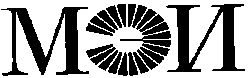
**Национальный исследовательский университет "МЭИ"**

****

**mpei_1**

КАФЕДРА РЕЛЕЙНОЙ ЗАЩИТЫ И АВТОМАТИЗАЦИИ ЭНЕРГОСИСТЕМ

Практическое задание по курсу «Основы кибербезопасности РЗА энергосистем»

|  |  |
| --- | --- |
| Студенты: | Энтентеев А.Р.  Максимов Р.С. |
| Группа: | Э–13м–19 |
| Преподаватель: | Карантаев В.Г. |

Москва, 2020 г.

# Выбор производителя и описание ПО

**Выбранное оборудование РЗА*:*** ABB RED670

**ПО для конфигурации*:*** PCM 600

**Используемые протоколы передачи данных:** МЭК 61850, МЭК 60870-5-103, SPA, LON, DNP.

**Интерфейсы*:*** *RS232*, *RS485*, *Ethernet, USB 2.0,* дисплей, кнопки на терминале, светодиоды.

# Описание диаграммы вариантов использования и определение объектов и субъектов доступа

Свойства безопасности информации:

* конфиденциальность;
* целостность;
* доступность;
* аутентичность;
* неотказуемость.

Аутентичность –  возможность однозначно идентифицировать автора/источник информации. Подлинность электронных данных часто удостоверяется таким средством, как электронно-цифровая подпись.

Конфиденциальность (информации) – это защита от несанкционированного доступа к информации, т.е. состояние доступности информации только авторизованным пользователям, процессам и устройствам.

Неотказуемость – это означает, что пользователи не могут позднее отказаться от выполненной транзакции (обычно реализуется с помощью цифровой подписи и инфраструктурыоткрытых ключей).

Целостность (информации) – это актуальность и непротиворечивость хранимой информации, ее защищенность от разрушения и несанкционированного изменения. Гарантия целостности особенно важна в тех случаях, когда информация представляет большую ценность и не должна быть потеряна, а также когда данные могут быть намеренно изменены в целях дезинформации получателя.

Доступность (информации) – это возможность за приемлемое время выполнить определенную операцию над данными или получить требуемую информационную услугу.

Таблица 1. Виды информации, обрабатываемые ИЭУ РЗА и предъявляемые требования к свойствам.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Функциональное назначение** | **Виды информации** | **Конфиденциальность** | **Целостность** | **Доступность** | **Неотказуемость** | **Аутентичность** |
| Телеизмерения (ТИ) | SV | - | + | + | +/-  (резервные источники) | + |
| C37.118, MMS | + | + | + | +/-  (резервные источники) | + |
| Телесигнализация (ТС) | GOOSE, DS через модуль BOM, C37.118 (не для РЗ) | - | + | + | - | + |
| Телеуправление (ТУ) | MMS,GOOSE, DS через модуль BIM | + | + | + | + | + |
| Конфигурационная информация | USB,MMS | + | + | + | - | + |
| Аутентификационная информация | Логин и пароль | + | + | + | - | + |
| Системная и сервисная информация | Сервер SNTP, GPS | + | + | + | - | + |

**Обоснование требований к передаваемой информации:**

**Телеизмерения (ТИ):**

1. Целостность – информация должна быть представлена в неискаженном виде;
2. Аутентичность – информация должна быть идентифицирована для корректного источника измерения.

**Телесигнализация (ТС):**

1. Целостность – для верного анализа состояния подключённых устройств к терминалу;
2. Доступность — для оперативного анализа состояния;
3. Аутентичность — для верного понимания источника сигнала.

**Телеуправление (ТУ):**

1. Конфиденциальность – сигналы управления коммутационными аппаратами не должны быть скомпрометированы;
2. Целостность – информация должна быть представлена в неискаженном виде для корректной работы релейной защиты;
3. Доступность – в случае нарушения данного свойства может произойти некорректная работа РЗ из-за отсутствия доступности;
4. Неотказуемость – в функционале терминала указано получение ответа о выполнении сигнала включения/отключения от КУ;
5. Аутентичность – для анализа причины изменения состояния коммутационного оборудования, иначе при отсутствии данного свойства у злоумышленников есть возможность скомпрометировать информацию.

**Конфигурационная информация:**

1. Конфиденциальность – свойства защиты и способ ее установки являются коммерческой тайной эксплуатирующей организации.
2. Целостность – любое конфигурирование должно производиться квалифицированным специалистом, если информация скомпрометирована, то есть опасность неправильной работы защиты.
3. Доступность – необходимо для оперативного доступа к информации о текущих параметрах оборудования;
4. Аутентичность – информация должна быть идентична заявленным, в ином случае может произойти неправильная работа терминала. важно отслеживать откуда и кем производится какое-либо изменение конфигурации или параметров срабатывания.

**Аутентификационная информация:**

1. Конфиденциальность – информация о ключах доступа должна быть доступна только по согласованию;
2. Целостность – целостность должна быть обеспечена для исключения отказа в доступе.

**Системная и сервисная информация:**

1. Конфиденциальность — информация должна быть доступна только по ключам доступа для исключения неправомерного доступа к состоянию энергосистемы и возможного удаления данных;
2. Целостность — информация должна быть целостна для правильного анализа состояния энергосистемы. Компрометация сигнала может нарушить синхронизацию работы всего комплекса защит и автоматики;
3. Доступность — информация должна быть доступна при любом запросе доступа. Потеря сигнала может нарушить синхронизацию работы всего комплекса защит и автоматики;
4. Аутентичность — для правильного анализа состояния и причин аварии информация должна быть подлинна.

# Субъекты и объекты доступа по отношению к ИЭУ РЗА

**Субъекты доступа:**Гость, Наблюдатель, Гость SPA, Системный оператор, Инженер по РЗ, Инженер разработчик, Администратор пользователей

Таблица 2. Права доступа у субъектов

|  |  |
| --- | --- |
| **Субъект** | **Права доступа** |
| Гость | Только права на считывание, представляемые только в местном ИЧМ |
| Наблюдатель | Может считывать параметры и просматривать меню с местного  ИЧМ. |
| Гость SPA | Может считывать параметры и просматривать меню с местного  ИЧМ. |
| Системный оператор | Может считывать параметры и просматривать меню, а также  выполнять управляющие воздействия. |
| Инженер по РЗ | Может создавать и загружать конфигурации и изменять уставки  ИЭУ, а также выполнять команды и справляться с аварийными  процессами |
| Инженер разработчик | Может загружать конфигурации и изменять уставки ИЭУ |
| Администратор пользователей | Может изменять присвоение уровней и настройки системы  безопасности. Может устанавливать сертификаты, просматривать контрольные журналы, изменять распределение ролей. |

**Объект доступа:** терминал ABB RED670 (Осциллограммы, Журнал событий, Бланк уставок, Конфигурация, ПО PCM600, Учетные записи, Сервер времени)

# UML диаграмма

На рисунке 1 представлена UML диаграмма.

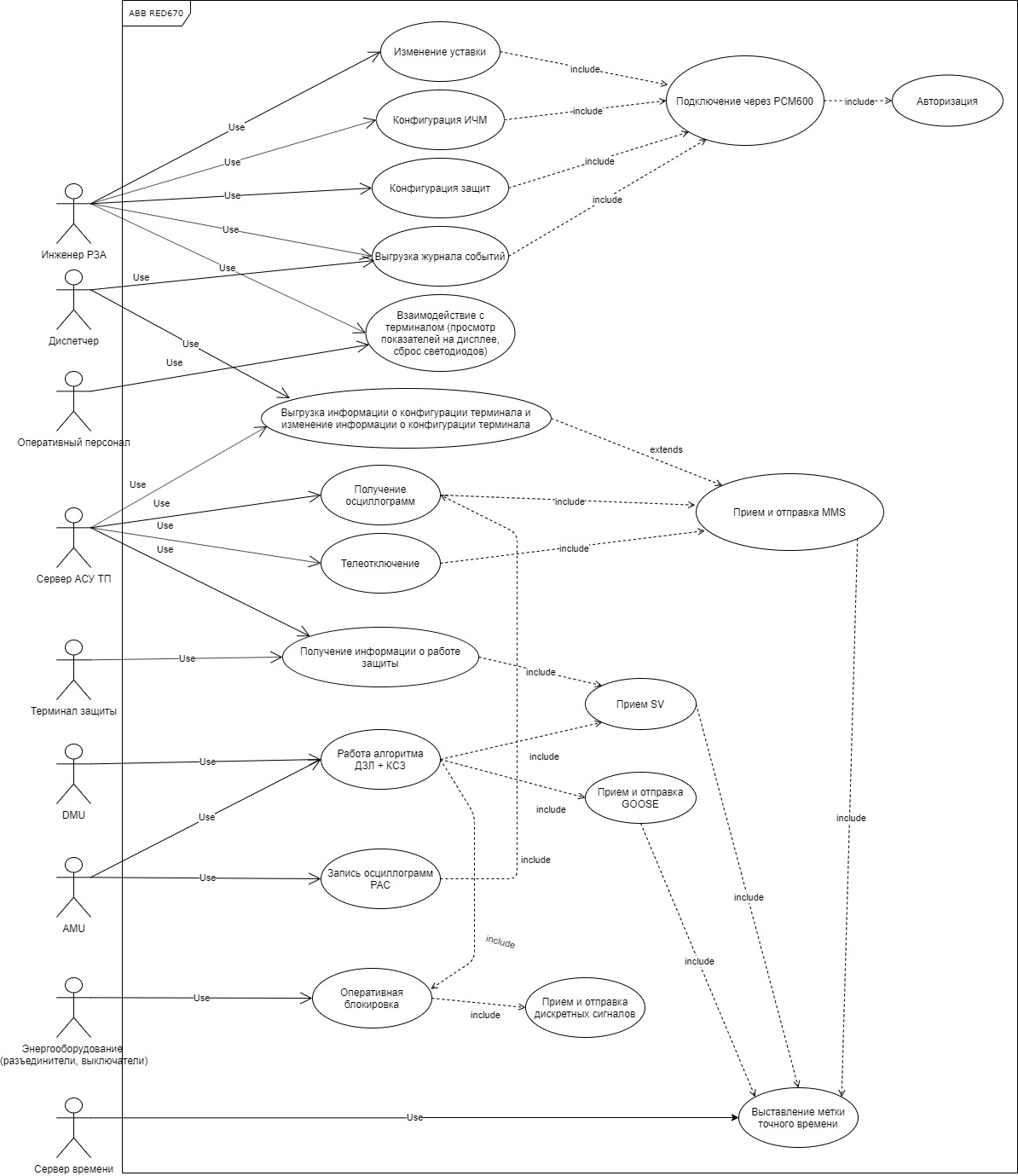


Рисунок 1 - UML диграмма

# Спецификация вариантов использования

**UC-1. Изменение уставок**

**Начальное условие**: ИЭУ включен и на нем запущено системное и прикладное ПО;

**Участники**: Инженер РЗА ПС;

**Пост-условие**: Инженер РЗА ПС может изменить уставки ИЭУ;

**Триггер**: Инженер РЗА ПС получил доступ к терминалу через PCM600;

**Основной поток**:

1. Инженер получает доступ к функционалу ИЭУ, используя ПО PCM600 после аутентификации.
2. После получения доступа Инженер проводит поиск нужной функции через ПО PCM 600.
3. Инженер выбирает функцию изменения уставок ИЭУ, а также просмотра группы уставок.
4. Инженер изменяет уставки.
5. Инженер сохраняет изменения и выходит из режима изменения конфигурации.

**UC-2. Конфигурация защит**

**Начальное условие**: ИЭУ включен и на нем запущено системное и прикладное ПО;

**Участники**: Инженер РЗА ПС;

**Пост-условие**: Инженер РЗА ПС может изменить конфигурацию терминала, добавив новый тип защиты или изменить алгоритм защиты;

**Триггер**: Инженер РЗА ПС получил доступ к терминалу через PCM600;

**Основной поток**:

1. Инженер получает доступ к функционалу ИЭУ, используя ПО PCM600 после аутентификации.
2. После получения доступа Инженер имеет доступ к текущей конфигурации.
3. Инженер выбирает функцию для добавления ее в текующую конфигурацию или изменяет алгоритм работы, путем добавления логических узлов в рабочее поле ПО PCM600.
4. Инженер сохраняет изменения и выходит из режима изменения конфигурации.

**UC-3. Телеотключение**

**Начальное условие**: у терминала настроен приём MMS сообшений от сервера АСУТП;

**Участники**: сервер АСУТП;

**Пост-условие**: Терминал может произвести отключение коммутационного аппарата при приеме сигнала телеотключения от сервера АСУТП;

**Триггер**: Управляющее воздействие на терминал;

**Основной поток**:

1. Терминал ожидает сигнала телеотключения
2. Коммутационный аппарат находится в отключенном состоянии
3. Терминал отправляет сигнал отключения при наличии сигнала телеотключения
4. Коммутационный аппарат происходит в отключенное состояние
5. Коммутационный аппарат направляет ответ об изменении своего состояния

# Разработка модели угроз кибербезопасности для ИЭУ РЗА

**Определение возможных последствий от реализации угроз безопасности информации**

1. Недопустимые последствия воздействий на подсистему РЗА.

|  |  |
| --- | --- |
| **№** | **Недопустимое последствие** |
| 1 | Ложное срабатывание ДЗЛ |
| 2 | Отказ срабатывания ДЗЛ (Изменение уставки/блокировки выходных сигналов) |
| 3 | Ложное срабатывание КСЗ |
| 4 | Отказ срабатывания КСЗ |
| 5 | Отказ AMU (выход из строя) |
| 6 | Отказ DMU (выход из строя)/отправка ложных GOOSE сообщений |
| 7 | Выход из строя терминала |
| 8 | Несанкционированная выгрузка данных из терминала |
| 9 | Блокирование ИЧМ модуля |
| 10 | Рассинхронизация ИЭУ |

1. Инвентаризация информационных ресурсов

|  |  |  |
| --- | --- | --- |
| **№** | **Компонент подсистемы** | **Информационные потоки** |
| 1 | ИЭУ РЗА | * Прием значений первичных величин * Прием/выдача сигналов срабатывания РЗ * Прием сигналов синхронизации времени * Прием/ выдача файла конфигурации |
| 2 | Устройство сопряжения | * Прием аналоговых сигналов * Прием дискретных сигналов * Отправка SV потоков * Отправка GOOSE сообщений |
| 3 | Устройство синхронизации времени | * Получение сигнала GPS * Отправка PTP пакета |



Диаграмма потоков данных для ИЭУ РЗА



Диаграмма потока данных для Устройства сопряжения



Диаграмма потока данных для Устройства сопряжения

1. Основные виды возможных воздействий

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Последствие** | **Компонент подсистемы** | **Воздействие** | **Пояснение** |
|  | Ложное срабатывание ДЗЛ | ИЭУ РЗА | Модификация конфигурационных данных | Изменение уставок срабатывания в сторону увеличения чувствительности |
| Порча SV и GOOSE пакетов | Неправильная работа алгоритма вследствие ложных первичных и дискретных значений |
|  | Отказ срабатывания ДЗЛ | ИЭУ РЗА | Модификация конфигурационных данных | Изменение уставок срабатывания в сторону уменьшения чувствительности |
| Порча SV и GOOSE пакетов | Неправильная работа алгоритма вследствие ложных первичных и дискретных значений |
|  | Ложное срабатывание КСЗ | ИЭУ РЗА | Модификация конфигурационных данных | Изменение уставок срабатывания в сторону увеличения чувствительности |
| Порча SV и GOOSE пакетов | Неправильная работа алгоритма вследствие ложных первичных и дискретных значений |
|  | Отказ срабатывания КСЗ | ИЭУ РЗА | Модификация конфигурационных данных | Изменение уставок срабатывания в сторону уменьшения чувствительности |
| Порча SV и GOOSE пакетов | Неправильная работа алгоритма вследствие ложных первичных и дискретных значений |
|  | Отказ AMU (выход из строя) | Устройство сопряжения | Модификация конфигурации | Ложные значения аналоговых сигналов(изменение коэф. трансформации) |
|  | Отказ DMU (выход из строя)/отправка ложных GOOSE сообщений | Устройство сопряжения | Модификация конфигурации | Ложные значения дискретных сигналов |
|  | Вывод из строя терминала | ИЭУ РЗА | Модификация конфигурации | Неработоспособность терминала из-за циклической перезагрузки терминала |
|  | Несанкционированная выгрузка данных из терминала | ИЭУ РЗА | Хищение данных, выгрузка параметров режима | Нарушение конфиденциальности данных |
|  | Блокирование ИЧМ модуля | ИЭУ РЗА | Перехват управления сигналами с ИЧМ | Невозможность взаимодействия с терминалом |
|  | Рассинхронизация ИЭУ | ИЭУ РЗА | Порча метки времени от GPS антенны | Изменение метки времени на ИЭУ |

1. Модель нарушителя безопасности информации для ИЭУ РЗА.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Вид нарушителя** | **Категория** | **Мотивация** | **Потенциал** |
|  | Лица, привлекаемые для администри-рования (управления) | Внутренний | Непреднамеренные, неосторожные или неквалифицированные действия | Базовый |
|  | Хакер | Внешний | Месть; Выявление уязвимостей с целью их продажи и получения финансовой выгоды;  Мошенничество, кража; Получение  конкурентных  преимуществ | Высокий |
|  | Лица, привлекаемые для ремонта, регламентного обслуживания и иных работ | Внутренний | Любопытство, желание самореализации, подтверждение статуса; Непреднамеренные, неосторожные или неквалифицированные действия; Выявление уязвимостей с целью их продажи и получения финансовой выгоды | Базовый |
|  | Конкурирующие организации | Внешний | Мошенничество, кража; Получение конкурентных преимуществ; Месть | Базовый повышенный |
|  |  |  |  |  |

1. Сценарии действий нарушителей по реализации угроз безопасности информации.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Нарушитель** | **Вид доступа** | **Воздействие** | **Набор шагов** |
|  | Инженер РЗА | Локальный | Невозможность выполнения возложенных функций (для ИЭУ РЗА) | 1) исследование информационной инфраструктуры (поиск какой-либо функции для выполнения служебных обязанностей);  2) управление и контроль в информационной инфраструктуре (выполнение служебных обязанностей);  3) реализация неправомерных действий (непреднамеренное осуществление доступа к ИЭУ РЗА, перевод в режим теста) |
|  | Оперативный персонал | Локальный | Модификация конфигурационных данных | 1) исследование информационной инфраструктуры (поиск точек воздействия);  2) управление и контроль в информационной инфраструктуре;  3) реализация неправомерных действий (изменение уставок РЗ в сторону увеличения чувствительности);  4) устранение признаков и следов неправомерных действий в информационной инфраструктуре. |
|  | Хакер | Удаленный | Кража конфигурационных данных | сбор данных об информационной инфраструктуре, необходимых для реализации угроз безопасности информации;  исследование информационной инфраструктуры и ее отдельных компонентов;  получение доступа к учетным записям;  повышение привилегий;  управление и контроль в информационной инфраструктуре; |
|  | Хакер | Физический | Порча коммуникационной инфраструктуры | сбор данных об информационной инфраструктуре, необходимых для реализации угроз безопасности информации;  Получение физического доступа к объекту  реализация неправомерных действий. |
|  |  |  |  |  |
|  |  |  |  |  |

1. Детализация воздействий на ИЭУ РЗА

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | | **Воздействие** | **Пояснение** | **Детализация** |
|  | Модификация конфигурационных данных | | Изменение уставок срабатывания в сторону увеличения чувствительности | 1. Несанкционированное получение доступа к изменению параметров РЗ  2. Подмена информации при взаимодействии |
|  | Порча SV и GOOSE пакетов | | Изменение содержимого пактов | 1. Несанкционированное получение доступа к изменению  2. Подмена информации |
|  | Хищение данных, выгрузка параметров режима | | Получение текущей информации о конфигурации объекта | 1.Несанкционированное получение доступа к конфигурационным данным  2.Выгрузка данных |
|  | Невозможность выполнения возложенных функций | | Перевод ИЭУ в режим теста | Социальная инженерия |
|  | Перехват управления сигналами с ИЧМ | | Получение доступа к программной или аппаратной части устройства | 1. Анализ целевого объекта воздействия  2. Инъекции кода (данных);  Или  1.Получение физического доступа и нарушение работы ИЧМ |
|  | Кража конфигурационных данных | | Получение текущей информации о конфигурации объекта | 1.Несанкционированное получение доступа к конфигурационным данным  2.Выгрузка данных |
|  | Порча коммуникационной инфраструктуры | | Физическое воздействие на кабель | 1.Использование слабостей в организации (в законодательстве, в контроле).  2.Получение физического доступа (обесточивание, замена элементов, кража); |
|  | Порча метки времени от GPS антенны | | Воздействие на радиосигнал | 1. Использование технических приемов по изменению GPS |

Таблица 3. Модель угроз и нарушителя для ИЭУ РЗА.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№** | **Последствие** | **Компонент подсистемы** | **Воздействие** | **Пояснение** | **Детализация реализации** | **Нарушитель** | **Категория** | **Потенциал** | **Мотивация** | **Вид доступа** | **Набор шагов** |
|  | Отказ срабатывания ДЗЛ | ИЭУ РЗА с функцией основной защиты ДЗЛ | Модификация конфигурационных данных | Изменение уставок срабатывания в сторону снижения чувствительности | 1.Несанкционированное получение доступа к изменению параметров РЗ  2. Подмена информации при взаимодействии | Инженер РЗА, Оперативный персонал | Внутренний | Базовый | Непреднамеренные, неосторожные или неквалифицированные действия | Локальный | 1) исследование информационной инфраструктуры (поиск какой-либо функции для выполнения служебных обязанностей);  2) управление и контроль в информационной инфраструктуре (выполнение служебных обязанностей);  3) реализация неправомерных действий (непреднамеренное осуществление доступа к ИЭУ РЗА) |
|  | Ложное срабатывание ДЗЛ | ИЭУ РЗА с функцией основной защиты ДЗЛ | Модификация конфигурационных данных | Изменение уставок срабатывания в сторону увеличения чувствительности | 1.Несанкционированное получение доступа к изменению параметров РЗ  2. Подмена информации при взаимодействии | Инженер РЗА, Оперативный персонал | Внутренний | Базовый | Непреднамеренные, неосторожные или неквалифицированные действия | Локальный | 1) исследование информационной инфраструктуры (поиск какой-либо функции для выполнения служебных обязанностей);  2) управление и контроль в информационной инфраструктуре (выполнение служебных обязанностей);  3) реализация неправомерных действий (непреднамеренное осуществление доступа к ИЭУ РЗА) |
| Порча SV и GOOSE пакетов | Неправильная работа алгоритма вследствие ложных первичных и дискретных значений |
|  | Ложное срабатывание КСЗ | ИЭУ РЗА с функцией основной защиты ДЗЛ | Модификация конфигурационных данных | Изменение уставок срабатывания в сторону увеличения чувствительности | 1.Несанкционированное получение доступа к изменению параметров РЗ  2. Подмена информации при взаимодействии | Инженер РЗА, Оперативный персонал | Внутренний | Базовый | Непреднамеренные, неосторожные или неквалифицированные действия | Локальный | 1) исследование информационной инфраструктуры (поиск какой-либо функции для выполнения служебных обязанностей);  2) управление и контроль в информационной инфраструктуре (выполнение служебных обязанностей);  3) реализация неправомерных действий (непреднамеренное осуществление доступа к ИЭУ РЗА) |
| Порча SV и GOOSE пакетов | Неправильная работа алгоритма вследствие ложных первичных и дискретных значений |
|  | Отказ срабатывания КСЗ | ИЭУ РЗА с функцией основной защиты ДЗЛ | Модификация конфигурационных данных | Изменение уставок срабатывания в сторону снижения чувствительности | 1.Несанкционированное получение доступа к изменению параметров РЗ  2. Подмена информации при взаимодействии | Инженер РЗА, Оперативный персонал | Внутренний | Базовый | Непреднамеренные, неосторожные или неквалифицированные действия | Локальный | 1) исследование информационной инфраструктуры (поиск какой-либо функции для выполнения служебных обязанностей);  2) управление и контроль в информационной инфраструктуре (выполнение служебных обязанностей);  3) реализация неправомерных действий (непреднамеренное осуществление доступа к ИЭУ РЗА) |
| Порча SV и GOOSE пакетов | Неправильная работа алгоритма вследствие ложных первичных и дискретных значений |
|  | Отказ AMU (выход из строя) | Устройство сопряжения | Модификация конфигурации | Ложные значения аналоговых сигналов(изменение коэф. трансформации) | 1. Несанкционированное получение доступа к изменению параметров РЗ  2. Подмена информации при взаимодействии | Инженер РЗА, Оперативный персонал | Внутренний | Базовый | Непреднамеренные, неосторожные или неквалифицированные действия | Локальный | 1) исследование информационной инфраструктуры (поиск какой-либо функции для выполнения служебных обязанностей);  2) управление и контроль в информационной инфраструктуре (выполнение служебных обязанностей);  3) реализация неправомерных действий (непреднамеренное осуществление доступа к ИЭУ РЗА) |
|  | Отказ DMU (выход из строя)/отправка ложных GOOSE сообщений | Устройство сопряжения | Модификация конфигурации | Ложные значения дискретных сигналов | 1.Несанкционированное получение доступа к изменению параметров РЗ  2. Подмена информации при взаимодействии | Инженер РЗА, Оперативный персонал | Внутренний | Базовый | Непреднамеренные, неосторожные или неквалифицированные действия | Локальный | 1) исследование информационной инфраструктуры (поиск какой-либо функции для выполнения служебных обязанностей);  2) управление и контроль в информационной инфраструктуре (выполнение служебных обязанностей);  3) реализация неправомерных действий (непреднамеренное осуществление доступа к ИЭУ РЗА) |
|  | Вывод из строя терминала | Модификация конфигурации | Неработоспособность терминала из-за циклической перезагрузки терминала | Модификация конфигурации | 1. Несанкционированное получение доступа к изменению параметров РЗ  2. Подмена информации при взаимодействии | Инженер РЗА, Оперативный персонал | Внутренний | Базовый | Непреднамеренные, неосторожные или неквалифицированные действия | Локальный | 1) исследование информационной инфраструктуры (поиск какой-либо функции для выполнения служебных обязанностей);  2) управление и контроль в информационной инфраструктуре (выполнение служебных обязанностей);  3) реализация неправомерных действий (непреднамеренное осуществление доступа к ИЭУ РЗА) |
|  | Несанкционированная выгрузка данных из терминала | ИЭУ РЗА | Хищение данных, выгрузка параметров режима | Нарушение конфиденциальности данных | 1.Несанкционированное получение доступа к конфигурационным данным  2.Выгрузка данных | Хакер | Внешний | Высокий | Месть; Выявление уязвимостей с целью их продажи и получения финансовой выгоды;  Мошенничество, кража; Получение  конкурентных  преимуществ | Удаленный | сбор данных об информационной инфраструктуре, необходимых для реализации угроз безопасности информации;  исследование информационной инфраструктуры и ее отдельных компонентов;  получение доступа к учетным записям;  повышение привилегий;  управление и контроль в информационной инфраструктуре; |
|  | Блокирование ИЧМ модуля | ИЭУ РЗА | Перехват управления сигналами с ИЧМ | Невозможность взаимодействия с терминалом | 1. Анализ целевого объекта воздействия  2. Инъекции кода (данных);  Или  1.Получение физического доступа и нарушение работы ИЧМ | Хакер | Внешний | Высокий | Месть; Выявление уязвимостей с целью их продажи и получения финансовой выгоды; | Физический | сбор данных об информационной инфраструктуре, необходимых для реализации угроз безопасности информации; |
|  | Рассинхронизация ИЭУ | ИЭУ РЗА | Порча метки времени от GPS антенны | Изменение метки времени на ИЭУ | 1. Использование технических приемов по изменению GPS | Хакер | Внешний | Высокий | Мошенничество, кража; Получение |  | исследование информационной инфраструктуры и ее отдельных компонентов; |

# Разработка требований к встроенным в ИЭУ РЗА средствам защиты информации

**Разработка матрицы разграничения доступа**

В подсистеме РЗА для управления доступом субъектов доступа к ИЭУ РЗА должны быть реализованы установленные методы управления доступом, назначены типы доступа субъектов к объекту доступа и реализованы правила разграничения доступа субъектов доступа к объекту доступа.

Таблица 4. Матрица разграничения доступа в автоматическом режиме работы

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Субъект / объект доступа** | **Бланк уставок** | **База данных с осциллограммами** | **Конфигурация** | **Данные процесса** | **Журнал событий** |
| **Сервер АСУ ТП** | Без доступа | Чтение | Без доступа | Чтение | Чтение |
| **Терминал защиты** | Без доступа | Без доступа | Без доступа | Чтение, запись(дискретных значений) | Запись |
| **MU** | Без доступа | Чтение, запись | Без доступа | Запись | Запись |
| **Оборудование** | Без доступа | Запись | Без доступа | Чтение | Без доступа |

Таблица 5. Матрица разграничения доступа в автоматизированном режиме

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Субъект / объект доступа** | **Журнал событий** | **Бланк уставок** | **База данных с осциллограммами** | **Конфигурация** | **ПО PCM600** | **ИЧМ** | **База данных пользователей** |
| **Гость** | Без доступа | Без доступа | Без доступа | Без доступа | Без доступа | Чтение | Без доступа |
| **Наблюдатель** | Без доступа | Без доступа | Без доступа | Без доступа | Без доступа | Чтение | Без доступа |
| **Гость SPA** | Без доступа | Без доступа | Без доступа | Без доступа | Без доступа | Чтение | Без доступа |
| **Диспетчер** | Чтение | Чтение | Чтение | Чтение | Чтение | Чтение, управление | Без доступа |
| **Инженер по РЗ** | Чтение | Чтение, запись | Чтение | Чтение, запись | Чтение, запись | Чтение, управление, запись | Без доступа |
| **Инженер разработчик** | Чтение | Чтение, запись | Чтение, запись | Чтение, запись | Чтение, запись | Чтение, запись | Без доступа |
| **Администратор пользователей** | Без доступа | Без доступа | Без доступа | Без доступа | Без доступа | Без доступа | Чтение, запись |

## **Синтез требований по реализации ВСЗИ для ИЭУ РЗА**

Таблица 6. Меры и средства защиты, обоснование их применения.

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Мера защиты** | **Средство или метод реализации** | **Обоснование** |
|  | Добавление входа по паролю | Аутентификация пользователя устройств; | Данная мера обеспечит конфиденциальность информации и ее целостность |
|  | Ведение журнала событий безопасности | Логирование событий безопасности | Данная мера направленна на обеспечение доступности данных и проверка аутентичности |
|  | Применение защищенных протоколов передачи данных | Защищенные протоколы обмена | Данная мера обеспечит конфиденциальность информации и ее аутентичность |
|  | Ограничение доступа извне | Использование встроенного МЭ | Данная мера обеспечит конфиденциальность информации и ее целостность |
|  | Требование подтверждения отправки, передачи, доставки, уведомления о приеме | Применение цифровых подписей | Данная мера обеспечит неотказуемость, аутентичность информации |

# Список литературы

1. Техническое руководство «Дифференциальная защита линии RED670», версия 2.2 МЭК.
2. Н.А. Гайдамакин. УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС Теоретические основы компьютерной безопасности Екатеринбург 2008. 212 c.
3. Гатчин Ю.А., Сухостат В.В., Куракин А.С., Донецкая Ю.В. ТЕОРИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И МЕТОДОЛОГИЯ ЗАЩИТЫ ИНФОРМАЦИИ – 2-е изд., испр. и доп. – СПб: Университет ИТМО, 2018. – 100 с.
4. Гома Х. UML. Проектирование систем реального времени, параллельных и распределенных приложений: Пер. с англ.-М.:ДМК Пресс, 2016.-700 с.:ил.
5. Фаулер М. UML. Основы, 3-издание.- Пер. с англ.- СПб: Символ-Плюс, 2020.-192 с., ил