечение (ПО) на серверах и АРМах:**

Все компоненты программного обеспечения, установленные на серверах и рабочих станциях.

1. **Сервера (приложений, баз данных):**

Сервера, обеспечивающие функционирование приложений и хранение данных в рамках Wazuh.

### Классификация и категорирование

1) Классификация как АС

Согласно руководящему документу (РД) «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»:

Wazuh является многопользовательской, права доступа сотрудников к информации разграничены. Так как система многопользовательская, ей присваивается первая группа. Данная группа включает многопользовательские АС, в которых обрабатывается и хранится информация разных уровней конфиденциальности.

Wazuh является АС с классом защищенности 1Г, так как в ней обрабатывается и хранится информация разных уровней конфиденциальности. Система не обрабатывает секретную информацию (исключаются классы 1А, 1Б, 1В).

2) Классификация, как АСУТП

Согласно приказу ФСТЭК от 14 марта 2014 г «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»: класс защищенности автоматизированной системы управления (первый класс (К1), второй класс (К2), третий класс (К3)) определяется в зависимости от уровня значимости (критичности) обрабатываемой в ней информации (УЗ).

Уровень значимости информации (УЗ) определяется степенью возможного ущерба от нарушения ее целостности (неправомерные уничтожение или модифицирование), доступности (неправомерное блокирование) или конфиденциальности (неправомерные доступ, копирование, предоставление или распространение), в результате которого возможно нарушение штатного режима функционирования автоматизированной системы управления или незаконное вмешательство в процессы функционирования автоматизированной системы управления.

УЗ = [(целостность, степень ущерба) (доступность, степень ущерба) (конфиденциальность, степень ущерба)].

Нарушение свойств безопасности информации в Wazuh может повлечь нарушения штатного режима функционирования автоматизированной системы управления, возможно возникновение ЧС регионального характера. Таким образом Wazuh присваивается *второй класс защищенности*.

3) Классификация как ИСПДн

Так как в Wazuh происходит обработка персональных данных, её можно отнести к информационным системам персональных данных. Классифицировать систему необходимо в соответствии с Приказом ФСТЭК России от 18 февраля 2013 г №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Уровень защищенности для ИСПДн определяется на основе Постановления Правительства РФ от 01.11.2012 N 1119: уровень защищенности персональных данных зависит от того, угрозы какого типа (1, 2 или 3) актуальны для информационной системы. Можно предположить, что угрозы 2-го типа являются актуальными для этой информационной системы (то есть угрозы, связанные с наличием недокументированных возможностей в прикладном программном обеспечении, используемом в информационной системе). Согласно Постановлению Правительства РФ от 01.11.2012 N 1119 персональные данные, обрабатывающиеся в АСУТ, относятся *ко 2 уровню защищенности*, так как они удовлетворяют условию: для информационной системы актуальны угрозы 2-го типа, и информационная система обрабатывает специальные категории персональные данных оператора.

## Определение угроз информационной безопасности, оценка возможностей внешних и внутренних нарушителей и анализ возможных уязвимостей, построение модели актуальных угроз информационным ресурсам АС

Определим угрозы безопасности информации для Wazuh:

1. Целостности:
   1. Незащищенный канал технической поддержки;
   2. Получения информации из неавторизованного источника;
   3. Не декларированные возможности программы ПЛК;
   4. Воздействия на канал связи на аппаратном и программном уровнях;
2. Конфиденциальности
   1. Незащищенный канал технической поддержки;
   2. Отправления информации неавторизованному объекту на аппаратном уровне
   3. Воздействия на канал связи на аппаратном уровне;
   4. Отправка информации неавторизованному источнику;
3. Доступности
   1. Перегрузка канала связи;
   2. Отказ в обслуживании;
   3. Уничтожение канала связи.

Определим угрозы безопасности информации для Wazuh, как для ИСПДн:

В соответствии с базовой моделью угроз безопасности информации при их обработке в ИСПДн:

1. Утечка по техническим каналам: перехват акустической, видовой информации, через ПЭМИН.
2. Угрозы модификации информации:

* Нештатные режимы работы: риск изменения нормального функционирования системы путем преднамеренных изменений служебных данных, игнорирования ограничений и модификации самих данных.
* Внедрение вредоносных программ: возможность внедрения вредоносных программ, которые могут нарушить работу системы, а также угрожать конфиденциальности и целостности данных.
* Комбинированные угрозы: риск возникновения ситуаций, когда несколько угроз объединяются для создания более сложных и опасных сценариев атак.

В соответствии с методикой оценки угроз безопасности информации ФСТЭК актуальные нарушители разделяются на следующие группы нарушителей:

внешние нарушители – нарушители, не имеющие прав доступа в контролируемую (охраняемую) зону (территорию) и (или) полномочий по доступу к информационным ресурсам и компонентам систем и сетей, требующим авторизации;

внутренние нарушители – нарушители, имеющие права доступа в контролируемую (охраняемую) зону (территорию) и (или) полномочия по автоматизированному доступу к информационным ресурсам и компонентам систем и сетей.

Составим перечень актуальных нарушителей и их возможностей для Wazuh:

1. специальные службы иностранных государств (внутренние, внешние) – обладают высокими возможностями по реализации угроз безопасности (Н4);
2. террористические, экстремистские группировки (внешние) - обладают высокими возможностями по реализации угроз безопасности (Н4);
3. преступные группы (внешние) - средними возможностями по реализации угроз безопасности информации (Н3);
4. отдельные физические лица (хакеры; внешние, внутренние) - базовыми повышенными возможностями по реализации угроз безопасности информации (Н2);
5. конкурирующие организации (внешние) - базовыми повышенными возможностями по реализации угроз безопасности информации (Н2);
6. разработчики программных, программно-аппаратных средств (внешние) - средними возможностями по реализации угроз безопасности информации (Н3);
7. лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем (внутренние) - базовыми повышенными возможностями по реализации угроз безопасности информации (Н2);
8. поставщики услуг связи, вычислительных услуг (внешние) - базовыми возможностями по реализации угроз безопасности информации (Н1);
9. лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ (внешние) - базовыми возможностями по реализации угроз безопасности информации (Н1);
10. лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем оператора (администрация, охрана, уборщики и др.; внутренние) - базовыми возможностями по реализации угроз безопасности информации (Н1);
11. авторизованные пользователи систем и сетей (внутренние) - базовыми возможностями по реализации угроз безопасности информации (Н1);
12. системные администраторы и администраторы безопасности (внутренние) - высокими возможностями по реализации угроз безопасности информации (Н4);
13. бывшие (уволенные) работники (пользователи; внешние) - базовыми возможностями по реализации угроз безопасности информации (Н1).

Возможные уязвимости перечислены в таблице 1:

Таблица 1 – Основные уязвимости объектов АСУТ

|  |  |
| --- | --- |
| Объект | Уязвимость |
| ПО | 1. Устаревшее ПО 2. Недостаточное тестирование программных средств перед их внедрением 3. Ввод некорректных данных 4. Удаленное выполнение кода 5. Манипулирование УЗ 6. Отсутствие контроля доступа |
| АРМы, серверы | 1. Скачки напряжения 2. Заражение машины 3. Неверное конфигурирование 4. Ненадлежащее техническое содержание 5. Хранение/использование в общедоступных местах 6. Недостаточная антивирусная защита 7. Отсутствие резервного копирования |
| СПД | 1. Незащищенные каналы связи 2. Уязвимости протоколов сетевого взаимодействия 3. Незащищенный трафик |

## Определение требований к системе или подсистеме (мерам и средствам) защиты информации в соответствии со стандартами ФСТЭК России

В РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» определены следующие подсистемы защиты информации для *класса АС 1Г* и меры, осуществляемые в них:

1) Подсистема управления доступом:

* должна осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия, длиной не менее шести буквенно-цифровых символов;
* должна осуществляться идентификация терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по логическим именам;
* должна осуществляться идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;
* должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа.

2) Подсистема регистрации и учета:

должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:

* дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
* результат попытки входа: успешная или неуспешная - несанкционированная;
* идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;
* код или пароль, предъявленный при неуспешной попытке;
* должна осуществляться регистрация выдачи печатных (графических) документов на "твердую" копию. В параметрах регистрации указываются:
* дата и время выдачи (обращения к подсистеме вывода);
* спецификация устройства выдачи [логическое имя (номер) внешнего устройства];
* краткое содержание (наименование, вид, шифр, код) и уровень
* конфиденциальности документа;
* идентификатор субъекта доступа, запросившего документ;
* должна осуществляться регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов. В параметрах регистрации указываются:
* дата и время запуска;
* имя (идентификатор) программы (процесса, задания);
* идентификатор субъекта доступа, запросившего программу (процесс, задание);
* результат запуска (успешный, неуспешный - несанкционированный);
* должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам.

При этом:

1. целостность СЗИ НСД проверяется при загрузке системы по контрольным суммам компонент СЗИ;
2. целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации;
3. должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая контроль доступа в помещения АС посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АС и хранилище носителей информации, особенно в нерабочее время;
4. должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест - программ, имитирующих попытки НСД;
5. должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление, и контроль работоспособности.

Для АСУ *второго класса* защищенности в Приказе ФСТЭК от 14 марта 2014 года №31 определены меры защиты информации и их базовые наборы:

Идентификация и аутентификация (ИАФ)

|  |  |
| --- | --- |
| ИАФ.0 | Разработка политики идентификации и аутентификации |
| ИАФ.1 | Идентификация и аутентификация пользователей и инициируемых ими процессов |
| ИАФ.2 | Идентификация и аутентификация устройств |
| ИАФ.3 | Управление идентификаторами |
| ИАФ.4 | Управление средствами аутентификации |
| ИАФ.5 | Идентификация и аутентификация внешних пользователей |
| ИАФ.7 | Защита аутентификационной информации при передаче |

Управление доступом (УПД)

|  |  |
| --- | --- |
| УПД.0 | Разработка политики управления доступом |
| УПД.1 | Управление учетными записями пользователей |
| УПД.2 | Реализация политик управления доступа |
| УПД.3 | Доверенная загрузка |
| УПД.4 | Разделение полномочий (ролей) пользователей |
| УПД.5 | Назначение минимально необходимых прав и привилегий |
| УПД.6 | Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему |
| УПД.10 | Блокирование сеанса доступа пользователя при неактивности |
| УПД.11 | Управление действиями пользователей до идентификации и аутентификации |
| УПД.13 | Реализация защищенного удаленного доступа |
| УПД.14 | Контроль доступа из внешних информационных (автоматизированных) систем |

Ограничение программной среды (ОПС)

|  |  |
| --- | --- |
| ОПС.0 | Разработка политики ограничения программной среды |
| ОПС.2 | Управление установкой (инсталляцией) компонентов программного обеспечения |

Защита машинных носителей информации (ЗНИ)

|  |  |
| --- | --- |
| ЗНИ.0 | Разработка политики защиты машинных носителей информации |
| ЗНИ.1 | Учет машинных носителей информации |
| ЗНИ.2 | Управление физическим доступом к машинным носителям информации |
| ЗНИ.5 | Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации |
| ЗНИ.7 | Контроль подключения машинных носителей информации |
| ЗНИ.8 | Уничтожение (стирание) информации на машинных носителях информации |

Аудит безопасности (АУД)

|  |  |
| --- | --- |
| АУД.0 | Разработка политики аудита безопасности |
| АУД.1 | Инвентаризация информационных ресурсов |
| АУД.2 | Анализ уязвимостей и их устранение |
| АУД.3 | Генерирование временных меток и (или) синхронизация системного времени |
| АУД.4 | Регистрация событий безопасности |
| АУД.6 | Защита информации о событиях безопасности |
| АУД.7 | Мониторинг безопасности |
| АУД.8 | Реагирование на сбои при регистрации событий безопасности |
| АУД.10 | Проведение внутренних аудитов |

Антивирусная защита (АВЗ)

|  |  |
| --- | --- |
| АВЗ.0 | Разработка политики антивирусной защиты |
| АВЗ.1 | Реализация антивирусной защиты |
| АВЗ.2 | Антивирусная защита электронной почты и иных сервисов |
| АВЗ.4 | Обновление базы данных признаков вредоносных компьютерных программ (вирусов) |

Предотвращение вторжений (компьютерных атак) (СОВ)

|  |  |
| --- | --- |
| СОВ.0 | Разработка политики предотвращения вторжений (компьютерных атак) |
| СОВ.1 | Обнаружение и предотвращение компьютерных атак |
| СОВ.2 | Обновление базы решающих правил |

Обеспечение целостности (ОЦЛ)

|  |  |
| --- | --- |
| ОЦЛ.0 | Разработка политики обеспечения целостности |
| ОЦЛ.1 | Контроль целостности программного обеспечения |
| ОЦЛ.4 | Контроль данных, вводимых в информационную (автоматизированную) систему |
| ОЦЛ.5 | Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях |

Обеспечение доступности (ОДТ)

|  |  |
| --- | --- |
| ОДТ.0 | Разработка политики обеспечения доступности |
| ОДТ.1 | Использование отказоустойчивых технических средств |
| ОДТ.2 | Резервирование средств и систем |
| ОДТ.3 | Контроль безотказного функционирования средств и систем |
| ОДТ.4 | Резервное копирование информации |
| ОДТ.5 | Обеспечение возможности восстановления информации |
| ОДТ.6 | Обеспечение возможности восстановления программного обеспечения при нештатных ситуациях |
| ОДТ.8 | Контроль предоставляемых вычислительных ресурсов и каналов связи |

Защита технических средств и систем (ЗТС)

|  |  |
| --- | --- |
| ЗТС.0 | Разработка политики защиты технических средств и систем |
| ЗТС.2 | Организация контролируемой зоны |
| ЗТС.3 | Управление физическим доступом |
| ЗТС.4 | Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр |
| ЗТС.5 | Защита от внешних воздействий |

Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)

|  |  |
| --- | --- |
| ЗИС.0 | Разработка политики защиты информационной (автоматизированной) системы и ее компонентов |
| ЗИС.1 | Разделение функций по управлению (администрированию) информационной  (автоматизированной) системой с иными функциями |
| ЗИС.2 | Защита периметра информационной (автоматизированной) системы |
| ЗИС.3 | Эшелонированная защита информационной (автоматизированной) системы |
| ЗИС.4 | Сегментирование информационной (автоматизированной) системы |
| ЗИС.5 | Организация демилитаризованной зоны |
| ЗИС.8 | Сокрытие архитектуры и конфигурации информационной (автоматизированной) системы |
| ЗИС.13 | Защита неизменяемых данных |
| ЗИС.16 | Защита от спама |
| ЗИС.19 | Защита информации при ее передаче по каналам связи |
| ЗИС.20 | Обеспечение доверенных канала, маршрута |
| ЗИС.21 | Запрет несанкционированной удаленной активации периферийных устройств |
| ЗИС.23 | Контроль использования мобильного кода |
| ЗИС.24 | Контроль передачи речевой информации |
| ЗИС.25 | Контроль передачи видеоинформации |
| ЗИС.27 | Обеспечение подлинности сетевых соединений |
| ЗИС.28 | Исключение возможности отрицания отправки информации |
| ЗИС.29 | Исключение возможности отрицания получения информации |
| ЗИС.32 | Защита беспроводных соединений |
| ЗИС.34 | Защита от угроз отказа в обслуживании (DOS, DDOS-атак) |
| ЗИС.35 | Управление сетевыми соединениями |
| ЗИС.38 | Защита информации при использовании мобильных устройств |
| ЗИС.39 | Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных |

Реагирование на компьютерные инциденты (ИНЦ)

|  |  |
| --- | --- |
| ИНЦ.0 | Разработка политики реагирования на компьютерные инциденты |
| ИНЦ.1 | Выявление компьютерных инцидентов |
| ИНЦ.2 | Информирование о компьютерных инцидентах |
| ИНЦ.3 | Анализ компьютерных инцидентов |
| ИНЦ.4 | Устранение последствий компьютерных инцидентов |
| ИНЦ.5 | Принятие мер по предотвращению повторного возникновения компьютерных инцидентов |

Управление конфигурацией (УКФ)

|  |  |
| --- | --- |
| УКФ.0 | Разработка политики управления конфигурацией информационной  (автоматизированной) системы |
| УКФ.2 | Управление изменениями |
| УКФ.3 | Установка (инсталляция) только разрешенного к использованию программного обеспечения |

Управление обновлениями программного обеспечения (ОПО)

|  |  |
| --- | --- |
| ОПО.0 | Разработка политики управления обновлениями программного обеспечения |
| ОПО.1 | Поиск, получение обновлений программного обеспечения от доверенного источника |
| ОПО.2 | Контроль целостности обновлений программного обеспечения |
| ОПО.3 | Тестирование обновлений программного обеспечения |
| ОПО.4 | Установка обновлений программного обеспечения |

Планирование мероприятий по обеспечению безопасности (ПЛН)

|  |  |
| --- | --- |
| ПЛН.0 | Разработка политики планирования мероприятий по обеспечению защиты информации |
| ПЛН.1 | Разработка, утверждение и актуализация плана мероприятий по обеспечению защиты информации |
| ПЛН.2 | Контроль выполнения мероприятий по обеспечению защиты информации |

Обеспечение действий в нештатных ситуациях (ДНС)

|  |  |
| --- | --- |
| ДНС.0 | Разработка политики обеспечения действий в нештатных ситуациях |
| ДНС.1 | Разработка плана действий в нештатных ситуациях |
| ДНС.2 | Обучение и отработка действий персонала в нештатных ситуациях |
| ДНС.3 | Создание альтернативных мест хранения и обработки информации на случай возникновения нештатных ситуаций |
| ДНС.4 | Резервирование программного обеспечения, технических средств, каналов связи на случай возникновения нештатных ситуаций |
| ДНС.5 | Обеспечение возможности восстановления информационной (автоматизированной) системы в случае возникновения нештатных ситуаций |
| ДНС.6 | Анализ возникших нештатных ситуаций и принятие мер по недопущению их повторного возникновения |

Информирование и обучение персонала (ИПО)

|  |  |
| --- | --- |
| ИПО.0 | Разработка политики информирования и обучения персонала |
| ИПО.1 | Информирование персонала об угрозах безопасности информации и о правилах безопасной работы |
| ИПО.2 | Обучение персонала правилам безопасной работы |
| ИПО.3 | Проведение практических занятий с персоналом по правилам безопасной работы |
| ИПО.4 | Контроль осведомленности персонала об угрозах безопасности информации и о правилах безопасной работы |

Для ИСПДн 2 класса защищенности в приказе ФСТЭК от 18 февраля 2013 года № 21 перечислены состав и содержание мер защиты информации. Так как меры в приказах 21 и 31 ФСТЭК схожи, то укажем только различия в содержании мер:

Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ) - содержание мер схоже с приказом ФСТЭК №31.

Управление доступом субъектов доступа к объектам доступа (УПД): добавляются следующие меры:

|  |  |
| --- | --- |
| УПД.14 | Регламентация и контроль использования в информационной системе технологий беспроводного доступа |
| УПД.15 | Регламентация и контроль использования в информационной системе мобильных технических средств |
| УПД.17 | Обеспечение доверенной загрузки средств вычислительной техники |

И отсутствует мера УПД.3 Доверенная загрузка

Ограничение программной среды (ОПС) – аналогично приказу ФСТЭК №31.

Защита машинных носителей персональных данных (ЗНИ) – аналогично приказу ФСТЭК №31. Требований к дополнению мер не предъявляется.

Регистрация событий безопасности (РСБ) – аналогично приказу ФСТЭК №31. Требований к дополнению мер не предъявляется.

Антивирусная защита (АВЗ) – аналогично приказу ФСТЭК №31. Требований к дополнению мер не предъявляется.

Обнаружение вторжений (СОВ) – аналогично приказу ФСТЭК №31. Требований к дополнению мер не предъявляется.

Контроль (анализ) защищенности персональных данных (АНЗ):

|  |  |
| --- | --- |
| АНЗ.1 | Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей |
| АНЗ.2 | Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации |
| АНЗ.3 | Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации |
| АНЗ.4 | Контроль состава технических средств, программного обеспечения и средств защиты информации |
| АНЗ.5 | Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе |

Обеспечение целостности информационной системы и персональных данных (ОЦЛ) – аналогично приказу ФСТЭК №31. Требований к дополнению мер не предъявляется.

Обеспечение доступности персональных данных (ОДТ):

|  |  |
| --- | --- |
| ОДТ.4 | Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных |
| ОДТ.5 | Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала |

Защита среды виртуализации (ЗСВ)

|  |  |
| --- | --- |
| ЗСВ.1 | Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации |
| ЗСВ.2 | Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин |
| ЗСВ.3 | Регистрация событий безопасности в виртуальной инфраструктуре |
| ЗСВ.6 | Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных |
| ЗСВ.7 | Контроль целостности виртуальной инфраструктуры и ее конфигураций |
| ЗСВ.8 | Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры |
| ЗСВ.9 | Реализация и управление антивирусной защитой в виртуальной инфраструктуре |
| ЗСВ.10 | Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей |

Защита технических средств (ЗТС) – аналогично приказу ФСТЭК №31. Требований к дополнению мер не предъявляется.

Защита информационной системы, ее средств, систем связи и передачи данных (3ИС)

|  |  |
| --- | --- |
| ЗИС.3 | Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи |
| ЗИС.15 | Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных |

Выявление инцидентов и реагирование на них (ИНЦ) – добавляется мера ИНЦ.1 Определение лиц, ответственных за выявление инцидентов и реагирование на них.

Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)

|  |  |
| --- | --- |
| УКФ.1 | Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных |
| УКФ.3 | Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных |
| УКФ.4 | Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных |

## Анализ существующих мер и средств защиты АСУТ

В системе реализована ролевая модель разграничения доступа. Существующие роли представлены в таблице 2.

Таблица 2 – Роли пользователей

|  |  |
| --- | --- |
| Название роли | Описание роли |
| security\_administrator | Отвечает за общую безопасность системы. Назначает права доступа, настраивает механизмы аутентификации и авторизации, а также следит за целостностью и конфиденциальностью данных. |
| incident\_manager | Координирует реагирование на инциденты, открывает и регистрирует инциденты, определяет их приоритет и назначает ответственных за их разрешение. |
| default\_user | Использует систему для выполнения своих задач. Обязан соблюдать политики безопасности, сообщать о любых подозрительных событиях и соблюдать меры предосторожности. |
| recovery\_specialist | Занимается восстановлением системы после инцидентов. Разрабатывает и внедряет планы восстановления, минимизирует потери и обеспечивает быстрое восстановление сервисов. |

Доступ к сервисам и производственным процессам осуществляется через двухфакторную аутентификацию с использованием телефона. Идентификация сотрудников осуществляется посредством логина.

Также производится журналирование действий работников.

Можно сказать, что по имеющимся данным Wazuh частично содержит меры защиты информации, представленные в нормативных документах, рассмотренных в подпункте выше.

# Организационные меры защиты АС

## Порядок доступа к защищаемым ресурсам и безопасного обращения с ними

Доступ к защищаемым информационным ресурсам осуществляется на рабочих местах посредством учетных данных (логину и паролю), а также специальному коду, высланному на телефон при попытке входа.

Порядок безопасного обращения с ресурсами должен регламентироваться соответствующими политиками.

## Порядок работы с конфиденциальной информацией

Порядок работы с конфиденциальной информацией регламентируется Политикой конфиденциальности, Инструкцией по работе с конфиденциальной информацией, договором о неразглашении конфиденциальной информации, Положениями о конфиденциальной информации.

Необходимо иметь перечень информации, относящейся к конфиденциальной, а также сотрудников, допущенных до ознакомления с ней. В зависимости от ценности защищаемых сведений, меняются требования. К примеру, доступ к наиболее ценной информации могут иметь только доверенные сотрудники или персонал конкретных структурных подразделений организации, которым эта информация нужна для служебных целей.

Каждый работник, который получил допуск к информации, должен быть ответственным за ее сохранность. В случае несанкционированного доступа, ответственность за возникшие проблемы несут также и те, кто выдавал допуск на изучение сведений.

При получении доступа к конфиденциальной информации сотрудник делает прямой запрос руководителю. В нем он должен указать причины, по которым ему понадобилась закрытая информация. Иногда запрос предварительно проверяют сотрудники более низкого ранга и служба безопасности.

Для получения разрешения сотрудник обязан изучить нормативно-правовую базу организации, касающуюся секретных сведений. Кроме того, он подписывает документ, по которому на него накладываются дополнительные обязательства, в том числе требование о неразглашении секретных данных.

Документ, который разрешает доступ к информации, – это допуск, в котором перечислены лица, получающие его, и перечень сведений, которые им выдаются. На нем обязательно должна быть подпись руководителя или официальная печать. Обязательному протоколированию подлежат дата и время получения информации.

Допуск могут выдавать и другие лица – заместители руководителя и иные должностные лица. Они выдают разрешения только в пределах своих полномочий.

## Организация администрирования (службы) информационной безопасности

В процессе управления системой защиты автоматизированной системы управления (АСУ) выполняются следующие задачи администрирования:

1. Назначение и управление ответственными лицами**:** Определение персонала, ответственного за администрирование системы защиты АСУ.
2. Управление учетными записями и разграничение доступа: управление пользователями, включая создание и поддержание учетных записей, а также обеспечение соблюдения правил разграничения доступа.
3. Управление средствами защиты информации: настройка и управление средствами защиты, включая параметры программного обеспечения и обеспечение восстановления их функциональности. Это также включает генерацию, смену и восстановление паролей.
4. Управление обновлениями программного обеспечения: организация процесса обновления программного обеспечения, включая средства защиты, с учетом особенностей функционирования АСУ.
5. Централизованное управление системой защиты: при необходимости осуществление централизованного контроля и управления системой защиты АСУ.
6. Анализ событий безопасности: проведение анализа зарегистрированных событий безопасности в АСУ.
7. Сопровождение эксплуатации системы защиты: осуществление поддержки и обеспечение нормального функционирования системы защиты АСУ в процессе ее эксплуатации. Включает в себя ведение эксплуатационной документации и организационно-распорядительных документов, связанных с защитой информации.

## Общие права и обязанности персонала

Права и обязанности сотрудников определяются соответствующими должностными инструкциями.

Права сотрудников Отдела безопасности:

* контролировать работу всех сотрудников организации и следить за соблюдением режима конфиденциальности, введенного в организации;
* пользоваться информацией для служебного пользования, запрашивать ее у сотрудников других структурных подразделений организации;
* вступать во взаимодействие с органами исполнительной, законодательной и судебной власти для решения правовых вопросов, касающихся функций службы;
* принимать все необходимые меры для обеспечения защиты конфиденциальной информации;
* привлекать сторонних специалистов для разработки, внедрения и анализа эффективности системы защиты конфиденциальной информации; • давать указания сотрудникам других структурных подразделений организации по вопросам, входящим в компетенцию службы;
* проводить внутренние служебные расследования при обнаружении фактов намеренного или ненамеренного разглашения, утери, искажения, похищения конфиденциальной информации;
* осуществлять другие действия, предусмотренные должностными инструкциями и направленные на реализацию целей и задач службы.

Обязанности сотрудников Отдела безопасности:

* контролировать работу всех сотрудников организации и следить за соблюдением режима конфиденциальности;
* проводить профилактику намеренного или ненамеренного разглашения, утери, искажения, похищения конфиденциальной информации путем проведения инструктажа сотрудников организации;
* участвовать в разработке комплексной системы защиты конфиденциальной информации;
* периодически проверять журналы инструктажа и оборудование организации;
* проводить аттестацию всех сотрудников организации, проверять их знания в области существующих методов превентивной защиты конфиденциальной информации;
* выполнять другую работу, направленную на реализацию целей и задач службы защиты информации.

Обязанности сотрудников, работающих за АРМ:

* строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами АРМ;
* знать и строго выполнять правила работы со средствами защиты информации, установленными на АРМ;
* хранить в тайне свой пароль (пароли). С установленной периодичностью менять свой пароль (пароли);
* немедленно ставить в известность администратора защиты информации при подозрении компрометации паролей;
* вызывать специалиста организации при обнаружении:

1. фактов совершения в его отсутствие попыток несанкционированного доступа (НСД) к АРМ;
2. несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств АРМ;
3. отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования узлов АРМ или периферийных устройств (дисковода, и т.п.), а также перебоев в системе электроснабжения;
4. некорректного функционирования установленных на АРМ технических средств защиты;
5. непредусмотренных отводов кабелей и подключенных устройств;
6. присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закрепленного за ним АРМ в подразделении.

## Меры по реагированию на нарушения информационной безопасности

Часть сотрудников отдела ИБ образуют группу реагирования на инциденты ИБ.

Для выявления инцидентов и реагирования на них осуществляются:

1. определение лиц, ответственных за выявление инцидентов и реагирование на них;
2. обнаружение и идентификация инцидентов, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, программного обеспечения и средств защиты информации, нарушений правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;
3. своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в автоматизированной системе управления персоналом;
4. анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;
5. планирование и принятие мер по устранению инцидентов, в том числе по восстановлению автоматизированной системы управления в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий,
6. приводящих к возникновению инцидентов;
7. планирование и принятие мер по предотвращению повторного возникновения инцидентов.

## Ответственность за нарушение режима безопасности

Сотрудники, нарушившие режим безопасности, разгласившие конфиденциальную информацию, несут ответственность в соответствии с ТК, РФУК РФ, КоАП РФ и Федеральными законами (например, ФЗ №152, ФЗ №149, ФЗ №98). Ответственность за нарушение требований обеспечения информационной безопасности накладывается на должностных лиц и зависит от величины причиненного ущерба

Например, Статья 183 УК РФ. Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну.

## Организационно-распорядительные документы

* Политика информационной безопасности;
* Модель угроз информационной безопасности;
* Парольная политика;
* Приказ о назначении ответственных лиц за исполнение режима безопасности информации;
* Приказ о назначении группы реагирования на инциденты информационной безопасности и инструкция по реагированию;
* Политика реагирования на компьютерные инциденты;
* Приказ о контролируемой зоне;
* Положение о контролируемой зоне;
* Инструкция пользователя;
* Инструкция системного администратора;
* Журнал учета носителей информации;
* Журнал учета ключевых носителей;
* Положение о защите и обработке персональных данных;
* Политика в отношении обработки персональных данных;
* Правила обработки персональных данных без использования средств автоматизации;
* Приказ о комиссии по уничтожению персональных данных, и форма акта уничтожения;
* Приказ об утверждении мест хранения персональных данных;
* Политика идентификации и аутентификации;
* Политика управления доступом;
* Политика защиты машинных носителей информации;
* Политика аудита безопасности;
* Политика антивирусной защиты;
* Политика предотвращения вторжений (компьютерных атак);
* Политика обеспечения целостности;
* Политика обеспечения доступности;
* Политика защиты технических средств и систем;
* Политика защиты автоматизированной системы и ее компонентов;
* Политика управления конфигурацией автоматизированной системы;
* Политика управления обновлениями программного обеспечения;
* Политика планирования мероприятий по обеспечению защиты информации;
* Политика планирования мероприятий по обеспечению защиты информации;
* Политика обеспечения действий в нештатных ситуация;

# Программно-технические меры защиты АСУ

## Принципы применения программно-технических мер защиты

Технические меры по обеспечению безопасности информации реализуются с использованием средств защиты, включая программные и аппаратные средства, в которых они реализованы и обладают необходимыми функциями безопасности. В первую очередь, рассматриваются механизмы защиты, такие как параметры настройки, встроенные в стандартное программное обеспечение автоматизированной системы управления.

При использовании сертифицированных по требованиям безопасности информации средств защиты в автоматизированных системах управления, имеющих 2 класс защищенности, применяются средства не ниже 5 класса. Эти средства соответствуют уровню доверия 5 или выше. Также используются вычислительные устройства не ниже 5 класса, соответствующие 5 или более высокому уровню доверия.

Внедрение технических мер защиты информации должно быть адаптировано под модель информационной системы предприятия. Это позволяет построить эффективную оборону от потенциальных угроз конфиденциальной информации.

К принципам построения такой системы относятся:

* простота архитектуры, упрощение компонентов, сокращение числа каналов и протоколов межсетевого взаимодействия. В системе должны присутствовать только те элементы, без которых она окажется нежизнеспособной;
* внедрение только протестированных программных решений, уже не раз опробованных другими предприятиями, плюсы и минусы которых очевидны;
* минимальные доработки имеющихся лицензионных программных продуктов силами собственных или привлеченных исполнителей;
* использование только лицензированного ПО, при возможности оно должно быть внесено в государственный реестр программ для ЭВМ и баз данных;
* использование для построения системы только аутентичных компонентов, надежных и долговечных, не способных неожиданно выйти из строя и подорвать работоспособность системы. Все они должны быть совместимыми друг с другом;
* управляемость, легкость администрирования как самой системы, так и применяемых программных продуктов, минимальное использование сторонней технической поддержки;
* протоколирование и документирование любых действий пользователей, осуществляемых с файлами, содержащими конфиденциальную информацию, случаев несанкционированного доступа;
* эшелонированность обороны. Каждый потенциальный канал утечки должен иметь несколько рубежей системы защиты, затрудняющих работу потенциального похитителя информации.

## Физическая защита АС

В общем случае система физической безопасности должна включать в себя следующие подсистемы:

* управления доступом (с функцией досмотра): помещения должны быть оборудованы системой контроля и управления доступом, также проход на территорию должен осуществляться через КПП;
* обнаружения проникновения, аварийной и пожарной сигнализации (тревожной сигнализации);
* инженерно-технической защиты (пассивной защиты): двери каждого помещения, подлежащего защите должны быть оснащены замками;
* отображения и оценки обстановки: помещения контролируются с помощью системы видеонаблюдения;
* управления в аварийных и тревожных ситуациях;
* оповещения и связи в экстремальных ситуациях;
* личной безопасности персонала.

Необходимо рассматривать следующие меры контроля:

* посетители зон безопасности должны сопровождаться или обладать соответствующим допуском; дату и время входа и выхода следует регистрировать. Доступ следует предоставлять только для выполнения определенных авторизованных задач. Необходимо также знакомить посетителей с требованиями безопасности и действиями на случай аварийных ситуаций;
* доступ к важной информации и средствам ее обработки должен контролироваться и предоставляться только авторизованным лицам. Следует использовать средства аутентификации, например, карты доступа плюс PIN-код для авторизации и предоставления соответствующего доступа. Необходимо также надежным образом проводить аудит журналов регистрации доступа;
* необходимо требовать, чтобы весь персонал носил признаки видимой идентификации, следует поощрять его внимание к незнакомым несопровождаемым посетителям, не имеющим идентификационных карт сотрудников;
* права доступа сотрудников в зоны информационной безопасности следует регулярно анализировать и пересматривать.

Для повышения степени защиты зон информационной безопасности могут потребоваться дополнительные меры по управлению информационной безопасностью и соответствующие руководства. Они должны включать мероприятия в отношении персонала или представителей третьих сторон, работающих в зоне безопасности и состоять в следующем:

* о существовании зоны информационной безопасности и проводимых в ней работах должны быть осведомлены только лица, которым это необходимо в силу производственной необходимости;
* из соображений безопасности и предотвращения возможности злонамеренных действий в охраняемых зонах необходимо избегать случаев работы без надлежащего контроля со стороны уполномоченного персонала;
* пустующие зоны безопасности должны быть физически закрыты, и их состояние необходимо периодически проверять;
* персоналу третьих сторон ограниченный авторизованный и контролируемый доступ в зоны безопасности или к средствам обработки важной информации следует предоставлять только на время такой необходимости. Между зонами с различными уровнями безопасности внутри периметра безопасности могут потребоваться дополнительные барьеры и периметры ограничения физического доступа;
* использование фото, видео, аудио или другого записывающего оборудования должно быть разрешено только при получении специального разрешения.

## Предложения по применению дополнительных средств программно-аппаратной защиты информационных ресурсов

К уже существующим средствам защиты информации для удовлетворения требований, представленных в нормативных документах и в пункте 1.3 данной работы, следует добавить следующие средства:

* Антивирус: для противодействия вирусам на каждом АРМ – рекомендуется использовать решение от Dr.Web;
* Для защиты каждого узла от атак, подробного сбора информации для аудита и анализа рекомендуется использовать ESET Endpoint Security;
* Применение технологии VPN для обеспечения защищенного соединения при удаленном взаимодействии с системой.
* Систему обнаружения/предотвращения вторжений: в качестве IDS/IPS выступает – Suricata.
* Межсетевые экраны: для защиты СПД; для фильтрации входящего и исходящего трафика – рекомендуется использовать продукт компании InfoTecs ViPNet xFirewall 5;
* SIEM: для анализа в реальном времени событий безопасности, исходящих от сетевых устройств и приложений, и позволяет реагировать на них до наступления существенного ущерба; Система взаимодействует с межсетевыми экранами, DLP системой, антивирусом и IDS/IPS, системами журналирования. В качестве SIEM-системы выступает другой продукт компании – Wazuh SIEM.
* Систему управления обновлениями: для устранения уязвимостей, связанных с устаревшим ПО;
* Система управления информационными потоками и предотвращения утечек конфиденциальной информации (DLP) разработана с целью эффективного предотвращения раскрытия конфиденциальных данных. Основанная на анализе данных, пересекающих границы защищаемой информационной системы, она активно контролирует передачу информации. При обнаружении потока, содержащего конфиденциальную информацию, система активирует механизм блокировки передачи сообщения, пакета или сессии. DLP-система включает в себя компоненты на сетевом уровне и компоненты на уровне хоста. Сетевые компоненты следят за трафиком, пересекающим границы информационной системы, и обычно установлены на прокси-серверах, почтовых серверах и отдельных серверах. Компоненты уровня хоста, в свою очередь, размещаются на персональных компьютерах сотрудников и контролируют каналы, такие как запись на носители информации (компакт-диски, флэш-накопители и т. д.). Хостовые компоненты также стремятся обнаруживать изменения в сетевых настройках, установку программ для туннелирования, использование стеганографии и другие потенциальные методы обхода контроля. К использованию рекомендуется DeviceLock DLP.

## Обобщенная архитектура системы защиты информации



# ЗАКЛЮЧЕНИЕ

В рамках выполнения курсового проекта осуществлен анализ подсистемы управления, мониторинга и реагирования на компьютерные инциденты (Wazuh). Первая глава работы посвящена определению информационных активов данной системы, выявлению потенциальных угроз безопасности, а также установлению соответствия требованиям, предъявляемым нормативными документами. В процессе исследования проведена классификация Wazuh в соответствии с тремя ключевыми нормативными документами:

1. Руководящий документ Гостехкомиссии «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» - присвоен класс АС 1Г;
2. Приказ ФСТЭК от 14 марта 2014 г №31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» - присвоен класс защищенности К2;
3. Приказ ФСТЭК от 18 февраля 2013 г №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» - 2 уровень защищенности.

Во второй главе были представлены требования к организационным мерам защиты информации и сами меры. Также был представлен перечень организационно-распорядительных документов в области защиты информации для Wazuh.

В третьей главе описаны программно-технические меры защиты Wazuh и предложения по применению дополнительных программно-аппаратных средств.

# Список литературы

1. Приказ ФСТЭК от 18 февраля 2013 г №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
2. Приказ ФСТЭК от 14 марта 2014 г №31 «Об утверждении требований к обеспечению

защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»

1. Руководящий документ Гостехкомиссии «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»
2. Постановления Правительства РФ от 01.11.2012 N 1119. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
3. ГОСТ Р ИСО/МЭК 17799 -2005 «Информационная технология. Практические правила управления информационной безопасностью»
4. DLP-Системы <https://searchinform.ru/informatsionnaya-bezopasnost/dlp-sistemy/>
5. Положение об отделе информационной безопасности

[https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/dokumenty-poinformatsionnoj-bezopasnosti/instruktsii-po-informatsionnoj-bezopasnosti/polozhenieob-otdele-informatsionnoj-bezopasnosti/](https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/dokumenty-po-informatsionnoj-bezopasnosti/instruktsii-po-informatsionnoj-bezopasnosti/polozhenie-ob-otdele-informatsionnoj-bezopasnosti/)

1. Банк данных угроз безопасности информации.<https://bdu.fstec.ru/threat>