Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт **информационных технологий и телекоммуникаций**
Кафедра **организации и технологии защиты информации**

Утверждена распоряжением по институту
от «12» марта 2020 г. № 029-р/12.00
Выполнена по заявке организации
(предприятия)_____
_____

Допущена к защите
« 20 » июня 2020 г.
Зав. кафедрой организации и технологии защиты информации
канд. техн. наук, доцент
В. И. Петренко

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

РАЗРАБОТКА РЕКОМЕНДАЦИЙ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ КОНТРОЛЯ И УЧЕТА ЭЛЕКТРОЭНЕРГИИ

Рецензенты:
Демурчев Никита Георгиевич
канд. техн. наук, доцент,
директор по проектам ООО «Инфоком-с»

(подпись)

Нормоконтролер:
Петренко Вячеслав Иванович
канд. техн. наук, доцент, доцент
кафедры организации и технологии
защиты информации

(*подпись*)

Выполнил (а):
Баран-Кешишев Никита Игоревич
студент 4 курса, группы ИНБ-б-о-16-2 направления подготовки 10.03.01 «Информационная безопасность» профиль «Организация и технология защиты информации» очной формы обучения

(*подпись*)

Руководитель:
Петренко Вячеслав Иванович
канд. техн. наук, доцент, доцент
кафедры организации и технологии
защиты информации

(*подпись*)

Дата защиты «30» июня 2020 г.

Оценка _____

Ставрополь, 2020 г.

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт информационных технологий и телекоммуникаций
Кафедра организации и технологии защиты информации
Направление Информационная безопасность
Направленность Организация и технология защиты информации

УТВЕРЖДАЮ
Зав. кафедрой организации и технологии защиты информации
канд. техн. наук, доцент
В. И. Петренко
«04» апреля 2020 г.

ЗАДАНИЕ НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ РАБОТУ (ДИПЛОМНУЮ РАБОТУ)

Студент Баран-Кешишев Никита Игоревич группа ИНБ-б-о 16-2
1. Тема Разработка рекомендаций по обеспечению информационной безопасности в автоматизированной системе контроля и учета электроэнергии
Утверждена распоряжением по институту «12» марта 2020 г. № 029-р/12.00
2. Срок представления работы к защите «20» июня 2020 г.
3. Исходные данные для выполнения работы Пример автоматизированной системы контроля и учета электроэнергии, содержащей информацию ограниченного доступа
4. Содержание ВКР:
4.1 Анализ существующих автоматизированных систем контроля и учета электроэнергии по принципу функционирования
4.2 Анализ информационных потоков в автоматизированных системах контроля и учета электроэнергии
4.3 Анализ угроз и уязвимостей информации в автоматизированной системе контроля и учета электроэнергии
4.4 Разработка рекомендаций по нейтрализации актуальных угроз в автоматизированной системе контроля и учета электроэнергии
Приложение
Дата выдачи задания «04» апреля 2020 г.
Руководитель работы В.И. Петренко
(*подпись*) (*инициалы, фамилия*)
Консультанты по разделам
(*подпись*) (*инициалы, фамилия*)
(*подпись*) (*инициалы, фамилия*)
(*подпись*) (*инициалы, фамилия*)
Задание к исполнению принял «04» апреля 2020 г. Н.И. Баран-Кешишев
подпись

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт информационных технологий и телекоммуникаций
Кафедра организации и технологии защиты информации
Направление Информационная безопасность
Направленность Организация и технология защиты информации

КАЛЕНДАРНЫЙ ПЛАН

Фамилия, имя, отчество Баран-Кешишев Никита Игоревич
Тема ВКР Разработка рекомендаций по обеспечению информационной безопасности в автоматизированной системе контроля и учета электроэнергии
Руководитель Петренко В.И.
Консультанты:

№	Наименование этапов выполнения выпускной квалификационной работы	Срок выполнения работы	Примечание
1.	Анализ литературы по теме работы	10.04.2020	
2.	Анализ существующих автоматизированных систем контроля и учета электроэнергии по принципу функционирования	20.04.2020	
3.	Анализ информационных потоков в автоматизированных системах контроля и учета электроэнергии	12.05.2020	
4.	Анализ угроз и уязвимостей информации в автоматизированной системе контроля и учета электроэнергии	31.05.2020	
5.	Разработка рекомендаций по нейтрализации актуальных угроз в автоматизированной системе контроля и учета электроэнергии	06.06.2020	
6.	Представление ВКР руководителю и нормоконтролёру	08.06.2020	
7.	Предварительная защита	10.06.2020	
8.	Представление ВКР заведующему кафедрой	19.06.2020	
9.	Рецензирование	23.06.2020	
10.	Представление ВКР в ГЭК	29.06.2020	

Руководитель В.И. Петренко
Зав. кафедрой В.И. Петренко
«04» апреля 2020 г.

Содержание

Введение

В настоящее время повсеместное распространение получает концепция контроля энергосетей. Сущность этой концепции заключается в переходе к автоматизированному управлению электроэнергетикой за счет внедрения современных телекоммуникационных и информационных технологий учета потребления электроэнергии, в том числе и индивидуальными потребителями путем создания автоматизированных систем контроля и учета электроэнергии. В создаваемой АСКУЭ обрабатывается информация ограниченного доступа, такая как: персональные данные потребителей, номера счетчиков, показания счетчиков и пр.

Для защиты информации, хранящейся и обрабатываемой в автоматизированной системе контроля и учета электроэнергии, предложено разработать рекомендации по обеспечению информационной безопасности АСКУЭ, следование которым повысит уровень защищенности данной системы[1].

Объектом исследования выбрана автоматизированная система контроля и учета электроэнергии.

Предметом исследования является уровень защищенности автоматизированной системы контроля и учета электроэнергии.

Целью исследования является повышение безопасности автоматизированной системы контроля и учета электроэнергии путем разработки организационных и технических мер.

Для достижения поставленной цели необходимо решить следующие задачи:

– выполнить анализ существующих автоматизированных систем контроля и учета электроэнергии;

– выполнить анализ информационных потоков в автоматизированных системах контроля и учета электроэнергии;

– выполнить анализ угроз и уязвимостей информации в АСКУЭ;

– разработать рекомендации по нейтрализации актуальных угроз в автоматизированной системе контроля и учета электроэнергии.

Данная выпускная квалификационная работа имеет четыре раздела, которые разбиты на пункты. В каждом разделе выполняются задачи, ведущие к достижению поставленной цели

1 Анализ существующих автоматизированных систем контроля и учета электроэнергии по принципу функционирования

1.1 Автоматизированная система контроля и учета электроэнергии на базе компании Saures

Система контроля и учета коммунальных ресурсов Saures предназначена для автоматизации учёта коммунальных ресурсов, сбора и передачи показаний счетчиков. SAURES совместима с широким спектром приборов учета, легко масштабируется от одной квартиры до многоквартирного дома. Также эта система подойдет для торговых и офисных центров, торговых сетей, сетей кафе и ресторанов, гостиниц и промышленных предприятий. Передача показаний производится в виде значений счетчиков импульсов в незашифрованном виде. Двусторонний канал связи не поддерживается, т.е. управляющая компания не может удаленно управлять нагрузкой или отключать потребителя[28].

Функциональные возможности:

1) Жильцы и арендодатели:

– автоматическая отправка показаний счетчиков;

– контроль нескольких объектов из одного аккаунта;

– гибкая система отправки уведомлений о событиях (email и push);

– почасовой архив показаний и графики расхода ресурсов;

– веб-кабинет, доступный через любой интернет-браузер;

– мобильное приложение для контроля со смартфона.

2) Управляющие компании:

– дистанционный сбор показаний ИПУ жильцов;

– недорогое внедрение и обслуживание даже на эксплуатируемых объектах;

– простое масштабирование от 1 квартиры до всего жилого фонда;

– специальный веб-кабинет с данными по всему жилфонду;

– удаленный контроль датчиков;

– готовая интеграция с 1С: Учет в управляющих компаниях ЖКХ, ТСЖ, ЖСК;

– дополнительные способы обмена данными с другими информационными системами.

3) Бизнес:

– удаленный сбор показаний счетчиков субабонентов;

– централизованный контроль расхода коммунальных ресурсов на нескольких объектах;

– простое внедрение и масштабируемость;

– открытый API для обмена со сторонними информационными системами.

Схема автоматизированной системы контроля и учета ресурсов ЖКХ Saures представлена на рисунке 1.

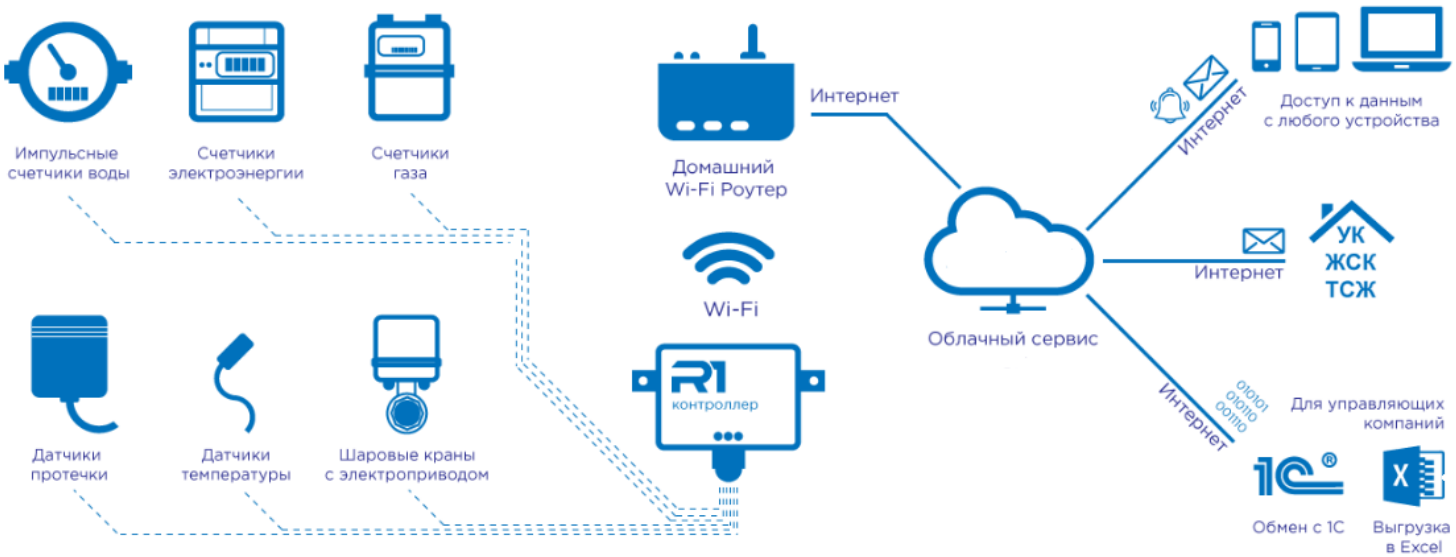

Рисунок 1 – Схема автоматизированной системы контроля и учета ресурсов ЖКХ Saures

Состав автоматизированной системы контроля и учета электроэнергии на базе компании Saures:

1) Контроллер:

– производит учет ресурсов на основании данных приборов учета;

– контролирует состояние подключенных датчиков;

– регулярно передает данные учета в облачный сервис;

– в аварийной ситуации посылает команду облачному сервису отправить вам оповещение о инциденте.

Для передачи данных в облачных сервис контроллер может использовать одну из двух технологий: Wi-Fi и NB-IoT.

Принципиальные отличия Wi-Fi и NB-IoT контроллеров:

– Канал передачи данных: Wi-Fi - подключение к домашнему роутеру без дополнительной оплаты связи, NB-IoT - подключение к сотовому оператору с оплатой связи.

– Дальность работы канала передачи данных: Wi-Fi - до 20 метров от точки доступа в пределах помещения, NB-IoT - до 5 километров от сотовой вышки в городской застройке.

– Частота радиоканала: Wi-Fi - 2.4 ГГц со средней пробивной способностью, NB-IoT - 900-1900 МГц с чувствительностью до -130dBm.

– Батарейки: Wi-Fi - пальчиковые бытовые батарейки 1.5 Вольта (температура эксплуатации до -20 градусов), NB-IoT - промышленные литиевые тионилхлоридные 3.6 Вольта (температура эксплуатации до -40 градусов).

– Работа с импульсными электросчетчиками: Wi-Fi - не поддерживаются, NB-IoT – поддерживаются.

– Способ настройки: Wi-Fi - с любого устройства с Wi-Fi через WEB-браузер, NB-IoT - с компьютера с Windows 7 и выше с использованием преобразователя USB->RS-485.

Преимущества Wi-Fi контроллеров:

– Низкая стоимость покупки;

– Низкая стоимость владения без дополнительных расходов на связь;

– Простота настройки и обслуживания.

Преимущества NB-IoT контроллеров:

– Независимость канала связи от оборудования и действий конечного пользователя;

– Высокая дальность работы канала связи;

– Работа в сложных условиях, в том числе при низких отрицательных температурах;

– Подключение до 32 устройств с интерфейсом RS-485.

2) Облачный сервис:

– хранит данные о расходе ресурсов, событиях, зафиксированных системой;

– производит отправку PUSH-уведомлений системы и оповещений по электронной почте;

– передает показания ваших приборов учета выбранным способом по назначенному расписанию;

– обеспечивает интеграцию системы со сторонними системами (например: «1С: Учет в управляющих компаниях ЖКХ, ТСЖ и ЖСК»).

Безопасность облачного сервиса:

– Система не хранит финансовых, паспортных данных и другой ценной информации, которая может быть использована злоумышленниками.

– Система не хранит паролей доступа, таким образом ваш пароль не знают даже сотрудники компании.

– Устройства выходят на связь с облаком в произвольное для каждого конкретного устройства время и всего на 10-60 секунд. Всё остальное время канал передачи данных полностью выключен. Это делает невозможным несанкционированный доступ к вашим данным или каналу передачи данных.

3) Web-интерфейс и мобильное приложение.

В системе предусмотрено два интерфейса кабинета: пользователя и компании. Кабинет пользователя предоставляет доступ только к своим собственным объектам недвижимости. Кабинет компании предоставляется

управляющим и монтажным организациям для осуществления обслуживания и поддержки всех своих клиентов.

Веб-кабинет пользователя предоставляет доступ к управлению системой и данным в рамках объектов недвижимости, которые этот пользователь контролирует.

Возможности кабинета:

– Мониторинг и анализ расхода ресурсов

– Контроль состояния датчиков:

– Настройка расписаний и способов автоматической отправки показаний;

– Настройка системы оповещений о событиях системы;

– Управление доступом к данным объекта;

– Настройка прочих параметров аккаунта.

Веб-кабинет компании предоставляет доступ ко всем объектам недвижимости, которые обслуживает компания. Так управляющая компания имеет доступ ко всему обслуживаемому жилфонду, а монтажная организации к объектам своих клиентов для осуществления поддержки.

Возможности кабинета:

– Мониторинг всех обслуживаемых объектов: контроль исправности оборудования и расписаний отправки показаний;

– Просмотр показаний счетчиков всех абонентов;

– Выгрузка данных о расходе ресурсов по всему зданию;

– Управление пользователями, адресами, объектами и контроллерами;

– Дистанционная поддержка пользовательских кабинетов.

Стоимость оборудования компании Saures представлена в таблице 1 [29].

Таблица 1 – Стоимость оборудования

№	Наименование	Цена
Контроллеры		
1	Контроллер SAURES R1, Wi-Fi, 4 канала	3 000 руб.

2	Контроллер SAURES R2 m2, Wi-Fi, 8 каналов	4 500 руб.
3	Контроллер SAURES R2 m3, Wi-Fi, 8 каналов, внешняя антенна	4 500 руб.
4	Контроллер SAURES R2 m5, Wi-Fi, 8 каналов, внешняя антенна, внешнее питание	5 500 руб.
5	Контроллер SAURES R4, Wi-Fi, 2 канала + 8 RS-485, внутренняя антенна	4 500 руб.
6	Контроллер SAURES R5, Wi-Fi, 8 каналов + 8 RS-485, внешняя антенна, внешнее питание	7 000 руб.
7	Контроллер SAURES R6 m1, NB-IoT, 8 каналов + 32 RS-485, SIM-чип МТС	7 000 руб.
8	Контроллер SAURES R6 m2, NB-IoT, 8 каналов + 32 RS-485, любая SIM-карта	7 000 руб.
9	Контроллер SAURES R7 m1, NB-IoT, 4 канала + 32 RS-485, SIM-чип МТС, вывод сбоку, IP66	6 000 руб.
10	Лицензия на программное обеспечение SAURES (на один канал RS-485 для контроллеров R6, R7) без НДС	800 руб.
Однофазные счетчики электроэнергии		
11	Счетчик электроэнергии НЕВА МТ 105 1S0 220V 5(40)А	1 300 руб.
12	Счетчик электроэнергии Энергомера CE102M R5 145-A	2 200 руб.
13	Счетчик электроэнергии Энергомера CE102M S7 145-AV	2 200 руб.
14	Счетчик электроэнергии Меркурий 206 RN	2 200 руб.
15	Счетчик электроэнергии Меркурий 206 PRSN	2 600 руб.
16	Счетчик электроэнергии ABB E31 412-200	3 500 руб.
Трехфазные счетчики электроэнергии		
17	Счетчик электроэнергии Меркурий 236 ART-01 PQRS	5 900 руб.
18	Счетчик электроэнергии Меркурий 236 ART-02 PQRS	5 900 руб.
19	Счетчик электроэнергии Меркурий 236 ART-03 PQRS	5 900 руб.
20	Счетчик электроэнергии Меркурий 230 ART-01 PQRSIN	5 700 руб.
21	Счетчик электроэнергии Меркурий 230 ART-02 PQRSIN	5 700 руб.
22	Счетчик электроэнергии Меркурий 230 ART-03 PQRSIN	5 700 руб.
Умные счетчики электроэнергии		
23	Электросчетчик Энергомера-1 Wi-Fi	6 500 руб.
24	Электросчетчик Меркурий-1 Wi-Fi	7 000 руб.
25	Электросчетчик ABB-1 Wi-Fi	8 000 руб.
26	Электросчетчик Меркурий-3 Wi-Fi	10 000 руб.
27	Электросчетчик Меркурий-3 NB-IoT	10 000 руб.

1.2 Автоматизированная система контроля и учета электроэнергии на базе компании «Стриж»

АСКУЭ «Стриж» предназначена для автоматизированного контроля и учета электроэнергии. Отличительной особенностью данной АСКУЭ является наличие базовых LPWAN-станций «Стриж». Вследствие чего для внедрения в АСКУЭ нужен только счетчик (котроллер не нужен), что делает данную систему проще в монтаже и дешевле[3].

Функциональные возможности:

– удаленный учет электроэнергии;

– сбор показаний в МКД дистанционно;

– выгрузка отчетов для электросетей;

– получение информации в облачном личном кабинете АСКУЭ «СТРИЖ.Cloud» (для пользователей)

– сбор показаний счетчиков во всем городе;

– отключение неплательщиков дистанционно;

– ограничение нагрузки должников без выезда бригады;

– добавление новых устройств plug-and-play (для предприятий).

Структурная схема АСКУЭ «Стриж» представлена на рисунке 2.

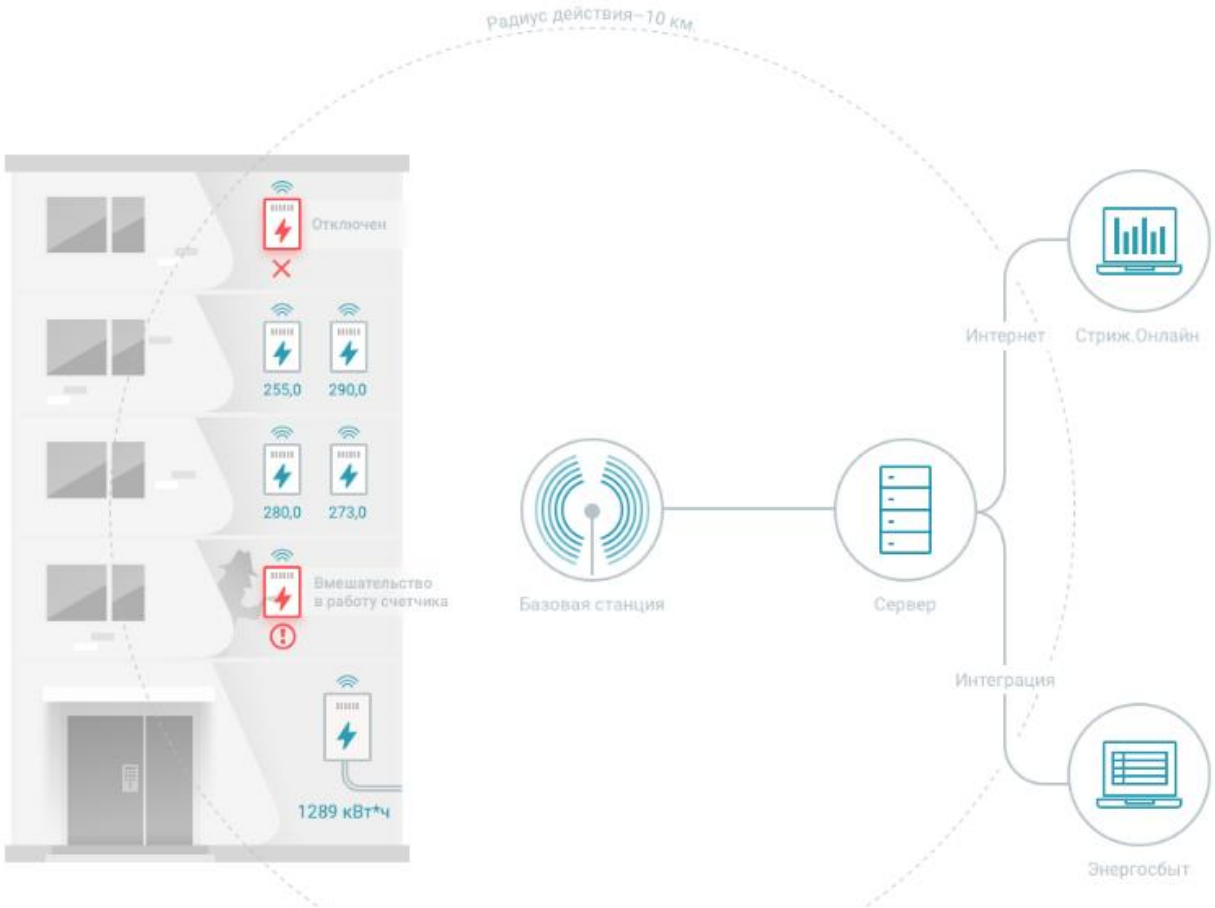

Рисунок 2 – Структурная схема АСКУЭ «Стриж»

В жилом доме для однофазных абонентов устанавливаются электросчетчики «А1», для трехфазных абонентов — «А3». Счетчики передают показания и параметры электроэнергии по настраиваемому

расписанию или стандартным схемам: ежечасно, ежедневно, ежемесячно. По беспроводному LPWAN-каналу данные передаются на базовую станцию, выполняющую роль устройства сбора и передачи данных (УСПД). Станция по защищенному каналу (используется шифрование AES 128 бит) передает данные в личный кабинет диспетчера. Также систем загружает данные в 1С и ГИС ЖКХ автоматически.

Состав АСКУЭ на базе компании «Стриж»:

1) Однофазный счетчик А-1 и трехфазный счетчик А-3.

Счетчик устанавливается plug-and-play без дополнительных настроек рядовым электриком.

Электросчетчик измеряет объем потребленной электроэнергии, фиксирует профили мощности и параметры электроэнергии. Встроенный радиомодуль передает накопленные данные по LPWAN-радиоканалу 868 МГц на ближайшую базовую станцию с заданной периодичностью.

Технология «СТРИЖ» поддерживает полнодуплексный способ связи (full duplex). Обратный канал связи обеспечивает удаленное управление электросчетчиком. Встроенное реле нагрузки решает задачу дистанционного ограничения или полного отключения электричества.

2) Базовая станция с использованием LPWAN-технологии.

LPWAN (от англ. Low-power Wide-area Network) — новый класс беспроводных сетей, разработанных для передачи данных телеметрии различных устройств, сенсоров, датчиков и приборов учета на дальние расстояния.

LPWAN-технология подразумевает наличие базовых станций (концентраторов) для сбора данных со счетчиков.

Основными достоинствами технологии LPWAN являются:

– дальность передачи сигнала: до 50 км на открытой территории и свыше 10 км при плотной городской застройке без промежуточного оборудования. Таким образом площадь покрытия в городских условиях — свыше 300 км², на открытой местности — порядка 8 000 км²;

– низкое энергопотребление: самое большое потребление происходит во время отправки пакета данных и составляет 50 мА. В остальное время потребление не превышает нескольких мкА. Эти параметры повышают срок автономной работы устройств до 10 лет без замены питания;

– высокая проникающая способность: энергетический потенциал канала связи (link budget) составляет 166 дБм. Этого хватает, чтобы сигнал легко «добивал» из подвалов, через бетонные стены и металлические шкафы. Кроме того, сигнал невозможно заглушить, так как передача идет в широком диапазоне частот;

– высокая масштабируемость: сеть масштабируется до нужно размера только за счет добавления новых датчиков, без промежуточного оборудования, mesh-архитектуры и снижения надежности. Одна базовая станция способна обслуживать около 2 000 000 устройств;

– использование нелицензируемого спектра: передача происходит на частоте 868,8 МГц при мощности до 25 мВт. На этом частотном диапазоне разрешено свободное и бесплатное использование радиопередающих устройств на основании Решений ГКРЧ.

Стоимость оборудования АСКУЭ «Стриж» представлена в таблице 2 [4].

Таблица 2 – Стоимость оборудования

№	Наименование	Цена
1	Электросчетчик «А1М» с радиомодемом «СТРИЖ» однофазный	3 560 руб.
2	«Умный» электросчетчик «А1» с радиомодемом «СТРИЖ» однофазный	6 040 руб.
3	Электросчетчик «А3» с радиомодемом «СТРИЖ» трехфазный	10 160 руб.
4	Электросчетчик «А1 Split» с радиомодемом «СТРИЖ» однофазный	8 130 руб.
5	Электросчетчик с радиомодемом «А3 Split» трехфазный	11 990 руб.
6	Внешний дисплей «УСП-1» для электросчетчиков «А1 Split», «А3 Split»	2 550 руб.
7	Базовая LPWAN-радиостанция «СТРИЖ»	112 645 руб.

1.3 Автоматизированная система контроля и учета электроэнергии на базе компании «Энергомера»

Функции АСКУЭ:

– Автоматический сбор данных с приборов учета электроэнергии;

– Хранение параметров учета в базе данных;

– Возможность установки многотарифного учета;

– Полное снятие воровства электричества;

– Возможность управления потреблением абонентов (удаленное отключение неплательщиков);

– Автоматизация выписки счетов абонентам [6].

Варианты построения АСКУЭ «Энергомера»:

– АСКУЭ на базе канала связи PLC G3;

– АСКУЭ на базе гибридного канала связи PLC + RF (подходит как для частного сектора, так и для использования в многоквартирных домах);

– АСКУЭ на базе GSM/GPRS (применяется при большой дальности между точками учёта);

– АСКУЭ на базе канала связи LoRa WAN (преимущественно для частного сектора);

– АСКУЭ на базе канала связи NB-IoT (преимущественно для частного сектора);

– АСКУЭ на базе проводных каналов связи.

Структурная схема АСКУЭ «Энергомера» представлена на рисунке 3.

Рисунок 3 – Структурная схема АСКУЭ «Энергомера»

Принцип работы АСКУЭ «Энергомера»:

1. Данные со счетчиков, установленных в домах, находящихся в частном секторе, могут передаваться по GPRS в центр обработки информации (ЦОИ) напрямую либо по протоколу ZigBee на устройство сбора и передачи данных (УСПД), расположенного на трансформаторной подстанции.

2. Данные со всех счетчиков установленных в квартирах автоматически собираются УСПД.

3. УСПД данные показания приборов учета передает на компьютер со специализированным программным обеспечением, где эти данные хранятся, обрабатываются, а также по этим данным выставляются «платежки» на оплату электроэнергии.

Система предоставляет пользователю возможность получать следующие показания приборов учета:

– потребление электроэнергии по месяцам, дням и часам;

– показания (накопительным итогом) на конец месяца, конец суток (по тарифам и суммарно);

– параметры электросети (ток, напряжение, частота).

Состав комплекса АСКУЭ «Энергомера»:

1. Счетчик электроэнергии однофазный микропроцессорный многотарифный CE201-S7.

Счетчик предназначен для измерения активной энергии в однофазных цепях переменного тока, организации многотарифного учета по четырем тарифам с передачей накопленной информации через оптопорт, RS-485, PLC, Ethernet или радиомодем. Хранение почасовых профилей нагрузки – 96 суток.

2. Счетчик электроэнергии однофазный многотарифный CE208-C2.

Счетчик предназначен для измерения активной и реактивной энергии в однофазных цепях переменного тока, организации многотарифного учета электроэнергии. Конструктивно счетчик разделен на две части: измерительный блок и индикаторное устройство. Имеет в составе интерфейсы для подключения к АСКУЭ и индикаторному устройству.

3. Счетчик электроэнергии трехфазный микропроцессорный многотарифный CE303-S34.

Счетчик является трехфазным трансформаторного или непосредственного включения, предназначен для измерения активной и реактивной электрической энергии, мощности, частоты напряжения, коэффициентов активной и реактивной мощностей, углов между векторами фазных напряжений и векторами фазных токов и напряжений, среднеквадратического значения напряжения, силы тока.

Счетчик имеет возможность организации многотарифного учета электроэнергии с передачей накопленной информации через оптопорт, интерфейс RS485, радио RF433, PLC или GSM/GPRS модемы.

4. Устройство сбора и передачи данных (УСПД) УСПД CE805.

УСПД предназначено для сбора, обработки и передачи измерительной информации и телеметрических данных в заданном формате для использования этих данных в многоуровневых территориально

распределенных автоматизированных системах контроля и учета энергоресурсов. Имеет возможность сбора и хранения данных с 1000 приборов учета по интерфейсу RS485.

Стоимость оборудования компании «Энергомера» представлена в таблице 3 [5].

Таблица 3 – Стоимость оборудования АСКУЭ «Энергомера»

№	Наименование	Цена
1	Счетчик электроэнергии однофазный микропроцессорный многотарифный CE201-S7	9 201 руб.
2	Счетчик электроэнергии однофазный многотарифный CE208-C2	8 188 руб.
3	Счетчик электроэнергии трехфазный микропроцессорный многотарифный CE303-S34	27 469 руб.
4	Устройство сбора и передачи данных (УСПД) УСПД CE805	87 732 руб.
5	Радиомодем CE831C1.03	23 771 руб.
6	PLC модем CE832C	10 293 руб.

1.4 Выводы по разделу

В данном разделе была решена первая задача, поставленная для достижения цели выпускной квалификационной работы, а так же рассмотрены следующие вопросы:

– описаны назначение и функциональные возможности существующих автоматизированных систем контроля и учета электроэнергии;

– проанализированы структура и состав действующих автоматизированных систем контроля и учета электроэнергии;

– проанализированны возможные варианты построения автоматизированной системы контроля и учет электроэнергии;

– описаны принципы работы существующих автоматизированных систем контроля и учета электроэнергии.

В ходе проведенного исследования выявлено, что большинство автоматизированных систем контроля и учета электроэнергии имеют 3 уровня.

2 Анализ информационных потоков в автоматизированных системах контроля и учета электроэнергии

2.1 Анализ информационных потоков в автоматизированных системах контроля и учета электроэнергии

В результате выполненного анализа установлено, что большинство существующих автоматизированных систем контроля и учета электроэнергии можно разделить на 3 уровня по принципу функционирования:

1. Уровень измерения - совокупность программно-технических средств, осуществляющих измерение параметров энергоучета, а также осуществляющих их первичную обработку в сигналы унифицированного вида. Часто эти устройства называют первичными измерительными приборами (ПИП), в качестве которых выступают электросчетчики, предоставляющие интерфейс доступа к информации по данной точке энергоучета. На данном уровне генерируется информация о номере счетчика и о показаниях. Данная информация передается на устройства второго уровня.

2. Информационно-измерительный комплекс - совокупность функционально объединенных программно-технических средств, предназначенных для сбора и обработки данных с одного или нескольких устройств первого уровня. Часто ко второму уровню относят: устройства сбора и передачи данных (УСПД), автоматизированные рабочие места (АРМ) и коммуникационные каналы между устройствами. Информация, которая была собрана с устройств первого уровня, передается на третий уровень.

3. Уровень управления включает в себя серверы со специализированным ПО, которые осуществляют сбор информации с устройств второго уровня, итоговую обработку этой информации, документирование и отображение в удобном для анализа виде. На данном уровне хранится и обрабатывается информация ограниченного доступа, такая как:

– Личные данные пользователей;
– Адреса;
– Номера счетчиков;
– Показания счётчиков;
– и пр.

Вся информация хранится в системе управления базами данных (СУБД). СУБД предназначена для хранения данных об устройствах, объектах, параметрах их конфигурации, событиях и показаниях, поступающих от объектового оборудования и приборов энергоучета.

Наиболее используемые СУБД в АСКУЭ:

– PostgreSQL;
– SQLite-хранилище;
– XML-хранилище;
– MySQL.

Также немаловажным аспектом в работе АСКУЭ является архивирование. Архивация предназначена для создания резервной копии всей базы данных. Архивная копия обеспечит сохранность данных: список счетчиков и показания для каждого счетчика, список контроллеров, список потребителей, список адресов и категорий. Рекомендуется данную процедуру выполнять периодически, а так же до момента выполнения технического обслуживания или обновления версии ПО. Архивация осуществляется остановленном сервере с помощью различных программ [2]:

– pgAdmin III;
– Effector Saver;
– Handy Backup.

Программа «Монитор» (другие названия: «Монитор активности», «Монитор обмена» и пр.) предназначен для диагностики проблем, удаленной отладки сервера, контроля процесса обмена с устройствами путем отображения информации об отправленных и принятых пакетах в реальном времени.

2.2 Анализ технических каналов передачи данных

Информация с устройств второго уровня преимущественно передается по радиоканалам, таким как:

1) GSM/GPRS (General Packet Radio Service) – это технология пакетной передачи данных через сеть сотовой связи стандарта GSM;

2) Wi-Fi (Wireless Fidelity) – технология беспроводной локальной сети с устройствами на основе стандартов IEEE 802.11;

3) LPWAN (от англ. Low-power Wide-area Network) — новый класс беспроводных сетей, разработанных для передачи данных телеметрии различных устройств, сенсоров, датчиков и приборов учета на дальние расстояния;

4) NB-IoT (Narrow Band Internet of Things) — стандарт сотовой связи для устройств телеметрии с низкими объёмами обмена данными.

Технические характеристики каналов передачи данных представлены в таблице 4.

Таблица 4 – Технические характеристики каналов передачи информации

Система (стандарт) и множественный доступ	Наименование характеристик				
	Полосы частот, МГц	Ширина полосы частот канала, кГц	Максимальная мощность, Вт	Число каналов (частотных)	Класс сигналов, тип модуляции
GSM-900 (2G)	890 – 915 (ПС) 935 – 960 (БС)	200	2 (ПС) 300 (БС)	124	200KF7WGMSK
GSM1800 (2G)	1710 – 1785 (ПС) 1805 – 1880 (БС)	200	<1 (ПС) 20(БС)	374	200KF7WGMSK
Wi-Fi 2,4 ГГц	2400 – 2483,5	$2*10^4/4*10^4$	<0,25	56	BPSK/ QPSK/ 16QAM/ 64QAM
Wi-Fi 5 ГГц	5180 – 5240 5745 – 5825	$2*10^4/4*10^4$	<0,1 <1	52	BPSK/ QPSK/ 16QAM/ 64QAM
LPWAN	868	0,1	<0,025	5000	DBPSK
NB-IoT	453–457,4 463–467	180	<0,2	12	GMSK/ QPSK/

	791–820 832–862 880–890 890–915 925–935 935–960 1710–1785 1805–1880 1920–1980 2110–2170 2500–2570 2620–2690				16QAM/ 64QAM

2.3 Классификация информации, обрабатываемой в различных элементах АСКУЭ

Анализ типов данных, передаваемых с устройств первого и второго уровней в АСКУЭ, построенных на базе продуктов одного из ведущих представителей рынка в России и ряде стран СНГ – ОАО «Концерн «Энергомера» позволил выделить следующие основные типы:

- данные интервала (3, 15, 30, 60 мин.);
- данные за сутки;
- данные за месяц;
- данные на конец суток (накопительным итогом);
- данные на конец месяца (накопительным итогом);
- текущие показания (накопительным итогом);
- показания с усреднениями за получасовые интервалы времени из внутренней памяти (90 — 180 суток);
- параметры электрической сети;
- журналы событий устройств нижних уровней;
- состояния реле (нагрузки, сигнализации) первичных измерительных приборов (например, счетчиков электроэнергии);
- существенные события (первичных измерительных приборов).

На третьем уровне хранится и обрабатывается следующая информация:

- личная информация пользователей;

– адреса пользователей;

– номера счетчиков;

– показания счетчиков;

– информация о контроллерах и прошивках.

Классификация информации, передаваемой с устройств первого и второго уровней приведена в таблице 5.

Таблица 5 – Классификация информации устройств нижних уровней

Вид информации	Гриф конфиденциальности
данные интервала (3, 15, 30, 60 мин.)	Персональные данные
данные за сутки	Персональные данные
данные за месяц	Персональные данные
текущие показания (накопительным итогом)	Персональные данные
показания с усреднениями за получасовые интервалы времени из внутренней памяти (90 — 180 суток)	Персональные данные
параметры электрической сети	Коммерческая тайна
журналы событий устройств нижних уровней	Коммерческая тайна
состояния реле (нагрузки, сигнализации) первичных измерительных приборов (например, счетчиков электроэнергии)	Коммерческая тайна
существенные события (первичных измерительных приборов)	Коммерческая тайна

Классификация информации, хранимой и обрабатываемой на устройствах верхнего уровня приведена в таблице 6.

Таблица 6 – Классификация информации, хранимой и обрабатываемой на устройствах верхнего уровня

Вид информации	Гриф конфиденциальности
Личная информация пользователей	Персональные данные
Адреса	Персональные данные
Номера счетчиков	Персональные данные
Показания счетчиков	Персональные данные
Сводка	Коммерческая тайна
Объекты	Коммерческая тайна
Пользователи	Коммерческая тайна
Контроллеры	Коммерческая тайна
Прошивки	Коммерческая тайна

Сравнительная таблица уровней доступа персонала на этапах развертывания, технического обслуживания и ремонта приведена в таблице 7.

Таблица 7 – Сравнительная таблица уровней доступа персонала на этапах развертывания, технического обслуживания и ремонта

Типы данных	Администратор	Оператор	Инженер
Личная информация пользователей	Полный	Просмотр	Просмотр
Сводка	Просмотр	Просмотр	Просмотр
Показания	Просмотр	Просмотр	Просмотр
Адреса	Полный	Просмотр	Просмотр
Объекты	Полный	Просмотр	Редактирование
Пользователи	Полный	Просмотр	Редактирование
Контроллеры	Полный	Просмотр	Полный
Прошивки	Просмотр	Нет	Полный

*Просмотр – просмотр информации без возможности добавления, редактирования, удаления.

*Редактирование – просмотр информации с возможностью редактирования, но без возможности добавления и удаления.

*Полный – просмотр информации с возможностью добавления, редактирования, удаления.

Сравнительная таблица уровней доступа персонала на этапе эксплуатации системы приведена в таблице 8.

Таблица 8 – Сравнительная таблица уровней доступа персонала на этапе эксплуатации системы

Типы данных	Администратор	Оператор
Личная информация пользователей	Полный	Просмотр
Сводка	Просмотр	Просмотр
Показания	Просмотр	Просмотр
Адреса	Полный	Просмотр
Объекты	Полный	Просмотр
Пользователи	Полный	Просмотр
Контроллеры	Полный	Просмотр
Прошивки	Просмотр	Нет

2.4 Выводы по разделу

В данном разделе была решена вторая задача, поставленная для достижения цели выпускной квалификационной работы, а также рассмотрены следующие вопросы:

– проведен анализ информационных потоков в автоматизированных системах контроля и учета электроэнергии;

– проведен анализ технических каналов передачи данных;

– проведена классификация информации, обрабатываемой в различных элементах автоматизированной системы контроля и учета электроэнергии.

Выявлено, что в автоматизированной системе контроля и учета электроэнергии хранится и обрабатывается информация ограниченного доступа, такая как: личная информация пользователей, показания счетчиков, информация о состоянии электрической сети и прочее.

3 Анализ угроз и уязвимостей информации в автоматизированной системе контроля и учета электроэнергии

3.1 Выбор модели угроз безопасности персональных данных

Для анализа угроз информационной безопасности АСКУЭ, как элемента Smart Grid, было выделено три типа данных, подлежащих защите:

1. Технические данные (параметры конфигураций, информация об ошибках и системных сбоях, логи), которыми обмениваются как активные, так и пассивные элементы системы. Целостность и доступность этих данных обеспечивает устойчивость энергосистемы.
2. Технические данные клиентов, поступающих от объектов энергоучета.
3. Персональные данные пользователей.

Для выбора базовой модели угроз безопасности персональных данных использовалась «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка) ФСТЭК»[7].

В зависимости от технологий, состава и характеристик технических средств ИСПДн, а также опасности реализации УБПДн и наступления последствий в результате несанкционированного или случайного доступа есть различные типы ИСПДн. АСКУЭ относится к типу распределенных ИСПДн, имеющих подключение к сетям связи общего пользования и (или) сетям международного информационного обмена.

При обработке ПДн в распределенных ИСПДн, имеющих подключение к сетям связи общего пользования и (или) сетям международного информационного обмена, возможна реализация следующих УБПДн:

– угрозы утечки информации по техническим каналам;

– угрозы НСД к ПДн, обрабатываемым на автоматизированном рабочем месте.

Угрозы утечки информации по техническим каналам включают в себя:

– угрозы утечки акустической (речевой) информации;

– угрозы утечки видовой информации;

– угрозы утечки информации по каналу ПЭМИН.

Возникновение угроз утечки акустической (речевой) информации, содержащейся непосредственно в произносимой речи пользователя ИСПДн, возможно при наличии функций голосового ввода ПДн в ИСПДн или функций воспроизведения ПДн акустическими средствами ИСПДн.

Реализация угрозы утечки видовой информации возможна за счёт просмотра информации с помощью оптических (оптикоэлектронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средства обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИСПДн.

Угрозы утечки информации по каналу ПЭМИН возможны из-за наличия электромагнитных излучений, в основном, монитора и системного блока компьютера. Основную опасность представляют угрозы утечки из-за наличия электромагнитных излучений монитора.

Угрозы НСД связаны с действиями нарушителей, имеющих доступ к ИСПДн, включая пользователей ИСПДн, реализующих угрозы непосредственно в ИСПДн, а также нарушителей, не имеющих доступа к ИСПДн, реализующих угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена. Кроме того, в такой ИСПДн имеют место угрозы, реализуемые с использованием протоколов межсетевого взаимодействия из внешних сетей, в том числе:

– угрозы «Анализа сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой в ИСПДн из внешних сетей информации;

– угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.;

– угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях;

– угрозы подмены доверенного объекта;

– угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных как внутри сети, так и во внешних сетях;

– угрозы выявления паролей;

– угрозы типа «Отказ в обслуживании»;

– угрозы удаленного запуска приложений;

– угрозы внедрения по сети вредоносных программ.

3.2 Определение актуальных угроз

Для описания угроз информационной безопасности были выделены основные зоны АСКУЭ:

1. Административная зона (управление персоналом). В этой зоне рассматриваются угрозы, связанные с умышленными или случайными действиями сотрудников [9].

2. Зона приложений - совокупность программных и технических средств АСКУЭ, подверженных угрозам ИБ.

3. Сеть - зона, объекты которой реализуют передачу данных между объектами одного уровня модели АСКУЭ, либо между объектами разных уровней.

Потенциальные угрозы безопасности в АСКУЭ [8]:

1) Административная зона:

– приведение системы в состояние «отказ в обслуживании»;

– утечка акустической (речевой) информации;

– утечка видовой информации;

– утечка информации по каналам ПЭМИН;

– изменение компонентов информационной системы;

– получение неправомерного доступа к управляющему сегменту;

– повышение привилегий в системе;

– использование идентификации/аутентификации, заданной по умолчанию;

– неправомерное ознакомление с защищаемой информацией;

– раскрытие информации о состоянии, параметрах, составе системы, а также о топологии сети;

– использование ПО, не предназначенного для обеспечения работоспособности системы, на АРМ;

– получение неправомерного доступа к техническим данным системы в результате небрежного отношения работников к своим обязанностям;

– получение неправомерного доступа к техническим данным системы в результате некомпетентности администраторов системы.

2) Зона приложений:

– удаленный запуск приложения путем использования возможностей удаленного управления системой, предоставляемых скрытыми программными и аппаратными закладками, либо используемыми штатными средствами;

– DoS/DDoS-атака на серверы системы управления/информирования;

– получение доступа к информации в результате передачи данных в открытом/незашифрованном виде (plaintext);

– получение неправомерного доступа из-за отсутствия механизмов аутентификации;

– XSS-атаки на систему управления/информирования;

– SQL-инъекции в систему управления/информирования;

– подбор паролей методами "грубой силы" или с использованием словарей.

3) Сеть:

– внедрение вредоносного кода за счет посещения зараженных сайтов в сети Интернет;

– внедрение вредоносного кода через рекламу, сервисы и контент;

– навязывание ложного маршрута сети;

– подмена доверенного пользователя;

– внедрение ложного объекта как в ИСПДн, так и во внешних сетях;

– анализ сетевого трафика;

– неправомерное подключение к сети управления/информирования на физическом уровне;

– перехват данных систем управления/информирования;

– подмена данных систем управления/информирования, передаваемых по сети;

– атаки подмены IP-адресов узлов систем управления/информирования.

Для того чтобы выделить наиболее актуальные угрозы безопасности АСКУЭ, необходимо знать вероятность реализации каждой угрозы. Список вероятности реализации угроз представлен в таблице 9:

Таблица 9 – Список вероятности реализации угроз

№	Угроза	Вероятность реализации угрозы	Коэффициент вероятности реализации угрозы нарушителем
1	приведение системы в состояние «отказ в обслуживании»	низкая	0,2
2	утечка акустической (речевой) информации	маловероятная	0,01
3	утечка видовой информации	низкая	0,2
4	утечка информации по каналам ПЭМИН	маловероятная	0,01
5	изменение компонентов информационной системы	низкая	0,2
6	получение неправомерного доступа к управляющему сегменту	низкая	0,2
7	повышение привилегий в системе	средняя	0,5
8	использование идентификации/аутентификации,	средняя	0,5

	заданной по умолчанию		
9	неправомерное ознакомление с защищаемой информацией	высокая	0,8
10	раскрытие информации о состоянии, параметрах, составе системы, а также о топологии сети	средняя	0,5
11	использование ПО, не предназначенного для обеспечения работоспособности системы, на АРМ	высокая	0,8
12	получение неправомерного доступа к техническим данным системы в результате небрежного отношения работников к своим обязанностям	средняя	0,5
13	получение неправомерного доступа к техническим данным системы в результате некомпетентности администраторов системы	средняя	0,5
14	удаленный запуск приложения путем использования возможностей удаленного управления системой, предоставляемых скрытыми программными и аппаратными закладками, либо используемыми штатными средствами	средняя	0,5
15	выявление паролей	средняя	0,5
16	DoS/DDoS-атака на серверы системы управления/информирования	низкая	0,2
17	получение доступа к информации в результате передачи данных в открытом/незашифрованном виде (plaintext)	низкая	0,2
18	получение неправомерного доступа из-за отсутствия механизмов аутентификации	средняя	0,5
19	SQL-инъекции в систему управления/информирования	низкая	0,2
20	внедрение вредоносного кода за счет посещения зараженных сайтов в сети Интернет	средняя	0,5
21	внедрение вредоносного кода через рекламу, сервисы и контент	средняя	0,5
22	навязывание ложного маршрута сети	низкая	0,2
23	подмена достоверного	низкая	0,2

	пользователя		
24	внедрение ложного объекта как в ИСПДн, так и во внешних сетях	низкая	0,2
25	анализ сетевого трафика	высокая	0,8
26	неправомерное подключение к сети управления/информирования на физическом уровне	низкая	0,2
27	перехват данных систем управления/информирования	низкая	0,2
28	подмена данных систем управления/информирования, передаваемых по сети	низкая	0,2
29	атаки подмены IP-адресов узлов систем управления/информирования	маловероятная	0,01

Круговая диаграмма, иллюстрирующая процентное соотношение угроз безопасности АСКУЭ, представлена на рисунке 4.

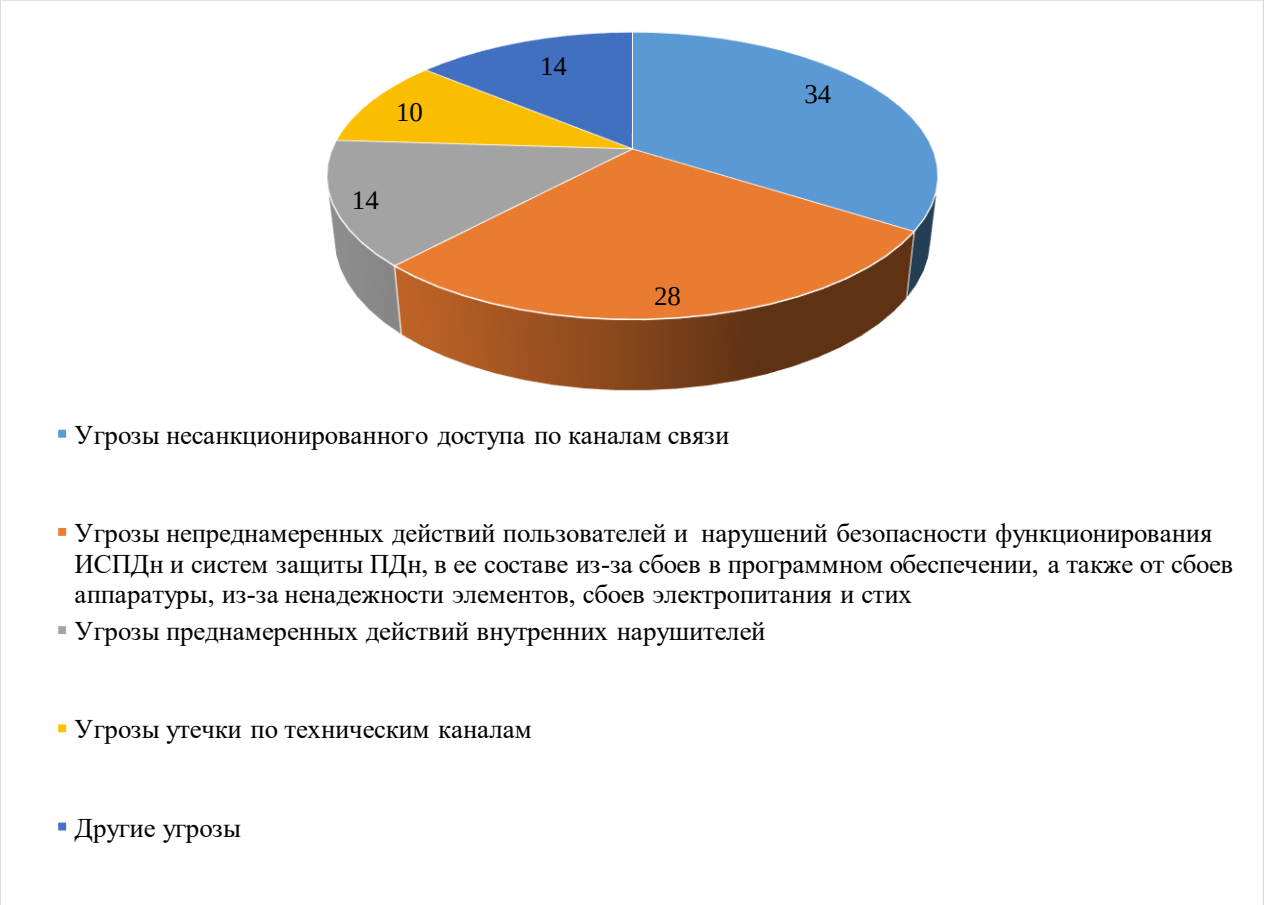

Рисунок 4 – Круговая диаграмма, иллюстрирующая процентное соотношение угроз безопасности АСКУЭ

Данная круговая диаграмма на рисунке иллюстрирует, что наиболее уязвимыми местами являются канал связи и персонал, работающий с

документами, информацией и базами данных. Причем в большинстве случаев утрата данных происходит не в результате преднамеренных действий, а из-за невнимательности или безответственности персонала, а также нехватки профессиональных навыков работы с вычислительной техникой и программным обеспечением, предназначенным для обработки данных. Другой возможной угрозой являются целенаправленные действия сотрудников, имеющих возможность подключения к распределенной сети и совершения противоправных действий, направленных на нанесение ущерба организации путем перехвата конфиденциальной информации или выведения из строя информационной системы.

3.3 Выводы по разделу

В данном разделе была решена третья задача, поставленная для достижения цели выпускной квалификационной работы, а также рассмотрены следующие вопросы:

- выбрана модель угроз безопасности персональных данных;
- определены актуальные угрозы.

Выявлено, что автоматизированная система контроля и учета электроэнергии относится к распределенным ИСПДн, имеющим подключение к сетям связи общего пользования и (или) сетям международного информационного обмена.

Выявлено, что наиболее уязвимыми местами являются канал связи и персонал, работающий с документами, информацией и базами данных.

4 Разработка рекомендаций по нейтрализации актуальных угроз в автоматизированной системе контроля и учета электроэнергии

4.1 Анализ автоматизированной системы контроля и учета электроэнергии как автоматизированной системы управления

В автоматизированной системе управления объектами защиты являются:

1) информация (данные) о параметрах (состоянии) управляемого (контролируемого) объекта или процесса (входная (выходная) информация, управляющая (командная) информация, контрольно-измерительная информация, иная критически важная (технологическая) информация);

2) программно-технический комплекс, включающий технические средства (в том числе автоматизированные рабочие места, промышленные серверы, телекоммуникационное оборудование, каналы связи, программируемые логические контроллеры, исполнительные устройства), программное обеспечение (в том числе микропрограммное, общесистемное, прикладное), а также средства защиты информации.

Защита информации в автоматизированной системе управления достигается путем принятия в рамках системы защиты автоматизированной системы управления совокупности организационных и технических мер защиты информации, направленных на блокирование (нейтрализацию) угроз безопасности информации, реализация которых может привести к нарушению штатного режима функционирования автоматизированной системы управления и управляемого (контролируемого) объекта и (или) процесса, на локализацию и минимизацию последствий от возможной реализации угроз безопасности информации, восстановление штатного режима функционирования автоматизированной системы управления в случае реализации угроз безопасности информации.

Принимаемые организационные и технические меры защиты информации:

– должны обеспечивать доступность обрабатываемой в автоматизированной системе управления информации (исключение неправомерного блокирования информации), ее целостность (исключение неправомерного уничтожения, модифицирования информации), а также, при необходимости, конфиденциальность (исключение неправомерного доступа, копирования, предоставления или распространения информации);

– должны соотноситься с мерами по промышленной, физической, пожарной, экологической, радиационной безопасности, иными мерами по обеспечению безопасности автоматизированной системы управления и управляемого (контролируемого) объекта и (или) процесса;

– не должны оказывать отрицательного влияния на штатный режим функционирования автоматизированной системы управления.

Для обеспечения защиты информации в автоматизированной системе управления проводятся следующие мероприятия:

– формирование требований к защите информации в автоматизированной системе управления;

– разработка системы защиты автоматизированной системы управления;

– внедрение системы защиты автоматизированной системы управления и ввод ее в действие;

– обеспечение защиты информации в ходе эксплуатации автоматизированной системы управления;

– обеспечение защиты информации при выводе из эксплуатации автоматизированной системы управления.

4.2 Разработка организационных мер для защиты автоматизированной системы контроля и учета электроэнергии

Для обеспечения информационной безопасности автоматизированной системы контроля и учета электроэнергии были разработаны

организационные меры в соответствии с приказом Приказ ФСТЭК России от 14 марта 2014 г. N 31 [17].

Ниже приведены рекомендованные организационные меры, внедрение которых на этапе внедрения автоматизированной системы управления и ввода ее в действие, позволяет дополнительно защитить автоматизированную систему контроля и учета электроэнергии (примеры разработанных документов приведены в приложениях А,Б):

– разработка документов, определяющих правила и процедуры (политики), реализуемые оператором для обеспечения защиты информации в автоматизированной системе управления в ходе ее эксплуатации (далее - организационно-распорядительные документы по защите информации);

– введение ограничений на действия персонала (пользователей (операторского персонала), администраторов, обеспечивающего персонала), а также на условия эксплуатации, изменение состава и конфигурации технических средств и программного обеспечения;

– определение администратора безопасности информации;

– реализация правил разграничения доступа, регламентирующих права доступа субъектов доступа к объектам доступа;

– проверка полноты и детальности описания в организационно-распорядительных документах по защите информации действий персонала автоматизированной системы управления и администратора безопасности информации, направленных на обеспечение защиты информации;

– отработка практических действий должностных лиц и подразделений, обеспечивающих эксплуатацию автоматизированной системы управления и защиту информации.

Разрабатываемые организационно-распорядительные документы по защите информации должны определять правила и процедуры (политики):

– реализаций отдельных мер защиты информации в автоматизированной системе управления в рамках ее системы защиты;

– планирования мероприятий по обеспечению защиты информации в автоматизированной системе управления;

– обеспечения действий в нештатных (непредвиденных) ситуациях в ходе эксплуатации автоматизированной системы управления;

– информирования и обучения персонала автоматизированной системы управления;

– анализа угроз безопасности информации в автоматизированной системе управления и рисков от их реализации;

– управления (администрирования) системой защиты информации автоматизированной системы управления;

– выявления инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования автоматизированной системы управления и (или) к возникновению угроз безопасности информации (далее - инциденты), и реагирования на них;

– управления конфигурацией автоматизированной системы управления и ее системы защиты;

– контроля (мониторинга) за обеспечением уровня защищенности автоматизированной системы управления;

– защиты информации при выводе из эксплуатации автоматизированной системы управления.

Обеспечение защиты информации в ходе эксплуатации автоматизированной системы управления осуществляется оператором в соответствии с эксплуатационной документацией на систему защиты и организационно-распорядительными документами по защите информации и включает следующие процедуры:

– планирование мероприятий по обеспечению защиты информации в автоматизированной системе управления;

– обеспечение действий в нештатных (непредвиденных) ситуациях в ходе эксплуатации автоматизированной системы управления;

– информирование и обучение персонала автоматизированной системы управления;

– периодический анализ угроз безопасности информации в автоматизированной системе управления и рисков от их реализации;

– управление (администрирование) системой защиты автоматизированной системы управления;

– выявление инцидентов в ходе эксплуатации автоматизированной системы управления и реагирование на них;

– управление конфигурацией автоматизированной системы управления и ее системы защиты;

– контроль (мониторинг) за обеспечением уровня защищенности автоматизированной системы управления;

– администратор должен выполнить настройку систем авторизации пользователей не только за счет операционной системы персональных рабочих станций, но и путем авторизации пользователя на сетевом оборудовании при подключении к информационной системе. Данные действия помогут повысить уровень защищенности путем ликвидации ряда угроз связанных с подключение злоумышленника к сетевому оборудованию.

В ходе планирования мероприятий по обеспечению защиты информации в автоматизированной системе управления осуществляются:

– определение лиц, ответственных за планирование и контроль мероприятий по обеспечению защиты информации в автоматизированной системе управления;

– разработка, утверждение и актуализация плана мероприятий по обеспечению защиты информации в автоматизированной системе управления;

– контроль выполнения мероприятий по обеспечению защиты информации в автоматизированной системе управления, предусмотренных утвержденным планом.

В ходе обеспечения действий в нештатных (непредвиденных) ситуациях при эксплуатации автоматизированной системы управления осуществляются:

– планирование мероприятий по обеспечению защиты информации в автоматизированной системе управления на случай возникновения нештатных (непредвиденных) ситуаций;

– обучение и отработка действий персонала по обеспечению защиты информации в автоматизированной системе управления в случае возникновения нештатных (непредвиденных) ситуаций;

– создание альтернативных мест хранения и обработки информации на случай возникновения нештатных (непредвиденных) ситуаций;

– обеспечение возможности восстановления автоматизированной системы управления и (или) ее компонентов в случае возникновения нештатных (непредвиденных) ситуаций.

В ходе информирования и обучения персонала автоматизированной системы управления осуществляются:

– периодическое информирование персонала об угрозах безопасности информации, о правилах эксплуатации системы защиты автоматизированной системы управления и отдельных средств защиты информации;

– периодическое обучение персонала правилам эксплуатации системы защиты автоматизированной системы управления и отдельных средств защиты информации, включая проведение практических занятий с персоналом на макетах или в тестовой зоне.

В ходе анализа угроз безопасности информации в автоматизированной системе управления и возможных рисков от их реализации осуществляются:

– периодический анализ уязвимостей автоматизированной системы управления, возникающих в ходе ее эксплуатации;

– периодический анализ изменения угроз безопасности информации в автоматизированной системе управления, возникающих в ходе ее эксплуатации;

– периодическая оценка последствий от реализации угроз безопасности информации в автоматизированной системе управления (анализ риска).

В ходе управления (администрирования) системой защиты автоматизированной системы управления осуществляются:

– определение лиц, ответственных за управление (администрирование) системой защиты автоматизированной системы управления;

– управление учетными записями пользователей и поддержание правил разграничения доступа в автоматизированной системе управления в актуальном состоянии;

– управление средствами защиты информации в автоматизированной системе управления, в том числе параметрами настройки программного обеспечения, включая восстановление работоспособности средств защиты информации, генерацию, смену и восстановление паролей;

– управление обновлениями программного обеспечения, включая программное обеспечение средств защиты информации, с учетом особенностей функционирования автоматизированной системы управления;

– анализ зарегистрированных событий в автоматизированной системе управления, связанных с безопасностью информации (далее - события безопасности);

– сопровождение функционирования системы защиты автоматизированной системы управления в ходе ее эксплуатации, включая ведение эксплуатационной документации и организационно-распорядительных документов по защите информации.

Для выявления инцидентов и реагирования на них осуществляются:

– определение лиц, ответственных за выявление инцидентов и реагирование на них;

– 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;

– своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в автоматизированной системе управления персоналом;

– анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;

– 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, приводящих к возникновению инцидентов;

– планирование и принятие мер по предотвращению повторного возникновения инцидентов.

В ходе управления конфигурацией автоматизированной системы управления и ее системы защиты осуществляются:

– поддержание конфигурации автоматизированной системы управления и ее системы защиты (структуры системы защиты автоматизированной системы управления, состава, мест установки и параметров настройки средств защиты информации, программного обеспечения и технических средств) в соответствии с эксплуатационной документацией на систему защиты (поддержание базовой конфигурации автоматизированной системы управления и ее системы защиты);

– определение лиц, которым разрешены действия по внесению изменений в базовую конфигурацию автоматизированной системы управления и ее системы защиты;

– регламентация и контроль технического обслуживания, в том числе дистанционного (удаленного), технических средств и программного обеспечения автоматизированной системы управления;

– управление изменениями базовой конфигурации автоматизированной системы управления и ее системы защиты, в том числе определение типов возможных изменений базовой конфигурации автоматизированной системы управления и ее системы защиты, санкционирование внесения изменений в базовую конфигурацию автоматизированной системы управления и ее системы защиты, документирование действий по внесению изменений в базовую конфигурацию автоматизированной системы управления и ее системы защиты, сохранение данных об изменениях базовой конфигурации автоматизированной системы управления и ее системы защиты, контроль действий по внесению изменений в базовую конфигурацию автоматизированной системы управления и ее системы защиты;

– анализ потенциального воздействия планируемых изменений в базовой конфигурации автоматизированной системы управления и ее системы защиты на обеспечение ее безопасности, возникновение дополнительных угроз безопасности информации и работоспособность автоматизированной системы управления;

– определение параметров настройки программного обеспечения, включая программное обеспечение средств защиты информации, состава и конфигурации технических средств и программного обеспечения до внесения изменений в базовую конфигурацию автоматизированной системы управления и ее системы защиты;

– внесение информации (данных) об изменениях в базовой конфигурации автоматизированной системы управления и ее системы

защиты в эксплуатационную документацию на систему защиты информации автоматизированной системы управления.

В ходе контроля (мониторинга) за обеспечением уровня защищенности автоматизированной системы управления осуществляются:

– контроль за событиями безопасности и действиями персонала в автоматизированной системе управления;

– контроль (анализ) защищенности информации, обрабатываемой в автоматизированной системе управления, с учетом особенностей ее функционирования;

– анализ и оценка функционирования системы защиты автоматизированной системы управления, включая выявление, анализ и устранение недостатков в функционировании системы защиты автоматизированной системы управления;

– документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности автоматизированной системы управления;

– принятие решения по результатам контроля (мониторинга) за обеспечением уровня защищенности автоматизированной системы управления о необходимости пересмотра требований к защите информации в автоматизированной системе управления и доработке (модернизации) ее системы защиты.

Обеспечение защиты информации при выводе из эксплуатации автоматизированной системы управления осуществляется оператором в соответствии с эксплуатационной документацией на систему защиты автоматизированной системы управления и организационно-распорядительными документами по защите информации и в том числе включает следующие организационные меры:

– архивирование информации, содержащейся в автоматизированной системе управления;

– уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации.

4.3 Разработка технических мер для защиты автоматизированной системы контроля и учета электроэнергии

4.3.1 Анализ технических средств для обеспечения безопасности автоматизированной системы контроля и учета электроэнергии

Для обеспечения информационной безопасности автоматизированной системы контроля и учета электроэнергии необходимо внедрить следующие технические средства:

– Установка антивирусного ПО на АРМ пользователей, находящихся на третьем уровне автоматизированной системы;

– Внедрение СЗИ от НСД;

– Внедрение программного обеспечения для создания защищенной сети.

На основе сравнительного анализа, представленного в таблице 10, было принято выбрать Kaspersky Endpoint Security [26,27].

Таблица 10 – Сравнительная таблица антивирусного ПО

Название антивирусного ПО	Файрвол	Антиспам	Проверка по расписанию	Персональные данные	Цена, руб
Kaspersky Endpoint Security	+	+	-	Не собираются	1200
Dr. Web Security Space	+	+	+	Собираются	1300

На основе сравнительного анализа, представленного в таблице 11, было принято выбрать СЗИ от НСД Secret Net 7 [12,14].

Таблица 11 – Сравнительная таблица СЗИ

Название СЗИ	Сертификаты	Применение	Цена, руб.
СЗИ от НСД Secret Net 7	– 2-й уровень контроля отсутствия НДВ; – 3-й класс защищенности СВТ	– АС до класса 1Б включительно (защита гостайны с грифом «совершенно секретно»); – ИСПДн до УЗ1	6131

		включительно; – ГИС до 1 класса включительно; – АСУ ТП до 1 класса включительно.	
(АПМДЗ) «Соболь» 4.2	2-й класс СДЗ уровня платы расширения	– АС до класса 1Б включительно (защита гостайны с грифом «совершенно секретно»); – ИСПДн до УЗ1 включительно; – ГИС до 1 класса включительно; – АСУ ТП до 1 класса включительно.	11995
	АПМДЗ класса 1Б	Информация, содержащая государственную тайну	
	НДВ2, 2-й класс СДЗ уровня платы расширения защиты	АС до класса 1Б включительно	

На основе сравнительного анализа, представленного в таблице 12, было принято выбрать VipNet CUSTOM [10,13].

Таблица 11 – Сравнительная таблица программно-аппаратных комплексов для создания защищенной сети

Название	Уровень контроля НДВ	Класс защищенности МСЭ	Класс автоматизированных систем	Шифрование данных	Цена, руб.
VipNet CUSTOM	По 3-му уровню	По 3-му классу	До 1В включительно	ГОСТ 28147-89	106 250
АПКШ «Континент 3.9»	По 2-му уровню	По 3-му классу	До 1В включительно	ГОСТ 28147-89	209 321

4.3.2 Обзор технических и программных средств комплекса VipNet CUSTOM для автоматизированной системы управления

В настоящее время в состав VipNet CUSTOM входит более 15-ти различных компонентов, позволяющих реализовать множество сценариев защиты информации в современных мультисервисных сетях связи.

VipNet Administrator (Администратор) - это базовый программный комплекс для настройки и управления защищенной сетью, включающий в себя:

– VipNet NCC (Центр Управления Сетью, ЦУС) – программное обеспечение, предназначенное для конфигурирования и управления виртуальной защищенной сетью VipNet;

– VipNet KC & CA (Удостоверяющий и Ключевой Центр, УКЦ) - программное обеспечение, которое выполняет функции центра формирования ключей шифрования и персональных ключей пользователей — Ключевого Центра, а также функции Удостоверяющего Центра.

VipNet StateWatcher (Центр мониторинга, ЦМ) – программный комплекс, который реализован по клиент-серверной технологии и предназначен для централизованного мониторинга состояния узлов защищенной сети VipNet. VipNet StateWatcher представляет собой программный сервер со стандартной SQL-базой данных состояния узлов сети, устанавливаемый совместно с ПО VipNet Client, с возможностью доступа к этим данным и результатам работы правил анализа состояния узлов через удаленный Web-доступ с использованием браузера.

Программа VipNet Publication Service (Сервис Публикации) предназначена для автоматизации процессов публикации выпущенных в УЦ VipNet сертификатов (администраторов, пользователей, кросс-сертификатов) и списков отозванных сертификатов (СОС) на точках распространения данных. Также обеспечивается импорт СОС, сформированных сторонними УЦ.

Программный комплекс VipNet Registration Point (Пункт Регистрации) предназначен для создания защищенного АРМ регистрации пользователей, хранения регистрационных данных, создания запросов на выпуск сертификатов и их обслуживание в УКЦ, а также запросов на формирование ключевых дистрибутивов пользователей сети VipNet в УКЦ.

VipNet Coordinator (Windows и Linux) – полнофункциональный программный сервер защищенной сети VipNet, устанавливаемый на ОС Linux с ядрами 2.4.2/31 -2.6.2/26 (дистрибутивы RedHat, Suse и др.) В

зависимости от настроек VipNet Coordinator может выполнять следующие функции:

– сервера IP-адресов;

– прокси-сервера защищенных соединений;

– туннелирующего сервера (криптошлюза);

– межсетевого экрана для открытых, защищенных ресурсов и туннелируемых ресурсов;

– сервера защищенной почты;

– отказоустойчивого сервера защищенной сети VipNet в конфигурации VipNet Failover.

Программный комплекс VipNet Cluster - это программное обеспечение для ОС Windows, основанное на принципах высокой доступности и распределения нагрузки. ПК VipNet Cluster способен обрабатывать сетевой трафик, поступающий из нескольких сетей, непосредственно подключенных к нему. Все элементы кластера представлены в каждой из подключенных сетей одним и тем же IP-адресом, который одновременно активен на всех элементах кластера. Это обеспечивает моментальное перераспределение функций в кластере в случае отказа одного из элементов. ПК VipNet Cluster позволяет создать инфраструктуру, которая гарантирует бесперебойность передачи данных, до тех пор, пока хотя бы один из элементов кластера работоспособен.

VipNet Coordinator HW-VPNM - программно-аппаратный, включающий в себя криптошлюз и межсетевой экран. VipNet Coordinator HW-VPNM, являясь модулем расширения для универсальных шлюзов безопасности USG2000 компании Huawei Symantec, легко инсталлируется в существующую инфраструктуру, надежно защищает передаваемую по каналам связи информацию от несанкционированного доступа и подмены.

В качестве одного из ключевых элементов управления сетью предлагается использовать VipNet Coordinator HW1000 - криптошлюз и межсетевой экран. Он легко инсталлируется в существующую

инфраструктуру, надежно защищает передаваемую по каналам связи информацию от несанкционированного доступа и подмены. Использование адаптированной ОС Linux и надежной аппаратной платформы серверов AquaServer позволяет применять VipNet Coordinator HW1000 в качестве корпоративного решения, к которому предъявляются самые жесткие требования по функциональности, удобству эксплуатации, надежности и отказоустойчивости.

Программное обеспечение создано на базе проверенного многолетней эксплуатацией ПО VipNet Coordinator Linux и технологии защиты информации VipNet. Количество одновременно установленных соединений через криптошлюз не ограничивается. Поддержка работы в современных мультисервисных сетях связи с серверами DHCP, WINS, DNS и преобразованием адресов (NAT, PAT). Использование в качестве центра генерации ключей шифрования сертифицированного ФСБ России ПО VipNet

Administrator из состава СКЗИ «Домен-КС2/КМ». Низкая стоимость по сравнению с аналогичными по возможностям СЗИ других отечественных компаний.

Программно-аппаратный комплекс (ПАК) VipNet Coordinator IG10 - сетевой шлюз безопасности в индустриальном исполнении, предназначенный для защиты каналов связи в промышленных системах и сегментирования их на защищенные объекты. VipNet Coordinator IG предназначен для обеспечения эффективной защиты от сетевых атак и несанкционированного доступа к информации путем создания защищенных каналов связи до 10 Мбит/с на основе технологии VipNet и фильтрации IP-трафика в соответствии с установленными правилами.

ПАК VipNet Coordinator IG10 предназначен для использования:

– в государственных информационных системах (ИС) до класса защищенности К1 включительно;

– в автоматизированных системах управления технологическим процессом (АСУ ТП) до класса защищенности К1 включительно;

– в информационных системах (ИС) для обеспечения 1 и 2 уровня защищенности персональных данных;

– в информационных системах (ИС), информационно-телекоммуникационных системах (ИТС) и автоматизированных системах (АСУ) критической информационной инфраструктуры (КИИ) до 1 категории значимости.

VipNet Coordinator HW1000 имеет следующие уровни сертификации:

- ИСПДн К1 / класс АС - 1В, сертификат по 3 классу МЭ, по 3 уровню НДВ;
- ФСБ России по требованиям к СКЗИ класса КС3.

VipNet Client (Клиент) — это программный комплекс для ОС Windows, выполняющий на рабочем месте пользователя или сервере с прикладным ПО функции VPN-клиента, персонального экрана, клиента защищенной почтовой системы, а также криптопровайдера для прикладных программ, использующих функции подписи и шифрования.

Базовыми компонентами VipNet CUSTOM, предлагаемыми для использования в АСКУЭ ПО VipNet Administrator, VipNet Coordinator (в разных вариантах исполнения) и VipNet Client. Эти компоненты являются основой для развертывания виртуальной частной сети и инфраструктуры открытых ключей. С целью расширения возможностей базовых компонентов могут использоваться дополнительные компоненты VipNet CUSTOM: VipNet StateWatcher и VipNet Registration Point.

«Координатор» в рамках VPN может нести различную нагрузку, выполнять разнообразные функции:

– функцию сервера-маршрутизатора, обеспечивающую маршрутизацию почтовых конвертов и управляющих сообщений при взаимодействии объектов сети между собой;

– функцию сервера IP-адресов, обеспечивающую регистрацию и предоставление информации о текущих IP-адресах и способах подключения объектов корпоративной сети;

– функцию сервера VipNet-Firewall, обеспечивающую работу защищенных компьютеров локальной сети в VPN от имени одного адреса; работу защищенных компьютеров локальной сети через другие Firewall; туннелирование пакетов в защищенное соединение от заданных адресов незащищенных компьютеров; фильтрацию открытых пакетов, в том числе и туннелируемых, в соответствии с заданной политикой безопасности (функции межсетевого экрана);

– функцию VipNet-сервера открытого Интернета, обеспечивающую организацию безопасного подключения части компьютеров локальной сети к Интернету без их физического отключения от локальной сети организации.

В состав пакетов «Координатор» и «Клиент» входят дополнительные модули, обеспечивающие защищенный обмен транспортными конвертами (файлами, сообщениями, электронной почтой) между клиентами защищенной сети. Основной транспортный модуль называется MFTP и предназначен для обеспечения надежной и безопасной передачи транспортных конвертов между узлами сети VipNet посредством протоколов TCP (канал передачи MFTP) и SMTP/POP3. При связи по каналу MFTP устанавливается TCP-соединение с узлом-получателем конвертов, проводится взаимная аутентификация узлов и осуществляется прием/передача конвертов друг для друга. При связи по каналу SMTP/POP3 транспортный модуль переадресует конверты для отправки модулю MailTrans, который передает их через сервер SMTP, а также забирает с сервера POP3 конверты, предназначенные для этого узла.

4.3.3 Обзор СЗИ от НСД Secret Net для АСКУЭ

Система Secret Net предназначена для защиты от несанкционированного доступа к информационным ресурсам компьютеров, функционирующих под управлением операционных систем MS Windows 10 и Windows Server.

Защита от несанкционированного доступа (НСД) обеспечивается комплексным применением набора защитных механизмов, расширяющих средства безопасности ОС Windows.

Система Secret Net может функционировать в следующих режимах:

– автономный режим — предусматривает только локальное управление защитными механизмами;

– сетевой режим — предусматривает локальное и централизованное управление защитными механизмами, а также централизованное получение информации и изменение состояния защищаемых компьютеров.

Основные функции, реализуемые системой Secret Net:

– контроль входа пользователей в систему;

– разграничение доступа пользователей к ресурсам файловой системы и устройствам компьютера;

– создание для пользователей ограниченной замкнутой среды программного обеспечения компьютера (замкнутой программной среды);

– разграничение доступа пользователей к конфиденциальным данным;

– контроль потоков конфиденциальной информации в системе;

– контроль вывода на печать и добавление грифов в распечатываемые документы (маркировка документов);

– контроль целостности защищаемых ресурсов;

– контроль подключения и изменения устройств компьютера;

– функциональный контроль ключевых компонентов Secret Net;

– защита содержимого дисков при несанкционированной загрузке;

– уничтожение (затирание) содержимого файлов при их удалении;

– теневое копирование выводимой информации;

– регистрация событий безопасности в журнале Secret Net;

– мониторинг и оперативное управление защищаемыми компьютерами (только в сетевом режиме функционирования);

– централизованный сбор и хранение журналов (только в сетевом режиме функционирования);

– централизованное управление параметрами механизмов защиты (только в сетевом режиме функционирования).

4.4 Технико-экономическое обоснование предложенных рекомендаций

Проведено технико-экономическое обоснование внедрения предложенных рекомендаций по использованию аппаратных и программных компонентов комплекса VipNet и СЗИ Secret Net для автоматизированной системы контроля и учета электроэнергии.

В таблице представлены результаты технико-экономического обоснования предложенных рекомендаций для автоматизированной системы контроля и учета электроэнергии на основе продуктов VipNet и Secret Net. С учётом потребностей в количестве оборудования и программного обеспечения для построения защищённых сегментов информационно-управляющей системы было подобрано оборудование и программное обеспечение, представлены цена на их приобретение и техническое сопровождение в течение 1 года. Предполагается, что в течение года соответствующие сотрудники подразделений по информационной безопасности и информационным технологиям освоят эксплуатацию оборудования и программного обеспечения и смогут самостоятельно в дальнейшем решать возникающие проблемы. В случае необходимости сотрудникам может быть оплачено обучение по соответствующим профильным курсам. Результаты технико-экономического обоснования приведены в таблице 12.

Таблица 12 – Результаты технико-экономического обоснования внедрения предложенных рекомендаций

№	Наименование продукта	Цена за ед., руб.	Единиц	Цена всего, руб.
1	Антивирусное ПО Kaspersky Endpoint Security для бизнеса на 10 устройств на срок 1 год	19 210	3	57 630
2	ПАК ViPNet Coordinator IG10 4.x	106 250	1	106 250
3	Модуль расширения 3G для ПАК ViPNet Coordinator IG	14 875	1	14 875
4	Сертификат активации сервиса прямой технической поддержки ПАК ViPNet Coordinator IG10 4.x на срок 1 год, уровень-Расширенный	108 000	1	108 000
5	ПАК ViPNet Coordinator HW100 C 4.x (+WiFi)	139 000	1	139 000
6	SC-99-4.X ViPNet StateWatcher 4.x: – Лицензия на использование ПО ViPNet StateWatcher 4.x; – Лицензия на 10 узлов мониторинга; – Лицензия на ПО ViPNet Client 4.x (КС2); – Сервис технической поддержки уровня Базовый на срок 1 год.	83 720	3	251 160
7	SC-35-КС2-4.X ViPNet Registration Point 4.x (КС2): – Лицензия на использование ПО ViPNet Registration Point 4.x (КС2); – Сервис технической поддержки уровня Базовый на срок 1 год.	21 420	1	21 420
8	SC-31-КС3-4.X - Лицензия на ПО ViPNet Administrator 4.x (КС3) - Лицензия на ПО ViPNet Client 4.x (КС3) - Сервис технической поддержки уровня (Базовый на срок 1 год)	97 350	1	97 350
9	SC-29-КС3-4.X - Лицензия на ПО ViPNet Client 4.x (КС3) - Сервис технической поддержки уровня (Базовый на срок 1 год)	5 430	30	162 900
10	Secret Net 7 Studio: – Зашита от НСД; – Контроль устройств; – Защита диска; – СОВ.	6 131	30	183 930
Итого				1 142 515

Поскольку защита критической информационной инфраструктуры является обязанностью организации, то необходимо оценить сумму затрат на приобретение оборудования, обеспечивающего требуемые характеристики защищённости. С учётом количества распределённых объектов, а также

количества сотрудников организации затраты на оборудование и его техническую поддержку составят 1 142 515 рублей.

4.5 Выводы по разделу

В данном разделе была решена четвертая задача, поставленная для достижения цели выпускной квалификационной работы, а также рассмотрены следующие вопросы:

1) разработаны организационные меры для защиты автоматизированной системы контроля и учета электроэнергии;

2) разработаны технические меры для защиты автоматизированной системы контроля и учета электроэнергии;

3) представлено технико-экономическое обоснование предложенных рекомендаций.

Для обеспечения информационной безопасности автоматизированной системы контроля и учета электроэнергии необходимо внедрить следующие технические средства:

4) установка антивирусного ПО Kaspersky Endpoint Security;

5) внедрение СЗИ от НСД Secret Net 7;

6) внедрение программно-аппаратного комплекса VipNet CUSTOM.

С учётом количества распределённых объектов, а также количества сотрудников организации затраты на оборудование и его техническую поддержку составят 1 142 515 рублей.

Заключение

В данной выпускной квалификационной работе разработаны рекомендации по обеспечению безопасности автоматизированной системы контроля и учета электроэнергии.

По итогам первого раздела было выявлено, что большинство автоматизированных систем контроля и учета электроэнергии делятся на 3 уровня:

1) уровень измерения;
2) информационно-измерительный комплекс;
3) информационно-вычислительный комплекс.

В ходе анализа технических каналов передачи данных и классификации информации, обрабатываемой в различных элементах автоматизированной системы контроля и учета электроэнергии было выявлено, что в данной системе присутствует информация ограниченного доступа, такая как: личная информация пользователей, показания счетчиков, информация о состоянии электрической сети и прочее.

В ходе анализа актуальных угроз безопасности автоматизированной системы контроля и учета электроэнергии выявлено, что наиболее уязвимыми местами являются канал связи и персонал, работающий с документами, информацией и базами данных.

В рамках четвертого раздела были разработаны организационные и технические меры по обеспечению информационной безопасности автоматизированной системы контроля и учета электроэнергии. С учётом количества распределённых объектов, а также количества сотрудников организации затраты на оборудование и его техническую поддержку составят 1 142 515 рублей.

Задачи, поставленные для достижения цели, выполнены:

– выполнен анализ существующих автоматизированных систем контроля и учета электроэнергии;

– выполнен анализ информационных потоков в автоматизированных системах контроля и учета электроэнергии;

– выполнен анализ угроз и уязвимостей информации в АСКУЭ;

– разработаны рекомендации по нейтрализации актуальных угроз в автоматизированной системе контроля и учета электроэнергии.

Разработанные рекомендации позволяют повысить уровень информационной безопасности в автоматизированной системе контроля и учета электроэнергии до допустимых значений.

Теоретическая значимость работы заключается в том, что в ней приведено достаточно объемный материал по теме данной выпускной квалификационной работы, вся информация систематизирована.

Практическая ценность работы заключается в том, что разработанные рекомендации можно в дальнейшем применять не только для продолжения исследований по данной теме, но и для решения проблем связанных с защитой данных, хранящихся и обрабатываемых в автоматизированной системе контроля и учета электроэнергии.

Список использованных источников

1 Автоматизированная система контроля и учёта энергоресурсов [Электронный ресурс], – https://ru.wikipedia.org/wiki/%D0%90%D0%B2%D1%82%D0%BE%D0%BC%D0%B0%D1%82%D0%B8%D0%B7%– (дата обращения 26.04.2020).

2 Автоматизированная система учета электроэнергии «Мираж». [Электронный ресурс], – https://www.nppstels.ru/products/asd/mirazh-gsm-sd-02/ – (дата обращения 03.05.2020).

3 Автоматизированная система учета электроэнергии «Стриж» на базе LPWAN-технологии. [Электронный ресурс], – https://strij.tech/portfolio/resheniya/gkh/askue/ – (дата обращения 05.05.2020).

4 Автоматизированная система учета электроэнергии «Стриж» на базе LPWAN-технологии. Продукция. [Электронный ресурс], – https://strij.tech/products// – (дата обращения 05.05.2020).

5 Автоматизированная система коммерческого учета электроэнергии «Энергомера». Продукция. [Электронный ресурс], – http://www.energomera.ru/ru/products – (дата обращения 07.05.2020).

6 Автоматизированная система коммерческого учета электроэнергии «Энергомера». [Электронный ресурс], – http://www.energomera.ru/ru/products/askue/about/ – (дата обращения 07.05.2020).

7 Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008 г. – 69 с.

8 Банк данных угроз безопасности информации ФСТЭК. [Электронный ресурс], – https://bdu.fstec.ru/threat – (дата обращения 15.05.2020).

9 Галатенко В.А. Стандарты информационной безопасности: Курс лекций. – М.: ИНТУИТ, 2013. – 253 с.

10 ИнфоТеКС. VipNet CUSTOM. [Электронный ресурс], – https://infotecs.ru/product/– (дата обращения 02.05.2020).

11 Исследование проблемы информационной безопасности АСКУЭ. [Электронный ресурс], – https://cyberleninka.ru/article/n/issledovanie-problemy-informatsionnoy-bezopasnosti-askue – статья в интернете.

12 Код безопасности. Secret Net 7. [Электронный ресурс], – https://www.securitycode.ru/products/secret_net/ – (дата обращения 17.05.2020).

13 Код безопасности. АПКШ «Континент» 3.9. [Электронный ресурс], – https://www.securitycode.ru/company/events/apksh-kontinent-3-9-bystree-udobnee-bezopasnee/ – (дата обращения 17.05.2020).

14 Код безопасности. Соболь. [Электронный ресурс], – https://www.securitycode.ru/products/pak_sobol/ – (дата обращения 21.05.2020).

15 Молочков В.П. Компьютерные сети – СПб.: «Издательство Полигон», 2010. – 320 с.

16 Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. – СПб.: Питер, 2014. – 672 с.

17 Приказ ФСТЭК России от 14 марта 2014 г. N 31

18 Семёнов Ю.А. Алгоритмы и протоколы каналов и сетей передачи данных: учебное пособие.-М.: Издательство БИНОМ, 2010 г.-254 с.

19 Счетчики «Инфотекс Меркурий» [Электронный ресурс], – https://www.incotexcom.ru/support/docs#tab1 – (дата обращения 10.05.2020).

20 Федеральный закон РФ «Об информации, информационных технологиях и о защите информации» №149-ФЗ от 27.07.2006

21 Федеральный закон РФ «О персональных данных» №152-ФЗ от 27.07.2006

22 Хогдал В.И., Анализ и диагностика компьютерных сетей – М.: Издательство ИПКИР, 2011г. – 378с.

23 Чекмарев Ю. В., Локальные вычислительные сети. – М.: ДМК Пресс, 2010. – 200 с.

24 Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие. – М.: ИД «ФОРУМ»: ИНФРА-М, 2011. – 416 с.

25 Ярочкин В.И. Информационная безопасность: Учебник для вузов. - М.: Академический проект; Фонд «Мир», 2003. - 640 с.

26 Dr. Web для бизнеса [Электронный ресурс], – https://promotions.drweb.ru/promo/migrate/v2/ – (дата обращения 19.05.2020).

27 Kaspersky Endpoint Security для бизнеса [Электронный ресурс], – https://store-kaspersky.ru/dlya_biznesa/ – (дата обращения 19.05.2020).

28 Saures – учет и контроль коммунальных ресурсов. [Электронный ресурс], – https://www.saures.ru/– (дата обращения 12.05.2020).

29 Saures – учет и контроль коммунальных ресурсов Продукция. [Электронный ресурс], – https://www.saures.ru/katalog/ (дата обращения 12.05.2020).

Приложение А

Положение по работе с инцидентами информационной безопасности

ООО УК «Развитие»

г. Москва

30.04.2020

УТВЕРЖДАЮ
Директор ООО УК «Развитие»
В. М. Ефимов
30.04.2020

ОКУД 0209369

ПОЛОЖЕНИЕ

по работе с инцидентами информационной безопасности

Аннотация

Настоящее Положение разработано в целях организации работы с инцидентами информационной безопасности в управляющей компании города Москва ООО УК «Развитие».

Инцидент – одно событие или группы событий, которые могут привести к сбоям или нарушению функционирования информационной системы (далее – ИС) и (или) к возникновению угроз безопасности информации, в том числе персональных данных.

1. Общие положения

Положение о работе с инцидентами информационной безопасности (далее – Положение) разработано в соответствии с:

1) Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

2) Федеральным законом Российской Федерации от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

3) Постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных

данных»;

4) Приказом ФСТЭК России от 14 марта 2014 года № 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»;

5) политикой обработки персональных данных субъектов ООО УК «Развитие».

Работа с инцидентами в области информационной безопасности помогает определить наиболее актуальные угрозы информационной безопасности и создает обратную связь в системе обеспечения информационной безопасности, что способствует повышению общего уровня защиты информационных ресурсов и информационных систем.

Работа с инцидентами включает в себя следующие направления:

1) определение лиц, ответственных за выявление инцидентов и реагирование на них;

2) обнаружение, идентификация и регистрация инцидентов;

3) своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами;

4) анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а так же оценка их последствий;

5) принятие мер по устранению последствий инцидентов;

6) планирование и принятие мер по предотвращению повторного возникновения инцидентов.

Для анализа инцидентов, в том числе определения источников и причин возникновения инцидентов, а также оценки их последствий; планирования и принятия мер по предотвращению повторного

возникновения инцидентов, назначается постоянно действующая комиссия по работе с инцидентами в соответствии с приказом директора.

2. Ответственные за выявление инцидентов и реагирование на них

2.1. В информационных системах.

Ответственными за выявление инцидентов в ИС являются:

1) лица, имеющие право доступа к ИС;

2) ответственный за техническое обслуживание ИС;

3) администратор ИС;

4) администратор информационной безопасности ИС.

Ответственными за реагирование на инциденты в ИС являются:

1) лица, имеющих право доступа к ИС;

2) руководитель подразделения ООО УК «Развитие», в котором выявлен инцидент;

3) ответственный за техническое обслуживание ИС;

4) администратор ИС;

5) администратор информационной безопасности ИС;

6) ответственный за организацию обработки персональных данных в ООО УК «Развитие», в случае, если ИС является информационной системой персональных данных (далее - ИСПДн);

7) председатель комиссии по работе с инцидентами.

2.2. Вне информационных систем.

Ответственными за выявление инцидентов вне ИС являются все сотрудники ООО УК «Развитие».

Ответственными за реагирование на инциденты вне ИС являются:

1) сотрудник, обнаруживший инцидент;

2) руководитель подразделения, в котором выявлен инцидент;

3) ответственный за организацию обработки персональных данных в ООО УК «Развитие», в случае, если существует угроза безопасности персональных данных;

4) председатель комиссии по работе с инцидентами.

3. Обнаружение, идентификация и регистрация инцидентов

3.1. Работа по обнаружению инцидентов в области информационной безопасности включает в себя мероприятия, направленные на:

1) выявление инцидентов в области информационной безопасности с помощью технических средств;

2) выявление инцидентов в области информационной безопасности в ходе контрольных мероприятий;

3) выявление инцидентов с помощью сотрудников.

3.2. Работа по идентификации инцидентов в области информационной безопасности включает в себя мероприятия, направленные на доведение до сотрудников информации, позволяющей идентифицировать инциденты.

3.3. Регистрацию инцидентов осуществляет председатель комиссии по работе с инцидентами в журнале регистрации инцидентов информационной безопасности. Форма журнала утверждается приказом директора.

3.4 Хранение журнала осуществляется в местах, исключающих доступ к журналу посторонних лиц. Журнал хранится в течение 5 лет после завершения ведения. Ответственный за хранение и ведение журнала – председатель комиссии по работе с инцидентами.

4. Информирование о возникновении инцидентов

Сотрудник (пользователь ИС), обнаруживший инцидент в ИС, должен незамедлительно, любым доступным способом, сообщить об инциденте непосредственному руководителю, администратору ИС, администратору информационной безопасности ИС, ответственному за организацию обработки персональных данных в ООО УК «Развитие» (в случае если ИС является ИСПДн), председателю комиссии по работе с инцидентами.

Администратор ИС, в случае необходимости, информирует пользователей ИС о возникновении инцидента и дает указания по дальнейшим действиям.

5. Анализ инцидентов, а также оценка их последствий

Анализ инцидентов, в том числе определение источников и причин

возникновения инцидентов, а также оценку их последствий осуществляет комиссия по работе с инцидентами информационной безопасности.

5.1. Источниками и причинами возникновения инцидентов в области информационной безопасности являются:

1) действия организаций и отдельных лиц враждебные интересам ООО УК «Развитие»;

2) отсутствие персональной ответственности сотрудников и их руководителей за обеспечение информационной безопасности, в том числе персональных данных;

3) недостаточная работа с персоналом по обеспечению необходимого режима соблюдения конфиденциальности, в том числе персональных данных;

4) отсутствие дисциплинарной мотивации соблюдения правил и требований информационной безопасности;

5) недостаточная техническая оснащённость подразделений, ответственных за обеспечение информационной безопасности;

6) совмещение функций по разработке и сопровождению или сопровождению и контролю за информационными системами;

7) наличие привилегированных бесконтрольных пользователей в информационной системе;

8) пренебрежение правилами и требованиями информационной безопасности сотрудниками;

9)и другие причины.

5.2. Оценка последствий инцидента производится на основании потенциально возможного или фактического ущерба.

6. Принятие мер по устранению последствий инцидентов

Меры по устранению последствий инцидентов включает в себя мероприятия, направленные на:

1) определение границ инцидента и ущерба от реализации угроз информационной безопасности;

2) ликвидацию последствий инцидента и полное либо частичное возмещение ущерба.

7. Планирование и принятие мер по предотвращению инцидентов

7.1. Планирование и принятие мер по предотвращению возникновения инцидентов осуществляет комиссия по работе с инцидентами информационной безопасности и основывается на:

1) планомерной деятельности по повышению уровня осознания информационной безопасности руководством и сотрудниками;

2) проведении мероприятий по обучению сотрудников правилам и способам работы со средствами защиты информационных систем;

3) доведении до сотрудников норм законодательства, внутренних документов ООО УК «Развитие», устанавливающих ответственность за нарушение требований информационной безопасности;

4) разъяснительной работе с увольняющимися сотрудниками и сотрудниками, принимаемыми на работу;

5) своевременной модернизации системы обеспечения информационной безопасности, с учетом возникновения новых угроз информационной безопасности, либо в случае изменения требований руководящих документов по организации обеспечения информационной безопасности

6) своевременном обновлении программного обеспечения, в том числе баз сигнатур антивирусных средств.

7.2. Работа с персоналом.

Как правило, самым слабым звеном в любой системе безопасности является человек. Поэтому работа с персоналом является основным направлением деятельности по обеспечению требований информационной безопасности.

В работе с персоналом основной упор должен делаться не на наказание сотрудника за нарушения в области информационной безопасности, а на поощрение за надлежащие выполнение требований информационной

безопасности, проявление личной инициативы в укреплении системы информационной безопасности.

Сотрудники являются важным источником сведений об инцидентах информационной безопасности, поэтому необходимо донести до них информацию о том, что оперативно предоставленные сведения об инциденте информационной безопасности являются основанием для смягчения либо отмены наказания за нарушение требований информационной безопасности.

Начальник отдела информационной
безопасности, сетей передачи данных
и вычислительных ресурсов Н.О. Степанян

Юрист ООО УК «Развитие»
Н.Е. Радимов
30.04.2020

Приложение Б

ООО УК «Развитие»

ПРИКАЗ

20.04.2020 №13

г. Москва

О журнале регистрации инцидентов информационной безопасности

В соответствии с требованиями «Положения по работе с инцидентами информационной безопасности» ООО УК «Развитие», в целях обеспечения требуемого режима информационной безопасности

ПРИКАЗЫВАЮ:

1. Утвердить форму журнала регистрации инцидентов информационной безопасности, указанную в Приложении.

2. Регистрировать в журнале все инциденты информационной безопасности.

3. При выявлении инцидентов информационной безопасности вносить в журнал следующую информацию:

1) фамилия, имя, отчество, должность, структурное подразделение сотрудника обнаружившего инцидент;

2) дата выявления инцидента;

3) описание инцидента;

4) принятые меры по устранению последствий инцидента;

5) причины возникновения инцидента;

6) размер потенциально-возможного ущерба;

7) размер фактического ущерба;

8) принятые меры по предотвращению повторного возникновения инцидента.

5. Назначить ответственным за ведение и сохранность журнала

заместителя директора по информатизации М.И. Фоминов.

6. Хранение журнала осуществлять в местах, исключающих доступ к журналу посторонних лиц.

7. Хранить журнал в течение 5 лет после завершения ведения.

8. Контроль за выполнением настоящего приказа оставляю за собой.

Директор ООО УК «Развитие» В. М. Ефимов

Юрист ООО УК «Развитие»
Н.Е. Радимов
20.04.2020

С приказом ознакомлен:
Секретарь-референт М.А. Марьин