«Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И.Ульянова (Ленина)»
(СПбГЭТУ «ЛЭТИ»)

Специальность	10.05.01 – «Компьютерная безопасность»
Специализация	Информационная безопасность объектов информатизации на базе компьютерных систем
Факультет	ФКТИ
Кафедра	Информационная безопасность

К защите допустить

Зав. кафедрой Воробьев Е.Г.

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА СПЕЦИАЛИСТА

Тема: ЗАЩИЩЕННАЯ СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ НА ОСНОВЕ ВСТРОЕННЫХ УСТРОЙСТВ

Студент		_____ *подпись*	Левшун Д.С.
Руководитель	*(к.т.н., доцент)*	_____ *подпись*	Воробьев Е.Г.
Консультант	*(к.т.н., с.н.с.)*	_____ *подпись*	Чечулин А.А.
Консультант	*(ст. преп.)*	_____ *подпись*	Лебедева Т.Н.

Санкт-Петербург

2017

ЗАДАНИЕ
НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ РАБОТУ

Утверждаю
Зав. кафедрой ИБ
_____ Воробьев Е.Г.
«___»_____2017 г.

Студент Левшун Д.С. Группа 1362

Тема работы: Защищенная система контроля и управления доступом на основе встроенных устройств.

Место выполнения ВКР: Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации РАН.

Исходные данные (технические требования):

система контроля и управления доступом; требования к системе контроля и управления доступом (функциональные и не функциональные).

Содержание ВКР:

1) обзор и анализ существующих решений и отдельных компонентов; 2) основные требования к системе; 3) методики оценки системы; 4) прототип системы и основные алгоритмы его работы; 5) эксперименты и анализ результатов.

Перечень отчетных материалов: пояснительная записка, иллюстративный материал, копии публикаций по теме ВКР, свидетельства о регистрации программ ЭВМ и баз данных, акт о внедрении.

Дополнительные разделы: экономическое обоснование.

Дата выдачи задания
«___»_____20__ г.

Дата представления ВКР к защите
«___»_____20__ г.

Студент _____ Левшун Д.С.
подпись

Руководитель *(к.т.н., доцент)* _____ Воробьев Е.Г.
подпись

Консультант *(к.т.н., с.н.с.)* _____ Чечулин А.А.
подпись

КАЛЕНДАРНЫЙ ПЛАН ВЫПОЛНЕНИЯ
ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ

Утверждаю
Зав. кафедрой ИБ
_____ Воробьев Е.Г.
«___»_____20___ г.

Студент Левшун Д.С. Группа 1362

Тема работы: Защищенная система контроля и управления доступом на основе встроенных устройств

№ п/п	Наименование работ	Срок выполнения
1	Обзор и анализ существующих решений и отдельных компонентов для построения системы контроля и управления доступом	26.09 – 19.10
2	Требования к защищенной системе контроля и управления доступом	20.10 – 31.10
3	Методики оценки систем на основе встроенных устройств	01.11 – 14.11
4	Прототип защищенной системы контроля и управления доступом и основные алгоритмы его работы	15.11 – 30.11
5	Описание проводимых экспериментов	01.12 – 25.12
6	Оформление пояснительной записки	11.01 – 21.01
7	Оформление иллюстративного материала	24.01 – 31.01

Студент _____ Левшун Д.С.
подпись

Руководитель *(к.т.н., доцент)* _____ Воробьев Е.Г.
подпись

Консультант *(к.т.н., с.н.с.)* _____ Чечулин А.А.
подпись

РЕФЕРАТ

Пояснительная записка 103 стр., 16 рис., 17 табл., 55 ист., 11 прил.

Ключевые слова и словосочетания: кибер-физические системы, системы защиты, безопасность встроенных устройств, безопасность распределенных систем, процесс корреляции событий безопасности.

Объектом исследования и разработки является защищенная система контроля и управления доступом на основе встроенных устройств.

Цель работы – повышение уровня защищенности организации за счет повышение уровня защищенности систем контроля и управления доступом и расширения их функциональности.

В работе предлагается разработка прототипа защищенной системы контроля и управления доступом на основе встроенных устройств. Защищенность прототипа системы обусловлена применением современных моделей и методик комбинирования средств защиты встроенных устройств. Функциональность систем контроля и управления доступом расширена за счет применения агентов рабочих станций для мониторинга состояния сеанса пользователя с операционной системой. Работа содержит обзор и анализ существующих решений и отдельных компонентов для построения системы контроля и управления доступом, требования к защищенной системе контроля и управления доступом, методики оценки систем на основе встроенных устройств и результаты оценки разрабатываемой системы, архитектуру, основные алгоритмы работы и компонентный состав прототипа системы, результаты экспериментов, а также технико-экономическое обоснование.

ABSTRACT

This research is devoted to development of the secure access control system based on embedded devices. Enhancing of access control systems self-security can be achieved by the usage of advanced models and techniques for combining of protection components of embedded devices. Improving of access control systems functionality can be achieved by unification of physical and cybernetic security events processing. In particular, this research contains existing solutions and individual components for building access control system were reviewed and analyzed. The requirements to the access control system were formulated, as well as, components for constructing the access control system through the application of combining methods were selected. In addition, the architecture of the system was developed, interaction of the access control system architecture elements was described, and system performance was obtained experimentally.

СОДЕРЖАНИЕ

ОПРЕДЕЛЕНИЯ, ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

В настоящей пояснительной записке применяют следующие термины с соответствующими определениями:

АС – аппаратное средство.

ВУ – встроенное устройство.

ВКР – выпускная квалификационная работа.

ИСПДн – информационная система персональных данных.

ПДн – персональные данные.

СКЗИ – средство криптографической защиты информации.

СУПО – создать, удалить, посмотреть, обновить.

ФИПС – Федеральный институт промышленной собственности.

ФСБ – Федеральная служба безопасности Российской Федерации.

ФСТЭК – Федеральная служба по техническому и экспортному контролю Российской Федерации.

ЭВМ – электронно-вычислительная машина.

API – Application Programming Interface.

CRUD – Create, Read, Update, Delete.

DDoS – Distributed Denial of Service.

HTTP – HyperText Transfer Protocol.

HTTPS – HyperText Transfer Protocol Secure.

IP – Internet Protocol.

RFID – Radio Frequency IDentification.

SOAP – Simple Object Access Protocol.

TCP – Transmission Control Protocol.

UML – unified modeling language.

Wi-Fi – Wireless Fidelity.

ВВЕДЕНИЕ

В настоящее время встроенные устройства получают все большее распространение в самых разных областях приложения − в системах управления и контроля на транспорте, в системах управления производственным процессом, системах, предоставляющих телекоммуникационные сервисы потребителям, в системах имплантируемых медицинских устройств для контроля жизненно важных показаний организма человека, в электроэнергетике, в системах обеспечения физической безопасности помещений, прикладных системах распознавания речи и др.

Критически важный характер таких систем, а также высокая степень взаимодействия встроенного устройства с другими элементами программно-аппаратного окружения и пользователями системы обуславливает важность разработки механизмов защиты таких устройств от угроз информационной безопасности.

При этом в существующих системах контроля и управления доступом, средства защиты внедряются уже после этапа разработки системы. А это значит, что средства защиты формируют защитную оболочку системы, преодолев которую, злоумышленник получит полный контроль, а значит, сможет делать с системой все что угодно.

Целью выпускной квалификационной работы является разработка защищенной системы контроля и управления доступом. При этом достижение поставленной цели будет осуществляться в рамках комплексного подхода к обеспечению безопасности, который заключается не только в объединении событий физического и кибернетического уровней в рамках единой системы, но и в учете уже на этапе разработки необходимости обеспечения защищенности системы к атакам на нее.

Разрабатываемый прототип защищенной системы контроля и управления доступом может быть полезен для организаций, занимающихся разработкой и внедрением систем контроля и управления доступом. Применение

решений задач, поставленных в дипломном проекте, позволит повысить защищенность уже существующих систем контроля и управления доступом, а также расширить их функциональность, тем самым повышая защищенность организации в целом.

Кроме того, подход к разработке защищенных систем, на основе которого разрабатывается прототип защищенной системы контроля и управления доступом, а также объединение источников событий физического и кибернетического уровней в рамках системы контроля и управления доступом можно использовать в обучающих и исследовательских целях в области информационной безопасности, интернета вещей и встроенных устройств.

1. ТЕХНИКО-ЭКОНОМИЧЕСКОЕ ОБОСНОВАНИЕ

В настоящее время наблюдается стремительное развитие информационных систем с разнообразными встроенными устройствами и их внедрения в существующую инженерно-техническую инфраструктуру объектов производства, энергетики, медицины, контроля и управления на транспорте, объектов кибер-физической безопасности помещений. Помимо усложненной информационной составляющей, бизнес-логика таких систем все в большей степени оказывается завязанной на элементы физического уровня: извещатели, оповещатели и датчики, а также внешние электронные компоненты (силовые приводы, считыватели, устройства вывода звуковых и световых сигналов), одноплатные компьютеры или микроконтроллеры с низким энергопотреблением.

1.1. Техническое обоснование

Под встроенным устройством понимается электронное устройство с ограниченным набором узкоспециализированных функций в системе, работающее, как правило, на стыке программно и аппаратного уровней системы. Такие устройства предназначены для организации информационного беспроводного и проводного обмена с объектами технического окружения системы и пользовательского интерфейса: RFID-сканеры, пульты управления, речевые анализаторы. Кроме того, встроенные устройства могут быть использованы для предварительной обработки данных от извещателей, оповещателей и датчиков, а также внешних электронных компонентов, связи с базами данных и серверами приложений.

К ключевым особенностям встроенных устройств, влияющим существенным образом на процесс выбора отдельных компонентов и их интеграции в систему можно отнести повышенные требования к энергопотреблению устройств и возможностям их автономной работы, производительности и быстродействию, физическим характеристикам и мобильности устройств,

поддерживаемым API и драйверам, совместимости устройств и их компонентов, а также стоимости.

1.1.1. Требования к системе контроля и управления доступом

Система должна осуществлять управление доступом в определенном здании (кого пускать, в какое время пускать, в какое помещение пускать), включая: ограничение доступа в заданное помещение и идентификацию лица, имеющего доступ в заданное помещение. При этом пользователь системы может находиться в одном из четырёх состояний (таблица 1).

Таблица 1 – Возможные состояния пользователя

Состояние	Описание
S_1	пользователь вошел в помещение
S_2	пользователь авторизовался на рабочем месте (начало сеанса работы с операционной системой)
S_3	пользователь завершил сеанс работы с операционной системой
S_4	пользователь покинул помещение

Вход пользователя в помещение или выход пользователя из помещения идентифицируется приложением бесконтактной карты к считывателю, который подсоединен к встроенному устройству. В ситуациях, когда пользователь не приложил карту, открытие двери идентифицируется переходом кнопки из зажатого состояния в свободное и/или инфракрасным датчиком движения. Как только установлено, что человек вошел в помещение или вышел из него, запускается обратный отсчет – время, за которое пользователю необходимо авторизоваться в системе при помощи карты. На основе уникальных данных карты, формируется специальный запрос к центральному серверу управления доступом для получения информации о наличии или отсутствии доступа к помещению у пользователя карты. Встроенное устройство, получив ответ от центрального сервера управления доступом, начинает обработку

полученной информации. Результат проверки карты пользователя сопровождается открытием замка, выводом текстовой информации на экран, световым и звуковым сигналом. Также результат работы встроенного устройства направляется на сервер журналирования. Информация о состоянии сеанса работы пользователя с операционной системой также направляется на сервер журналирования.

Для поддержания системы контроля и управления доступом, необходимо управление информацией базы данных центрального сервера управления доступом. Любое изменение информации, содержащейся в базе данных, осуществляется пользователем с правами администратора, и отражается на работе системы в целом. Поэтому результаты каждого действия администратора направляются на сервер журналирования.

Встроенное устройство должно осуществлять работу в локальной сети системы по беспроводному каналу передачи данных. Это необходимо для защиты от физического воздействия на канал передачи данных между микроконтроллером и центральным сервером управления (например, повреждение Ethernet-кабеля), а так же для существенного снижения стоимости установки системы.

Встроенное устройство должно поддерживать интерфейс для взаимодействия с удалённым сервером приложений. Это необходимо для удобства интеграции встроенного устройства в общую систему контроля и управления доступом. Взаимодействие с сервером приложений может осуществляется по HTTP, HTTPS, SOAP. Данные, передаваемые по HTTP и SOAP, должны быть предварительно зашифрованы.

Для взаимодействия с центральным сервером управления доступом, встроенное устройство должно поддерживать запуск приложений, разработанных на одном из высокоуровневых языков программирования (Java, C++, Python).

Разрабатываемое встроенное устройство должно поддерживать аварийный режим работы. Под аварийным режимом работы рассматривается

ситуация, при которой обмен данными между встроенным устройством и центральным сервером управления доступом перестает быть возможным (отсутствие соединения с сервером, отказ в обслуживании на стороне сервера и т.п.). При аварийном режиме работы, решение о предоставлении пользователю доступа в помещение принимается на основе локальной базы данных, расположенной на встроенном устройстве. Локальная база данных представляет собой резервную копию сетевой базы данных доступа и содержит информацию об администраторах системы. Таким образом, при аварийном режиме работы, доступ в помещение может получить только сотрудник с правами администратора. При этом разрабатываемое встроенное устройство должно обладать объемом памяти, достаточным для хранения и поддержи локальной базы данных.

Также, встроенное устройство должно предоставлять веб-интерфейс для управления встроенным устройством при локальном Ethernet подключении. Данный веб-интерфейс должен содержать внутренний журнал встроенного устройства и инициализацию резервного копирования сетевой базы данных доступа. Таким образом, функциональные требования могут быть сведены в общее представление (таблица 2).

В случае выхода из строя электрической цепи, к которой подсоединено встроенное устройство, обеспечение энергией выполняет источник резервного питания. В подобной ситуации, функционирование встроенного устройства не нарушается, но максимально возможное время работы встроенного устройства зависит от емкости источника и количества потребляемой им энергии. Таким образом, при выборе устройства (здесь под устройством понимается набор компонент, позволяющий при совместной работе достичь заданных функциональных и нефункциональных требований), предпочтение следует отдавать тому, у которого энергоэффективность выше.

Встроенное устройство представляет собой микроконтроллер, снабженный множеством сенсоров, компонентов управления, связи и периферии. Стоимость устройства рассчитывается комплексно: учитывается микро-

контроллер со всем множеством компонент. Таким образом, предпочтение следует отдавать тому устройству, итоговая стоимость которого будет ниже.

Таблица 2 – Функциональные требования к встроенному устройству

Функциональные требования	Описание
к аппаратному обеспечению	Поддержка взаимодействия с внешними электронными компонентами: механическими замками, сканерами бесконтактных карт технологии RFID, инфракрасными датчиками движения, устройствами вывода текстовой, звуковой информации, звуковых и световых сигналов.
	Поддержка беспроводного канала передачи данных.
	Поддержка передачи данных через Ethernet.
к программному обеспечению	Поддержка обмена данными по HTTP, HTTPS, SOAP.
	Поддержка запуска приложений, написанных на Java, Python, C++.
	Поддержка и хранение локальной резервной копии базы данных.
	Поддержка шифрования данных, передаваемых по каналам передачи данных.
	Поддержка управления встроенным устройством через веб-интерфейс при локальном Ethernet подключении.

Предполагается, что устройство будет располагаться в непосредственной близости от входа в помещение. Устройство должно обладать соответствующими размерами, позволяющими поместить его на малой площади. Наименьшей поверхностью, в данной ситуации, обладает дверь. Таким обра-

зом, при встраивании в дверь, устройство должно быть не толще трех сантиметров, при условии, что наиболее распространённая толщина двери четыре сантиметра. Отметим, что толщиной менее трех сантиметров обладает большая часть популярных микроконтроллеров. Таким образом, нефункциональные требования могут быть сведены в едином представлении (таблица 3).

Таблица 3 – Нефункциональные требования к встроенному устройству

Нефункциональные требования	Описание
к энергоэффективности	Поддержка функционирования встроенного устройства в условиях выхода из строя электрической цепи, к которой подсоединено встроенное устройство, за счёт энергии резервного источника питания.
к стоимости	Минимизация стоимости микроконтроллера, расширений микроконтроллера, сенсоров и периферии, необходимых для соответствия функциональным требованиям.
к занимаемому пространству	Минимизация размеров микроконтроллера, расширений микроконтроллера, сенсоров и периферии, таким образом, чтобы толщина встроенного устройства не превышала толщины двери.

1.1.2. Краткое техническое описание системы

Разрабатываемый прототип системы контроля и управления доступом может быть использована для контроля входа в помещения и выхода из помещений сотрудников и гостей организации; обнаружения попыток несанкционированного доступа в защищаемое помещение; мониторинга начала и завершения сеанса сотрудников с операционной системой ЭВМ; обнаруже-

ния попыток несанкционированного доступа к операционной системе ЭВМ; учета времени прихода и ухода сотрудников с работы; журналирования событий, происходящих в системе, для дальнейшего анализа и обработки.

При этом гибкие настройки системы позволят регистрировать в системе, а также удалять из нее встроенные устройства, ответственные за контроль доступа в защищаемые помещения; обновлять или изменять информацию о встроенных устройствах, зарегистрированных в системе; учитывать в системе временную неработоспособность встроенных устройств в связи с ремонтом или техническим обслуживанием; вносить в систему или удалять из нее данные бесконтактных смарт-карт, выдаваемых гостям и сотрудникам организации; регистрировать в системе сотрудников и гостей организации; удалять из системы уволенных сотрудников; учитывать в системе длительное отсутствие сотрудников, связанное с отпусками, командировками или больничными; регулировать политику доступа в помещения, основываясь на должности сотрудника, а также отделе, в котором он работает; регулировать доступ сотрудников к настройкам системы, основываясь на отделе, в котором работает сотрудник, а также его должности.

1.2. Экономическое обоснование

Целью выпускной квалификационной работы является разработка прототипа защищенной системы контроля и управления доступом. При этом достижение поставленной цели будет осуществляться в рамках комплексного подхода к обеспечению безопасности, который заключается не только в объединении событий физического и кибернетического уровней в рамках единой системы, но и в учете уже на этапе разработки необходимости обеспечения защищенности системы к атакам на нее.

1.2.1. Конкурентные преимущества

Новизна предлагаемых в проекте решений достигается за счет использования современных моделей и методик комбинирования средств защиты

встроенных устройств непосредственно на этапе разработки системы контроля и управления доступом, что позволяет учитывать применение средств защиты системы уже на этапах проектирования и разработки, обуславливая ее защищенность. Кроме того, в разрабатываемой системе использован современный подход к процессу корреляции событий безопасности, позволяющего одновременно учитывать события физического и кибернетического уровней. Что позволит снизить риски, связанные с проведением киберфизических атак, за счет автоматического формирования инцидентов и определения сценариев атак и аномальной активности, выявление которых при использовании существующих систем контроля и управления доступом возможно только на этапе расследования.

Также, в разрабатываемой системе используется модульный подход при построении архитектуры системы контроля и управления доступом, который обеспечит масштабируемость и гибкость системы. Что позволит системе работать с неограниченным количеством встроенных устройств, а внедрение дополнительного функционала свести к разработке соответствующего аппаратного или программного модуля, без внесения изменений в архитектуру системы.

Таким образом, основными конкурентными преимуществами разрабатываемого прототипа системы являются:

- защищенность системы от атак на нее;
- модульная архитектура;
- объединение источников событий физического и кибернетического уровней.

1.2.2. Область применения

Разрабатываемый прототип защищенной системы контроля и управления доступом может быть полезен для организаций, занимающихся разработкой и внедрением систем контроля и управления доступом. Применение решений задач, поставленных в дипломном проекте, позволит повысить за-

щищенность уже существующих систем контроля и управления доступом, а также расширить их функциональность, тем самым повышая защищенность организации в целом.

Кроме того, подход к разработке защищенных систем, на основе которого разрабатывается прототип защищенной системы контроля и управления доступом, а также объединение источников событий физического и кибернетического уровней в рамках разрабатываемой системы можно использовать в обучающих и исследовательских целях в области информационной безопасности, интернета вещей и встроенных устройств.

1.3. Постановка задачи

Целью данной выпускной квалификационной работы является повышение уровня защищенности организации за счет решения двух задач: (1) повышения уровня защищенности систем контроля и управления доступом, а также (2) расширения их функциональности. Решение поставленных задач будет осуществляться в рамках комплексного подхода к обеспечению безопасности. Отметим, что комплексность подхода заключается не только в объединении событий физического и кибернетического уровней. Не менее важным является учет уже на этапе разработки системы необходимости обеспечения защищенности такой системы к атакам на нее.

Отметим, что для решения поставленных задач, необходимо решить следующие подзадачи:

- обзор и анализ существующих решений и отдельных компонентов для построения системы контроля и управления доступом;
- постановка требований к защищенной системе контроля и управления доступом на основе встроенных устройств;
- обзор, анализ и выбор эффективных методик оценки систем на основе встроенных устройств;
- разработка прототипа защищенной системы контроля и управления доступом на основе встроенных устройств;

- описание основных алгоритмов работы прототипа защищенной системы контроля и управления доступом на основе встроенных устройств;
- проведение экспериментов и оценка прототипа на основе выбранных методик.

Основным результатом выполнения выпускной квалификационной работы является программно-аппаратный прототип защищенной системы контроля и управления доступом.

2. МЕТОДИКИ ОЦЕНКИ СИСТЕМ НА ОСНОВЕ ВСТРОЕННЫХ УСТРОЙСТВ

Сложность разработки защищенных систем на основе встроенных устройств обуславливается разнородностью устройств системы, используемых коммуникационных протоколов, изменчивостью топологии системы во времени, мобильностью и автономностью отдельных устройств и ограничениями на аппаратные ресурсы устройств. Кроме того, возможна аппаратная несовместимость встроенных устройств и их компонентов.

Также отметим, что в настоящее время нет единой методологии, которую могли бы использовать разработчики систем на основе встроенных устройств для постановки и реализации требований безопасности. При этом основными проблемами, с которыми сталкиваются разработчики систем на основе встроенных устройств, являются: сложность анализа и моделирования требований к защите системы на основе встроенных устройств; отсутствие стандартов в области обеспечения безопасности программно-аппаратного обеспечения встроенных устройств.

2.1. Адаптация модели нарушителя

Модель нарушителя позволяет выявлять перечень возможных атак на инфраструктуру системы на основе встроенных устройств и ее сервисы. Кроме того, модель позволяет описывать события безопасности, сценарии атак и аномальную активность, а также определить возможные цели злоумышленника. Модель будет также способствовать оценке конкретных атак с точки зрения их выполнимости, а также потребления ресурсов, которые нарушителю необходимо затратить для успешного проведения атаки. Модель нарушителя применима для проектирования механизмов защиты от различных классов атак на инфраструктуру системы или ее сервисы, а также тестирования системы на предмет его подверженности тем или иным угрозам информационной безопасности.

2.1.1. Обзор и анализ существующих моделей нарушителя

Основными нормативными документами, определяющими модель нарушителя на территории Российской Федерации, являются:

- "Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных", Федеральная служба по техническому и экспортному контролю (ФСТЭК России), 15 февраля 2008 г. [1].
- "Методика определения угроз безопасности информации в информационных системах", Федеральная служба по техническому и экспортному контролю (ФСТЭК России), проект, 2015 г. [2].
- "Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности", Федеральная служба безопасности (ФСБ России), 31 марта 2015 года, № 149/7/2/6-432 [3].

В нормативном документе ФСТЭК России [1] нарушители подразделяются на два типа: внешние и внутренние. При этом к внешним нарушителям относятся нарушители, не имеющие доступа к ИСПДн, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена. Внешними нарушителями могут быть: разведывательные службы государств; криминальные структуры; конкуренты (конкурирующие организации); недобросовестные партнеры; внешние субъекты (физические лица).

К внутренним нарушителям относятся нарушители, имеющие доступ к ИСПДн, включая пользователей ИСПДн, реализующие угрозы непосредственно в ИСПДн. При этом в нормативном акте подчеркивается, что возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны режимных и организационно-

технических мер защиты, в том числе по допуску физических лиц к ПДн и контролю порядка проведения работ.

Внутренние потенциальные нарушители подразделяются на восемь категорий в зависимости от способа доступа и полномочий доступа к ПДн. Рассмотрим каждую из категорий более подробно.

Категория 1: лица, имеющие санкционированный доступ к ИСПДн, но не имеющие доступа к ПДн. К этому типу нарушителей относятся должностные лица, обеспечивающие нормальное функционирование ИСПДн.

Категория 2: зарегистрированные пользователи ИСПДн, осуществляющие ограниченный доступ к ресурсам ИСПДн с рабочего места.

Категория 3: зарегистрированные пользователи ИСПДн, осуществляющие удаленный доступ к ПДн по локальным и (или) распределенным информационным системам.

Категория 4: зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности сегмента (фрагмента) ИСПДн.

Категория 5: зарегистрированные пользователи с полномочиями системного администратора ИСПДн.

Категория 6: зарегистрированные пользователи с полномочиями администратора безопасности ИСПДн.

Категория 7: программисты-разработчики (поставщики) прикладного программного обеспечения и лица, обеспечивающие его сопровождение на защищаемом объекте.

Категория 8: разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств на ИСПДн.

В нормативном документе ФСТЭК России [2] вводится понятие потенциала нарушителя, который может быть базовым (низким), базовым повышенным (средним) и высоким соответственно. Рассмотрим данное понятие более подробно.

Нарушитель с **базовым** (низким) **потенциалом** имеет возможность получить информацию об уязвимостях отдельных компонент информационной

системы, опубликованную в общедоступных источниках. Кроме того, нарушитель данного потенциала имеет возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществляет создание методов и средств реализации атак и реализацию атак на информационную систему.

Нарушитель с **базовым повышенным** (средним) **потенциалом** обладает всеми возможностями нарушителей с базовым потенциалом, а также имеет осведомленность о мерах защиты информации, применяемых в информационной системе данного типа. Кроме того, нарушитель данного потенциала имеет возможность получить информацию об уязвимостях отдельных компонент информационной системы путем проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного программного обеспечения и отдельных программных компонентов общесистемного программного обеспечения и имеет доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования информационной системы.

Нарушитель с **высоким потенциалом** обладает всеми возможностями нарушителей с базовым и базовым повышенным потенциалами, а также имеет возможность осуществлять несанкционированный доступ из выделенных (ведомственных, корпоративных) сетей связи, к которым возможен физический доступ (незащищенных организационными мерами). Кроме того, нарушитель данного типа имеет возможность получить доступ к программному обеспечению чипсетов (микропрограммам), системному и прикладному программному обеспечению, телекоммуникационному оборудованию и другим программно-техническим средствам информационной системы для преднамеренного внесения в них уязвимостей или программных закладок и имеет хорошую осведомленность о мерах защиты информации, применяемых в информационной системе, об алгоритмах, аппаратных и программных средствах, используемых в информационной системе. Также, нарушитель данно-

го потенциала имеет возможность получить информацию об уязвимостях путем проведения специальных исследований (в том числе с привлечением специализированных научных организаций) и применения специально разработанных средств для анализа программного обеспечения, имеет возможность создания методов и средств реализации угроз безопасности информации с привлечением специализированных научных организаций и реализации угроз с применением специально разработанных средств, в том числе обеспечивающих скрытное проникновение в информационную систему и воздействие на нее, имеет возможность создания и применения специальных технических средств для добывания информации (воздействия на информацию или технические средства), распространяющейся в виде физических полей или явлений.

В нормативном документе ФСБ России [3] приводятся обобщенные возможности источников атак, в том числе и нарушителей (при этом основное внимание уделяется возможностям нарушителя по атакам на криптографические средства и среду их функционирования):

- возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны;
- возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, но без физического доступа к АС, на которых реализованы СКЗИ и среда их функционирования;
- возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны с физическим доступом к АС, на которых реализованы СКЗИ и среда их функционирования;
- возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области анализа сигналов ли-

нейной передачи и сигналов побочного электромагнитного излучения и наводок СКЗИ);

- возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей прикладного программного обеспечения);
- возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей аппаратного и программного компонентов среды функционирования СКЗИ).

Помимо основных нормативных документов, существует ряд научно-исследовательских работ в области анализа угроз информационной безопасности и нарушителей систем со встроенными устройствами. Так, в работах [4, 5] обосновывается необходимость и важность построения модели нарушителя как элемента процесса проектирования и разработки защищенных встроенных устройств. Кроме того, в работе [6] рассматриваются аспекты противодействия несанкционированному доступу к информации на примере извлечения секретных данных из смарт-карт. При этом авторы выделяют основные четыре типа атак:

- программные атаки, которые базируются на использовании уязвимостей коммуникационных протоколов, а также криптографических алгоритмов;
- прослушивание аналоговых интерфейсов и микросхем на основе анализа электромагнитного воздействия;
- атаки типа «внесение неисправностей» (*fault generation*), используемые для повышения привилегий доступа;
- микро-пробирование (*microprobing*) для осуществления прямого доступа к микросхемам.

В работе [7] рассматривается классификация нарушителя на основе уровня компетенции нарушителя и знаниях о его возможностях. При этом основное внимание уделяется следующим видам атак:

- атаки на микросхемы, включая метод «внесения неисправностей» и прослушивание (что согласуется с классификацией, упомянутой в работе [6]);
- атака замены электронных модулей, отвечающих за функции защиты (*substitution attack*).

Отметим, что в работе [4] предложена классификация атак в соответствии с наиболее типичными злонамеренными воздействиями, встречающимися на практике: использованием данных профилей других пользователей; злонамеренная модификация данных; раскрытие секретной информации; отказ доступа; получение привилегий. Отметим, что в данной классификации основное внимание уделяется возможностям нарушителя, а не его целям.

В работе [8] предлогается разделить нарушителей на несколько групп в зависимости от уровня взаимодействия нарушителя со встроенным устройством. А в работе [9] предложен механизм по объединению моделирования защиты с процессом разработки компонентов защиты встроенных устройств. Кроме того, в работе представлен инструмент для анализа защищенности, который может быть интегрирован с существующими средствами в рамках совместной среды проектирования с учетом вопросов безопасности, функциональности и архитектуры системы.

В работе [10] предложен базирующийся на анализе угроз подход к проектированию и анализу архитектур защищенных информационных систем. В рамках данного подхода были промоделированы угрозы информационной безопасности с использованием специально подготовленных примеров неправильного использования.

С другой стороны, в работе [11] представлено исследование возможности использования моделирования угроз в качестве основы для спецификации требований к защите информационно-телекоммуникационных систем.

В работе [12] были рассмотрены вопросы безопасности и конфиденциальности распределенных систем интеллектуальных камер, включая требования к защите, возможные атаки, типовые риски, представляя имеющиеся решения по анализу как на уровне отдельных узлов сети, так и на уровне всей системы.

В [13] предложена экспериментальная установка, при помощи которой встроенные устройства атакуются с использованием нескольких образцов данных посредством изменения напряжения источника питания. При помощи экспериментальной установки исследуется влияние эффекта блокировки данных на возможности нарушителя.

2.1.2. Адаптированная модель нарушителя

В данном разделе предлагается адаптированная модель нарушителя для задачи обеспечения защиты помещения системой контроля и управления доступом. Данная модель описывает возможные типы нарушителя, пытающегося скомпрометировать инфраструктуру системы контроля и управления доступом или ее сервисы, а также базируется на классификации нарушителя по двум направлениям: типу доступа к инфраструктуре системы контроля и управления доступом или ее сервисам и по возможностям нарушителя.

Рассмотрим классификацию нарушителя по типу доступа к инфраструктуре системы контроля и управления доступом или ее сервисам более подробно (таблица 4). При этом важно отметить, что данная классификация является иерархической (каждый следующий тип взаимодействия с инфраструктурой или сервисами включает функциональные возможности предыдущих типов).

Таблица 4 – Классификация нарушителя по типу доступа

Тип	Описание
0	Нарушитель не имеет доступа к инфраструктуре или сервисам системы контроля и управления доступом и, по сути, нарушители данного типа воздействуют на них опосредованно, зачастую с использованием методов социального инжиниринга.
1	Нарушитель взаимодействует с инфраструктурой или сервисами системы контроля и управления доступом опосредованно, осуществляя непрямой доступ к ним, например удаленный доступ через сеть Интернет с использованием протоколов TCP/IP.
2	Нарушитель может воздействовать на инфраструктуру системы контроля и управления доступом или его сервисы напрямую, находясь при этом на некотором расстоянии от защищаемого помещения, к примеру с использованием интерфейсов Wi-Fi, IR, Bluetooth.
3	Нарушитель имеет физический доступ к инфраструктуре системы контроля и управления доступом, например с использованием интерфейсов последовательного порта и USB, но не имеет возможности исследовать и модифицировать её внутренние электронные компоненты.
4	Нарушитель имеет полный доступ к инфраструктуре системы контроля и управления доступом и всем ее микросхемам и внутренним интерфейсам, таким как интерфейсы шины памяти, периферийных шин, а также отладочному интерфейсу.

Важно отметить, что для оценки уровня защищенности необходимо также определить сложность возможных компрометирующих действий нарушителя с учетом возможных вовлеченных инструментов, знаний и времени. Рассмотрим классификацию нарушителя по уровню его возможностей более подробно (таблица 5).

Таблица 5 – Классификация нарушителя по уровню возможностей

уровень	Описание
1	Нарушитель не имеет или имеет недостаточные знания об инфраструктуре и сервисах системы контроля и управления доступом, а также может использовать программные инструменты, находящиеся в публичном доступе. Нарушители данного уровня могут в большей степени эксплуатировать уже существующие общеизвестные уязвимости, нежели чем обнаруживать новые.
2	Нарушитель владеет информацией об инфраструктуре системы контроля и управления доступом и ее сервисах и имеет доступ к специализированным атакующим средствам. Нарушитель имеет достаточное время и информацию для поиска ранее неиспользовавшихся уязвимостей.
3	Нарушитель представляет собой группу нарушителей уровня 2 и способен к осуществлению глубокого анализа инфраструктуры системы контроля и управления доступом и ее сервисов при помощи специализированных инструментов анализа.

В соответствии с приведенными выше классификациями модель нарушителя описывает анализ возможностей нарушителя, возможные атаки на инфраструктуру и сервисы системы контроля и управления доступом, а также особенности защиты для противодействия таким атакам в соответствии с типом нарушителя.

2.1.3. Модель инцидентов безопасности

Вектора атак на помещение, защищаемое системой контроля и управления доступом, можно разделить на несколько видов: атаки с использованием социальной инженерии, атаки на инфраструктуру системы контроля и управления доступом и ее сервисы, а также атаки на элементы инфраструк-

туры системы. При этом атаки с использованием социальной инженерии являются единственным возможным способом для нарушителей типа 0 оказать вредоносное воздействие. Для нарушителей типа 1, 2, 3 и 4 атаки с использованием социальной инженерии представляют собой подготовительный этап, связанный с анализом поведения пользователей системы контроля и управления доступом. Данный этап необходим для облегчения, а также повышения вероятности успеха, других компрометирующих воздействий. Предполагаемая защита от векторов атак данного вида включает в первую очередь обучение пользователей особенностям защиты от социально инженерных атак.

Атаки на инфраструктуру системы контроля и управления доступом и ее сервисы предполагают наличие внешних интерфейсов для удаленного доступа к ним. При этом элементы инфраструктуры и сервисы системы представляют собой некоторые адреса в рамках ее сети. Таким образом, атакующие воздействия аналогичны типичным атакам на рабочие станции и серверы. Нарушитель способен прослушивать коммуникационные каналы, исследовать удаленные сервисы системы контроля и управления доступом и осуществлять поиск ошибок в программном обеспечении, затрагивающем безопасность инфраструктуры и сервисов системы. Предполагается, но не является обязательным, чтобы нарушитель был знаком с моделью системы контроля и управления доступом, тем не менее, атака может проводиться без каких-либо предварительных знаний. Основной угрозой векторов атак данного вида являются перехват, анализ и подделка сообщений, передаваемых по сети для выполнения сетевых атак на встроенные устройства системы. Примерами атак, которые могут быть произведены нарушителем типа 1, являются: перехват, модификация и подделка TCP/IP-сообщений от встроенного устройства (*man-in-the-middle*); классические сетевые атаки (DDoS, TCP SYN Flood); атаки на основе использования конкретных уязвимостей (отправка некорректных сетевых пакетов, переполнения буфера); криптографический анализ зашифрованных сообщений; воздействия на систему аутентификации; атаки на систему обновления. Нарушитель типа 2 расширяет данный пере-

чень атак воздействиями на беспроводные интерфейсы системы контроля и управления доступом (Bluetooth, Wi-Fi или IR). Кроме того, среди первоначальных угроз, которые могут быть реализованы, может быть также атака получения информации по сторонним каналам (например, анализ электромагнитного излучения).

Атаки на элементы инфраструктуры системы контроля и управления доступом предполагают наличие физического доступа нарушителя к ним. Так, с точки зрения нарушителя типа 3 каждый элемент инфраструктуры рассматривается как «черный ящик» с возможностью прямого подсоединения ко всем открытым интерфейсам элемента инфраструктуры. Это открывает возможность создания полностью контролируемой среды для исследования различных характеристик (в том числе энергопотребления, производительности и других). Примерами атак, которые могут выполняться нарушителями типа 3, являются атаки по сторонним каналам на основе различных характеристик с использованием прямого доступа; атаки на интерфейсы элементов инфраструктуры с использованием прямого доступа к ним; помещение поддельных элементов инфраструктуры в систему вместо оригинальных. Для нарушителя типа 4 каждый элемент инфраструктуры системы контроля и управления доступом представляет собой множество взаимосвязанных микросхем, причем атакующий имеет неограниченный доступ к ним. Нарушитель может проводить дизассемблирование элементов инфраструктуры и использовать аппаратные эксплоиты: внутренние интерфейсы, скрытые порты, а также осуществлять нелегитимные воздействия с использованием межкомпонентной коммуникации. Нарушитель данного типа может осуществлять чтение или модификацию данных, расположенных внутри электронных компонентов элементов инфраструктуры, в том числе ключей шифрования.

2.2. Методика оценки защищенности

Существо современных моделей и методик комбинирования средств защиты встроенных устройств заключается в выявлении и учете перечня

возможных атак, которым может быть подвержена система в соответствии с выбранной моделью нарушителя, а также используемыми программно-аппаратными компонентами, уже на этапе проектирования (рисунок 1).

Рисунок 1 – Модели и методики комбинирования средств защиты ВУ

Методика оценки защищенности для сетей встроенных устройств относится непосредственно к третьему шагу методик и моделей комбинирования средств защиты встроенных устройств – статическому тестированию. Статический подход подразумевает анализ защищенности встроенных устройств без их непосредственной эксплуатации. Итоговая оценка формируется на основе компонентного состава, а также программного кода прошивки встроенных устройств.

В основе статического тестирования лежат правила, устанавливающие взаимосвязь между компонентным составом встроенных устройств, моделью нарушителя и атаками на систему. Таким образом, если защищенность встроенных устройств, используемых анализируемой системой, достаточна, то можно переходить к этапу разработки инфраструктуры для построения защищенной системы встроенных устройств. В противном случае, необходим пересмотр функциональных требований, что означает возврат к первому шагу моделей и методик комбинирования средств защиты встроенных устройств.

Общий вид формата правил статического тестирования может быть представлен следующим образом:

$$Rule = Number, Component \,\&\, Violator \rightarrow Attack, \quad (1)$$

где $Rule$ – правило, $Number$ – номер правила, $Component$ – функциональная особенность (компонент) встроенного устройства (может быть NULL, если данная атака не зависит от функциональных особенностей встроенного устройства), $Violator$ – типы нарушителей различного уровня, $Attack$ – возможная атака на встроенное устройство.

При этом типы нарушителей различного уровня $Violator$ представлены следующим образом:

$$Violator = type(i), level(i); \dots; type(i+n), level(i+n) \quad (2)$$

где $Violator$ – типы нарушителей различного уровня, $type$ – тип доступа нарушителя к встроенному устройству, $level$ – уровень возможностей нарушителя.

2.3. Методика оценки оперативности

Оперативность – способность системы контроля и управления доступом к проверке идентификационных данных пользователей, а также обнаружению нарушений политики безопасности организации. Требование к оперативности задается в виде:

$$TIME_N \rightarrow min \quad (3)$$

$$TIME_N \leq \min_{s \in S} TIME_N^S \quad (4)$$

где $TIME_N$ – время, необходимое для проверки идентификационных данных пользователя, а также обнаружения нарушений политики безопасности организации в помещении N с использованием предлагаемой системы, S – множество возможных состояний пользователя в системе, $TIME_N^S$ – время, необходимое для проверки идентификационных данных пользователя, а также обнаружения нарушений политики безопасности организации для состояния пользователя в системе $s \in S$. Необходимо отметить, что время, необходимое для проверки идентификационных данных пользователя, как правило,

значительно меньше времени, необходимого для обнаружения нарушений политики безопасности организации.

Для того чтобы система контроля и управления доступом могла использоваться в режиме реального времени при проверке идентификационных данных пользователя, а также в режиме близком к реальному времени при обнаружении нарушений политики безопасности организации, она должна осуществлять проверку идентификационных данных пользователей, а также обеспечивать обнаружение нарушений политики безопасности организации за время, не превышающее некоторой границы. Такое требование к оперативности задается в виде:

$$P_{\text{ОП}}(TIME_N \leq TIME^{\text{ДОП}}) \geq P_{\text{ОП}}^{\text{ДОП}} \quad (4)$$

где $P_{\text{ОП}}$ – вероятность осуществить проверку идентификационных данных пользователей, а также обеспечить обнаружение нарушений политики безопасности организации за заданное время, $TIME^{\text{ДОП}}$ – допустимое время проверки идентификационных данных пользователей, а также обнаружения нарушений политики безопасности организации, $P_{\text{ОП}}^{\text{ДОП}}$ – допустимое значение вероятности. Основываясь на результатах опроса экспертов и серии проведенных экспериментов, было выбрано $TIME^{\text{ДОП}}$ равное 0.5 секунды для проверки идентификационных данных пользователей, а также $TIME^{\text{ДОП}}$ равное 2 секунды для обнаружение нарушений политики безопасности организации. За это время должен быть выполнен запрос к базе данных центрального сервера доступа, определены возможные контрмеры, а также сформировано соответствующее уведомление.

2.4. Методика оценки обоснованности

Обоснованность – свойство соответствия результатов проверки идентификационных данных пользователей, а также обнаружения нарушений политики безопасности организации фактическому состоянию. В данной вы-

пускной квалификационной работе выбраны следующие показатели обоснованности:

- количество учитываемых параметров для идентификации пользователя системы контроля и управления доступом;
- количество обнаруженных нарушений политики безопасности организации, т.е. вероятность того, что выходная информация соответствует реальному состоянию.

Требования к данным показателям задаются сравнением с существующими системами:

$$POL_N \geq \max_{s \in S} MAL_N^S \tag{6}$$

$$PARAMS \geq \max_{s \in S} PARAMS^S \tag{7}$$

где POL_N и $PARAMS$ – количество обнаруженных нарушений политики безопасности организации для помещения N и учитываемых параметров для идентификации пользователя системы контроля и управления доступом соответственно, S – множество возможных состояний пользователя в системе, POL_N^S и $PARAMS^S$ – количество обнаруженных нарушений политики безопасности организации, а также учитываемых параметров для идентификации пользователя системы контроля и управления доступом для состояния пользователя $s \in S$. Таким образом, разрабатываемая система должна обнаруживать максимально возможное (и не меньшее чем аналогичные системы) количество нарушений политики безопасности организации, а также учитывать не меньшее количество параметров для идентификации пользователя системы, нежели существующие аналоги. Это позволит говорить о том, что новая система как минимум не уступает существующим аналогам по качеству обнаружения нарушений политики безопасности организации.

2.5. Методика оценки ресурсопотребления

Ресурсопотребление характеризует номенклатуру и количество необходимых программных и аппаратных средств, объемы необходимых информационных массивов, кадровые ресурсы и другие ресурсы, затрачиваемые на

реализацию процесса проверки идентификационных данных пользователей, а также обнаружения нарушений политики безопасности организации в помещении в рамках системы контроля и управления доступом. Требования к ресурсопотреблению задаются следующим образом:

$$P_{\text{РЕС}}(r \leq R^{\text{ДОП}}) \geq P_{\text{РЕС}}^{\text{ДОП}} \quad (8)$$

где $P_{\text{РЕС}}$ – вероятность того, что ресурсы, затрачиваемые на процесс проверки идентификационных данных пользователей, а также обнаружения нарушений политики безопасности организации r, не превышают допустимого значения $R^{\text{ДОП}}$, $P_{\text{РЕС}}^{\text{ДОП}}$ – допустимое значение вероятности, принятое равным $P_{\text{РЕС}}^{\text{ДОП}} = 0.99$. При этом для выполнения процесса проверки идентификационных данных пользователей, а также обнаружения нарушений политики безопасности организации предполагается выделение отдельного сервера, однако часть задач, связанных со сбором и предварительной обработкой идентификационных данных будет выполняться микроконтроллерах. Отметим, что при аварийном режиме работы системы, проверка идентификационных данных пользователей будет осуществляться на микроконтроллерах в полном объеме на основе локальной базы данных. Кроме того, часть ресурсов будет занята операционной системой или прошивкой, поэтому процесс проверки идентификационных данных пользователей, а также обнаружения нарушений политики безопасности организации не должен занимать более 75% от общего объема ресурсов.

2.6. Сводная таблица

Целью разработки системы контроля и управления доступом является минимизация времени $TIME_N$, необходимого для проверки идентификационных данных пользователя, а также обнаружения нарушений политики безопасности организации, при соблюдении требований к обоснованности и ресурсопотреблению.

Сведем свойства для оценки результатов выпускной квалификационной работы и требования к ним в единую таблицу 6.

Таблица 6 – Свойства для оценки системы контроля и управления доступом

Свойство	Показатели	Требования
Оперативность	Время, необходимое для проверки идентификационных данных пользователей, а также обнаружения нарушений политики безопасности организации.	$TIME_N \to min$ $TIME_N \leq \min\limits_{s \in S} TIME_N^S$ $P_{\text{ОП}}(TIME_N \leq TIME^{\text{ДОП}}) \geq P_{\text{ОП}}^{\text{ДОП}}$
Обоснованность	Количество обнаруженных нарушений политики безопасности организации присущих анализируемому помещению и количество учитываемых параметров для идентификации пользователя системы.	$POL_N \geq \max\limits_{s \in S} POL_N^S$ $PARAMS \geq \max\limits_{s \in S} PARAMS^S$
Ресурсопотребление	Вероятность того, что количество использованных ресурсов не будет превышать допустимое значение	$P_{\text{РЕС}}(r \leq R^{\text{ДОП}}) \geq P_{\text{РЕС}}^{\text{ДОП}}$

3. ПРОТОТИП СИСТЕМЫ И ОСНОВНЫЕ АЛГОРИТМЫ ЕГО РАБОТЫ

В настоящее время широкое распространение получили сложные, многошаговые, а также растянутые во времени атаки, одновременно происходящие как на физическом (например, незаконное проникновение в помещение), так и на кибернетическом (например, эксплуатация уязвимостей системы управления базами данных) уровнях. Для защиты от атак такого типа необходимо обрабатывать и анализировать данные от множества гетерогенных источников. При этом большинство существующих систем физической и кибернетической защиты работают независимо друг от друга, а интеграция таких систем практически не встречается [14]. Кроме того, в существующих системах контроля и управления доступом, средства защиты внедряются уже после этапа разработки системы. При таком подходе, средства защиты формируют защитную оболочку системы, преодолев которую, злоумышленник получит полный контроль, а значит, сможет делать с системой все что угодно. Именно поэтому, для соответствия современным вызовам, требуется реализовать комплексный подход к обеспечению безопасности. Отметим, что комплексность подхода заключается не только в объединении систем физической и кибернетической безопасности. Не менее важным является учет уже на этапе разработки системы необходимости обеспечения устойчивости такой системы к атакам на нее [15,16].

3.1. Архитектура системы

Архитектура разрабатываемой системы контроля и управления доступом состоит из нескольких основных частей (рисунок 2):

- источники данных (1,2);
- модуль сбора данных (3);
- модуль обработки событий (4);
- модуль аналитической обработки данных и визуализации (5).

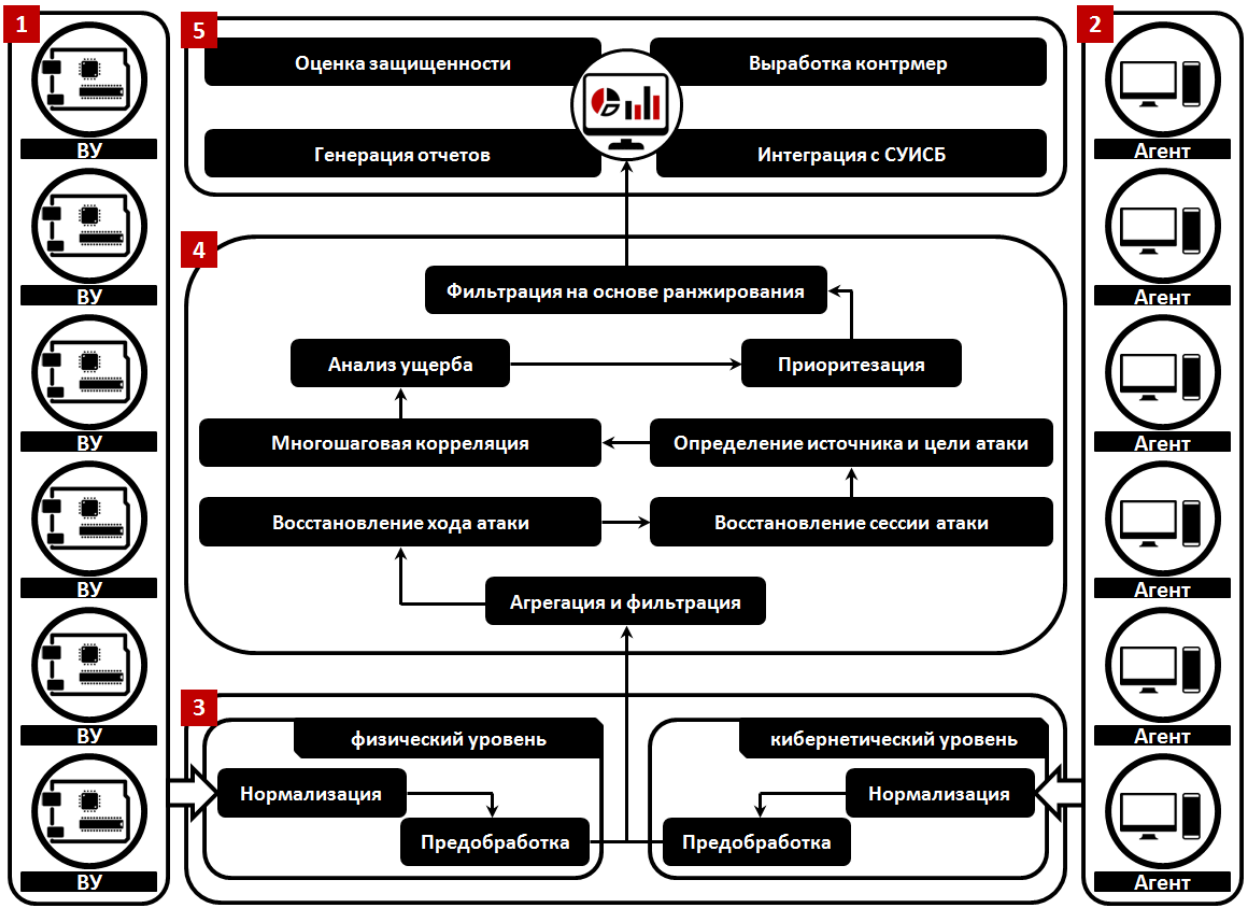

Рисунок 2 – Архитектура системы

Модуль сбора данных подвергает процессам нормализации и предобработки сырые гетерогенные исходные данные. При этом под нормализацией понимается процесс преобразования исходных данных в единый формат. Предобработка исходных данных позволяет изменить типы полей, убрать несущественные данные, сформировать новые поля. Важно отметить, что исходные данные могут быть условно разделены на данные физического и кибернетического уровней.

К источникам данных физического уровня (1) относятся встроенные устройства, отвечающие за контроль доступа в определенном помещении. К источникам данных кибернетического уровня (2) относятся агенты рабочих станций, отвечающие за мониторинг сеанса пользователя с операционной системой ЭВМ.

Объединение исходных данных от источников данных физического и кибернетического уровней позволит снизить риски, связанные с проведением

сложных, растянутых во времени и происходящих на разных уровнях киберфизических атак, за счет применения корреляции данных, поступающих от гетерогенных источников. Это даст возможность процессу корреляции событий безопасности в модуле обработки событий (4) автоматически формировать инциденты, выявлять аномальную активность, а также определять сценарии атак, выявление которых при использовании современных систем защиты возможно только на этапе расследования. Кроме того, будет снижена нагрузка на человека-оператора за счет аналитической обработки данных и визуализации (5).

К основным этапам процесса корреляции событий безопасности относятся: агрегация и фильтрация, восстановление хода атаки, восстановление сессии атаки, определение цели и источника атаки, многошаговая корреляция, анализ ущерба, приоритезация, фильтрация на основе ранжирования [17,18,19,20].

На этапе *агрегации и фильтрации* происходит удаление части исходных данных, поступающих из модуля обработки событий по заранее определенным правилам (или фильтрам), а также объединение нескольких вхождений одного и того же события в результате обнаружения различными источниками.

На этапе *восстановления хода атаки* выполняется объединение событий, вызванных активностью одного злоумышленника к одной цели.

Этап *восстановления сессии атаки* направлен на уточнение событий, полученных в результате восстановления хода атаки. В результате становится известна информация об объекте, который был атакован, и субъекте, который осуществил атаку.

На этапе *определения цели и источника атаки* происходит объединение атак, полученных в результате восстановления сессии атаки. Выявление общего субъекта или объекта атаки позволяет определить сценарии один-ко-многим и много-к-одному атак соответственно.

Многошаговая корреляция направлена на объединение атак, обнаруженных на этапе восстановления сессии атаки, и сценариев атак, обнаруженных на этапе определения цели и источника атаки. Это необходимо для выявления более сложных сценариев атак. Обычно, эти сценарии выявляются на основе экспертных знаний.

На этапе *анализа ущерба* рассчитываются численные или качественные показатели ущерба от реализации обнаруженных сценариев атак.

На этапе *приоритезации* определяются степени важности обнаруженных атак для пользователя системы. Приоритеты зависят от политики безопасности организации и требований к безопасности.

На этапе *фильтрации на основе ранжирования* происходит снижение количества рассматриваемых сценариев атак на базе результатов этапов анализа ущерба и приоритезации.

К основным используемым методам корреляции событий относятся методы на основе правил, конечных автоматов, а также Байесовской или нейронной сети [18,19,21,22].

Существо *метода на основе правил* заключается в формировании правил корреляции, понятных модулю обработки событий. Эти правила позволяют, например, создавать и анализировать состояния сотрудников или гостей организации в системе учета доступа. При этом возможные переходы между состояниями задаются с помощью методов на основе конечных автоматов. Состояния, а также возможные переходы между ними, позволяют в режиме реального времени выявлять нарушения политики безопасности организации.

В основе *Байесовской сети* лежит модель направленного ациклического графа. Суть метода заключается в расположении в вершинах графа корреляционных признаков. При этом связывающие их направленные дуги представляют собой отношение условной независимости одного признака от другого. В основе *нейронной сети* лежит математическая модель, также состоя-

щая из признаков, имеющих собственное состояние, и линий связи, определяющих зависимость одних корреляционных признаков от других.

Методы на основе Байесовской или нейронной сети могут использоваться для выявления аномальной активности. Предполагается, что обнаружение аномалий позволит выявлять атаки, использующие недостатки политики безопасности организации.

В рамках реализации данных методов в прототипе защищенной системы контроля и управления доступом, в качестве переменных или искусственных нейронов могут использоваться как отдельные события или атаки, характерные для модуля обработки системы, так и обобщенные характеристики множества событий и атак.

3.2. Основные алгоритмы работы системы

В качестве исходных данных для описания основных алгоритмов работы системы использована следующая бизнес-логика:

- Пользователи системы контроля и управления доступом могут иметь одну из следующих ролей: *гость*, *сотрудник* или *администратор*. При этом под администратором рассматривается сотрудник организации с правами администратора.
- Каждый сотрудник организации принадлежит одному или нескольким отделам организации, среди которых: *технический отдел*, *отдел по работе с клиентами*, *отдел кадров*, *отдел безопасности*.

3.2.1. Основные теоретические сведения

Основные алгоритмы работы системы удобно представимы с помощью *диаграмм прецедентов*, основное назначение которых – описание функциональности и поведения системы, позволяющие заказчику, конечному пользователю и разработчику совместно обсуждать проектируемую или уже существующую систему. Прежде чем дать определение диаграмме прецедентов, рассмотрим ее основные элементы. К основным элементам данной диаграм-

мы относятся: *актор*, *прецедент*, а также *отношения* между ними. Рассмотрим каждый из элементов более подробно.

Актор – это множество логически связанных ролей в UML, исполняемых при взаимодействии с прецедентами или сущностями. Актором может быть человек или другая система, подсистема, класс.

Прецедент – это возможность моделируемой системы (часть ее функциональности), благодаря которой актор может получить конкретный, измеримый и нужный ему результат. Прецедент соответствует отдельному сервису системы, определяет один из вариантов её использования и описывает типичный способ взаимодействия актора с системой. Варианты использования обычно применяются для спецификации внешних требований к системе.

Таким образом, диаграмма прецедентов может быть определена как диаграмма, отражающая отношения между акторами и прецедентами. Данная диаграмма является составной частью модели прецедентов, позволяющей описать систему на концептуальном уровне.

К основным отношениям между элементами диаграммы прецедентов относятся следующие отношения: *обобщение*, *включение* и *расширение*. Рассмотри каждое из отношений на основе конкретного примера.

Обобщение: множество акторов с похожими ролями в системе могут быть объединены в одного, более абстрактного, актора (рисунок 3).

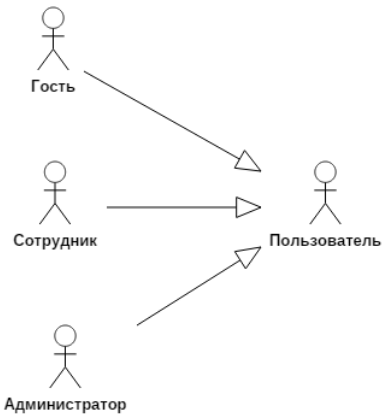

Рисунок 3 – Обобщение акторов

В соответствии с бизнес-логикой системы, пользователи системы могут иметь одну из следующих ролей: гость, сотрудник или администратор. Выражаясь в терминах диаграммы прецедентов, актор пользователь – это обобщение акторов гость, сотрудник и администратор.

Включение: один прецедент связывается с другим прецедентом отношением включения в ситуации, когда выполнение первого невозможно без выполнения второго (рисунок 4).

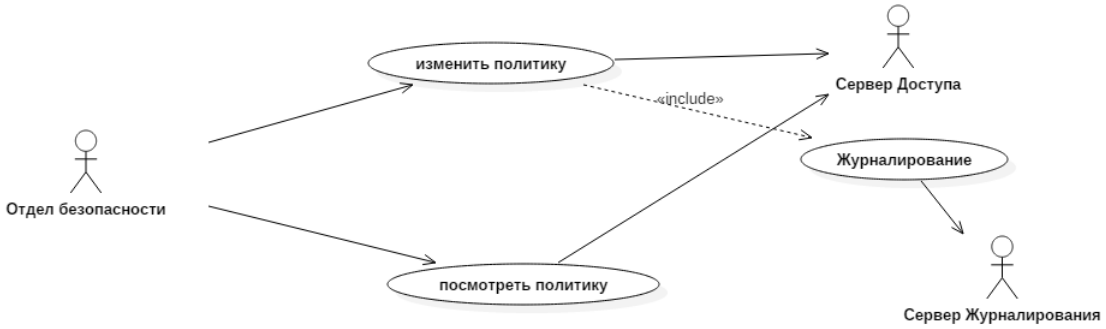

Рисунок 4 – Отношение включения между прецедентами

В качестве примера, рассмотрим прецедент изменения политики безопасности организации сотрудником отдела безопасности. Каждое подобное действие сотрудника формирует соответствующую журнальную запись, которая направляется на сервер журналирования. Таким образом, прецедент изменить политику невозможен без последующего прецедента журналирование.

Расширение: один прецедент связывается с другим отношением расширения в ситуации, когда для выполнения первого не обязательно выполнение второго (рисунок 5).

В качестве примера, рассмотрим прецедент операции над политиками безопасности организации, актором которого является сотрудник отдела безопасности. В перечень возможных операций прецедента входят такие операции, как: изменение политики безопасности организации и просмотр политики безопасности организации. Любое действие сотрудника отдела безопасности, в результате которого была изменена политика безопасности организа-

ции, должно быть зафиксировано на сервере журналирования в виде журнальной записи. Если же сотрудник отдела безопасности только просмотрел политику безопасности организации без внесения каких-либо изменений, то журнальная запись не создается.

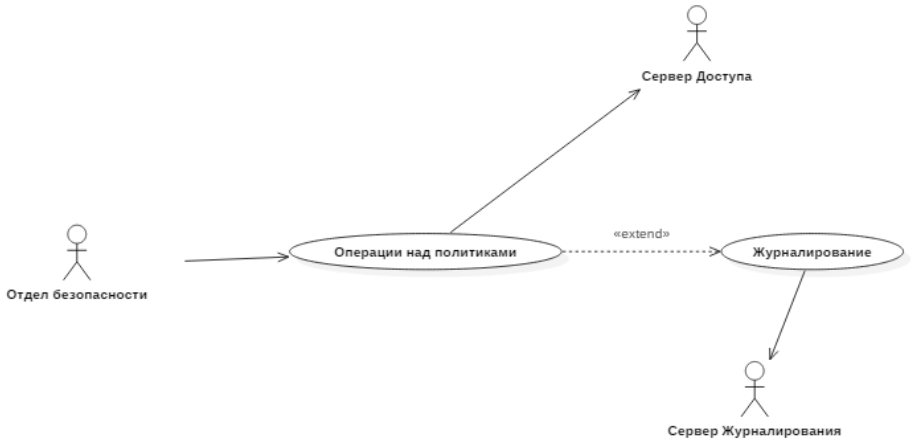

Рисунок 5 – Отношение расширения между прецедентами

В качестве шаблона описания прецедента будем использовать следующие поля для заполнения: прецедент (название), краткое описание, актор, зависимость, предусловие, основной поток событий, альтернативные потоки событий, постусловие.

Примечание: Далее по тексту будет использован русскоязычный аналог аббревиатуры CRUD (create, read, update, delete) – СУПО (создать, удалить, посмотреть, обновить). Это связано с тем, что логика взаимодействия приложения для управления сервером доступа с базой данных сервера доступа будет строиться на четырех базовых функциях СУПО (CRUD).

3.2.2. Диаграмма прецедентов системы

Рассмотрим каждый из прецедентов, представленный на диаграмме (рисунок 6), более подробно.

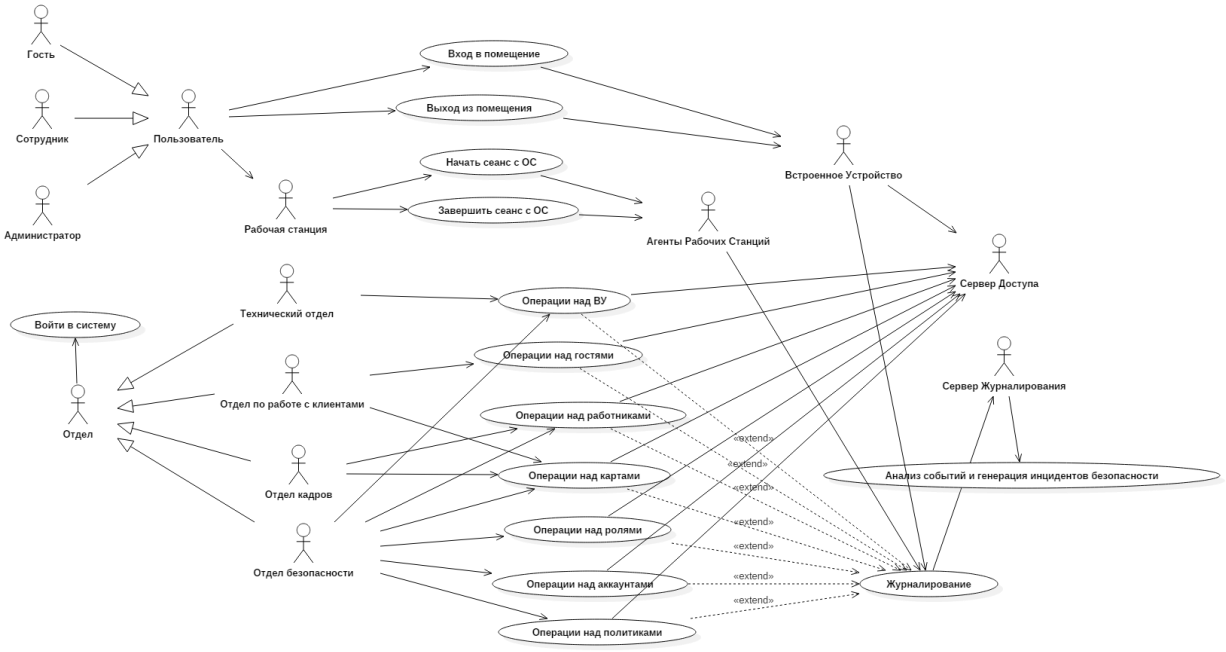

Рисунок 6 – Диаграмма прецедентов системы

Прецедент: выход из помещения.

Краткое описание: данный прецедент описывает процесс выхода пользователя из помещения.

Актор: пользователь.

Зависимость: нет.

Предусловие: пользователь вошел в помещение.

Основной поток событий: данный прецедент начинает выполняться, когда пользователь пытается выйти из помещения. Рассмотрим последовательность событий более подробно:

1. пользователь прислоняет бесконтактную смарт-карту к считывателю;
2. номер карты пользователя пересылается на сервер доступа;
3. сервер доступа присылает ответ, содержащий: имя пользователя, уникальный идентификатор карты, тип доступа (true/false);
4. формируется журнальная запись о произошедшем событии.

Альтернативные потоки событий: в ситуации, когда сервер доступа перестает быть доступным ввиду потери интернет соединения или других при-

чин, начинает выполняться альтернативный поток событий данного прецедента. Рассмотрим последовательность событий более подробно:

1. встроенное устройство переходит в аварийный режим (переход осуществляется при соответствующем звуковом и световом оповещении);
2. наличие номера карты пользователя проверяется в локальной базе данных доступа;
3. локальная база данных доступа присылает ответ, содержащий: имя пользователя, уникальный идентификатор смарт-карты, тип доступа (true/false);
4. в локальном журнале формируется запись о произошедшем событии.

Постусловие: если прецедент выполнен успешно (тип доступа = true), тогда дверь открывается, а информация о пользователе и предоставлении доступа выводится на дисплей встроенного устройства. В противном случае, информация о пользователе и отказе в доступе выводится на дисплей встроенного устройства.

Прецедент: завершение сеанса с операционной системой

Краткое описание: данный прецедент описывает процесс завершения работы пользователя с операционной системой рабочей станции, принадлежащей организации.

Актор: пользователь (сотрудник или администратор).

Зависимость: нет.

Предусловие: пользователь начал сеанс с операционной системой.

Основной поток событий: данный прецедент начинает выполняться, когда пользователь пытается завершить сеанс работы с операционной системой рабочей станции, принадлежащей организации. Рассмотрим последовательность событий более подробно:

1. пользователь (сотрудник или администратор) завершает сеанс работы с операционной системой;
2. формируется журнальная запись о произошедшем событии.

Альтернативные потоки событий: отсутствуют.

Постусловие: если прецедент выполнен успешно, то пользователь завершает сеанс работы с операционной системой. В противном случае, состояние системы не изменяется.

Прецедент: вход в систему.

Краткое описание: данный прецедент описывает процесс входа сотрудника отдела организации в приложение администратора для управления системой контроля и управления доступом.

Актор: отдел.

Зависимость: нет.

Предусловие: отсутствует.

Основной поток событий: данный прецедент начинает выполняться, когда сотрудник отдела организации пытается войти в приложение администратора для управления системой контроля и управления доступом. Рассмотрим последовательность событий более подробно:

1. ввод пары логин/пароль;
2. введенная пара логин/пароль пересылается на сервер доступа, где осуществляется проверка, на основе которой формируется ответ о предоставлении доступа к приложению администратора или отказе в его предоставлении;
3. формируется журнальная запись о произошедшем событии.

Альтернативные потоки событий: при отсутствии соединения с сервером, а также вводе неверной пары логин/пароль формируется соответствующее уведомление о произошедшей ошибке.

Постусловие: если прецедент выполнен успешно, то сотрудник отдела входит в приложение администратора для управления системой контроля и управления доступом, при этом ему предоставляются соответствующие его отделу права по редактированию и просмотру данных. В противном случае, во входе в приложение администратора будет отказано.

Прецедент: начало сеанса с операционной системой.

Краткое описание: данный прецедент описывает процесс начала работы пользователя с операционной системой рабочей станции, принадлежащей организации.

Актор: пользователь (сотрудник или администратор).

Зависимость: нет.

Предусловие: отсутствует.

Основной поток событий: данный прецедент начинает выполняться, когда пользователь пытается начать сеанс работы с операционной системой рабочей станции, принадлежащей организации. Рассмотрим последовательность событий более подробно:

1. пользователь вводит пару логин/пароль;
2. система проверяет пару логин/пароль и предоставляет доступ к операционной системе рабочей станции или отказывает в предоставлении доступа к операционной системе рабочей станции;
3. агент рабочей станции анализирует ответ операционной системы;
4. формируется журнальная запись о произошедшем событии.

Альтернативные потоки событий: отсутствуют.

Постусловие: если прецедент выполнен успешно, то пользователь начинает сеанс работы с операционной системой. В противном случае, состояние системы не изменяется.

Прецедент: операции над встроенными устройствами.

Краткое описание: данный прецедент описывает процесс СУПО (создать, удалить, посмотреть, обновить) пользователя (сотрудника или администратора) над встроенными устройствами системы контроля и управления доступом.

Актор: технический отдел или отдел безопасности (только просмотр).

Зависимость: является обобщением прецедентов создать встроенное устройство, удалить встроенное устройство, посмотреть встроенное устройство, по-

лучить список состояния встроенных устройств, обновить встроенное устройство.

Предусловие: пользователь (сотрудник или администратор) вошел в систему с правами технического отдела или отдела безопасности (только просмотр).

Основной поток событий: данный прецедент начинает выполняться, когда пользователь (сотрудник или администратор) с правами технического отдела пытается совершить один из процессов СУПО над встроенными устройствами системы. Также, данный прецедент начинает выполняться, когда пользователь (сотрудник или администратор) с правами отдела безопасности осуществляет поиск информации о встроенных устройствах системы. Рассмотрим последовательность событий более подробно:

1. СУПО над встроенными устройствами:
   1.1.создание встроенного устройства;
   1.2.удаление встроенного устройства;
   1.3.просмотр встроенных устройств;
   1.4.обновление информации о встроенных устройствах;
2. формируется журнальная запись о произошедшем событии.

Альтернативные потоки событий: если в процессе реализации СУПО над встроенными устройствами системы, обнаружено, что один из процессов не может быть выполнен, то выдается уведомление о соответствующей ошибке.

Постусловие: если прецедент выполнен успешно, то осуществляется реализация СУПО над встроенными устройствами системы. В противном случае, выдается уведомление о соответствующей ошибке.

Прецедент: операции над гостями.

Краткое описание: данный прецедент описывает процесс СУПО (создать, удалить, посмотреть, обновить) пользователя (сотрудника или администратора) над пользователями с правами гостя в системе контроля и управления доступом.

Актор: отдел по работе с клиентами.

Зависимость: является обобщением прецедентов создать гостя, освободить карту гостя, обновить гостя, посмотреть актуальных гостей, посмотреть историю посещений.

Предусловие: пользователь (сотрудник или администратор) вошел в систему с правами отдела по работе с клиентами.

Основной поток событий: данный прецедент начинает выполняться, когда пользователь (сотрудник или администратор) с правами отдела по работе с клиентами пытается совершить один из процессов СУПО над пользователями с правами гостя в системе. Рассмотрим последовательность событий более подробно:

1. СУПО над пользователями с правами гостя:
   1.1. создание пользователя с правами гостя;
   1.2. освобождение смарт-карты, выданной пользователю с правами гостя;
   1.3. просмотр актуальных пользователей с правами гостя;
   1.4. просмотр истории посещений пользователей с правами гостя;
   1.5. обновление информации о пользователях с правами гостя;
2. формируется журнальная запись о произошедшем событии.

Альтернативные потоки событий: если в процессе реализации СУПО над пользователями с правами гостя в системе, обнаружено, что один из процессов не может быть выполнен, то выдается уведомление о соответствующей ошибке.

Постусловие: если прецедент выполнен успешно, то осуществляется реализация СУПО над пользователями правами гостя в системе. В противном случае, выдается уведомление о соответствующей ошибке.

Прецедент: операции над работниками.

Краткое описание: данный прецедент описывает процесс СУПО (создать, удалить, посмотреть, обновить) пользователя (сотрудника или администра-

тора) над пользователями с правами сотрудника или администратора в системе контроля и управления доступом.

Актор: отдел кадров или отдел безопасности (только просмотр).

Зависимость: является обобщением прецедентов создать работника, удалить работника, посмотреть работника, обновить работника.

Предусловие: пользователь (сотрудник или администратор) вошел в систему с правами отдела кадров или отдела безопасности.

Основной поток событий: данный прецедент начинает выполняться, когда пользователь (сотрудник или администратор) с правами отдела кадров пытается совершить один из процессов СУПО над пользователями правами сотрудника или администратора в системе. Также, данный прецедент начинает выполняться, когда пользователь (сотрудник или администратор) с правами отдела безопасности осуществляет поиск информации о пользователях с правами сотрудника или администратора в системе. Рассмотрим последовательность событий более подробно:

1. СУПО над пользователями правами сотрудника или администратора:
   1.1. создание пользователя с правами сотрудника или администратора;
   1.2. удаление пользователя с правами сотрудника или администратора;
   1.3. просмотр информации о пользователях с правами сотрудника или администратора;
   1.4. обновление информации о пользователях с правами сотрудника или администратора;
2. формируется журнальная запись о произошедшем событии.

Альтернативные потоки событий: если в процессе реализации СУПО над пользователями с правами сотрудника или администратора в системе, обнаружено, что один из процессов не может быть выполнен, то выдается уведомление о соответствующей ошибке.

Постусловие: если прецедент выполнен успешно, то осуществляется реализация СУПО над пользователями правами сотрудника или администратора в

системе. В противном случае, выдается уведомление о соответствующей ошибке.

Прецедент: операции над картами.

Краткое описание: данный прецедент описывает процесс СУП (создать, удалить, посмотреть) пользователя (сотрудника или администратора) над информацией о смарт-картах, зарегистрированных в системе контроля и управления доступом.

Актор: отдел кадров, отдел по работе с клиентами, отдел безопасности.

Зависимость: является обобщением прецедентов посмотреть свободные карты, удалить карту, создать карту.

Предусловие: пользователь (сотрудник или администратор) вошел в систему с правами отдела безопасности, или отдела кадров (только просмотр), или отдела по работе с клиентами (только просмотр).

Основной поток событий: данный прецедент начинает выполняться, когда пользователь (сотрудник или администратор) с правами отдела безопасности пытается совершить один из процессов СУП над информацией о смарт-картах, зарегистрированных в системе. Также, данный прецедент начинает выполняться, когда пользователь (сотрудник или администратор) с правами отдела по работе с клиентами или отдела кадров осуществляет поиск информации о смарт-картах, зарегистрированных в системе. Рассмотрим последовательность событий более подробно:

1. СУП над информацией о смарт-картах:
   1.1. создание (регистрация) смарт-карты;
   1.2. удаление смарт-карты;
   1.3. просмотр свободных смарт-карт;
2. формируется журнальная запись о произошедшем событии.

Альтернативные потоки событий: если в процессе реализации СУП над информацией о смарт-картах, зарегистрированных в системе, обнаружено,

что один из процессов не может быть выполнен, то выдается уведомление о соответствующей ошибке.

Постусловие: если прецедент выполнен успешно, то осуществляется реализация СУП над информацией о смарт-картах, зарегистрированных в системе. В противном случае, выдается уведомление о соответствующей ошибке.

Прецедент: операции над ролями.

Краткое описание: данный прецедент описывает процесс СУПО (создать, удалить, посмотреть, обновить) пользователя (сотрудника или администратора) над ролями пользователей в системе контроля и управления доступом.

Актор: отдел безопасности.

Зависимость: является обобщением прецедентов создать роль, удалить роль, посмотреть роль, обновить роль.

Предусловие: пользователь (сотрудник или администратор) вошел в систему с правами отдела безопасности.

Основной поток событий: данный прецедент начинает выполняться, когда пользователь (сотрудник или администратор) с правами отдела безопасности пытается совершить один из процессов СУПО над ролями пользователей в системе. Рассмотрим последовательность событий более подробно:

1. СУПО над ролями пользователей:
   1.1. создание роли пользователя;
   1.2. удаление роли пользователя;
   1.3. просмотр информации о ролях пользователей;
   1.4. обновление информации о ролях пользователей;
2. формируется журнальная запись о произошедшем событии.

Альтернативные потоки событий: если в процессе реализации СУПО над ролями пользователей в системе, обнаружено, что один из процессов не может быть выполнен, то выдается уведомление о соответствующей ошибке.

Постусловие: если прецедент выполнен успешно, то осуществляется реализация СУПО над ролями пользователей в системе. В противном случае, выдается уведомление о соответствующей ошибке.

Прецедент: операции над аккаунтами.

Краткое описание: данный прецедент описывает процесс СУПО (создать, удалить, посмотреть, обновить) пользователя (сотрудника или администратора) над аккаунтами пользователей в системе контроля и управления доступом.

Актор: отдел безопасности.

Зависимость: является обобщением прецедентов создать аккаунт, удалить аккаунт, посмотреть аккаунт, обновить аккаунт.

Предусловие: пользователь (сотрудник или администратор) вошел в систему с правами отдела безопасности.

Основной поток событий: данный прецедент начинает выполняться, когда пользователь (сотрудник или администратор) с правами отдела безопасности пытается совершить один из процессов СУПО над аккаунтами пользователей в системе. Рассмотрим последовательность событий более подробно:

1. СУПО над аккаунтами пользователей:
   1.1. создание аккаунта пользователя;
   1.2. удаление аккаунта пользователя;
   1.3. просмотр информации об аккаунтах пользователей;
   1.4. обновление информации об аккаунтах пользователей;
2. формируется журнальная запись о произошедшем событии.

Альтернативные потоки событий: если в процессе реализации СУПО над аккаунтами пользователей в системе, обнаружено, что один из процессов не может быть выполнен, то выдается уведомление о соответствующей ошибке.

Постусловие: если прецедент выполнен успешно, то осуществляется реализация СУПО над аккаунтами пользователей в системе. В противном случае, выдается уведомление о соответствующей ошибке.

Прецедент: анализ событий и генерация инцидентов безопасности.

Краткое описание: данный прецедент описывает процесс преобразования событий или отдельных прецедентов в системе контроля и управления доступом в инциденты безопасности.

Актор: сервер журналирования.

Зависимость: нет.

Предусловие: отсутствует.

Основной поток событий: данный прецедент начинает выполняться, когда на сервере журналирования формируются журнальные записи о произошедших событиях или прецедентах. Рассмотрим последовательность событий более подробно:

1. сопоставление текущего и предшествующего прецедента (события) в соответствии с допустимыми в системе последовательностями событий (конечными автоматами).

Альтернативные потоки событий: в ситуациях, когда допустимая последовательность событий (конечный автомат) в системе нарушена, формируется уведомление о произошедшем инциденте безопасности. Данная информация направляется сотруднику отдела безопасности.

Постусловие: в ситуациях, когда допустимая последовательность событий (конечный автомат) в системе не нарушается, система продолжает работать в нормальном режиме. В противном случае, информация о произошедшем инциденте направляется сотруднику отдела безопасности.

Прецедент: операции над политиками.

Краткое описание: данный прецедент описывает процесс ПО (посмотреть, обновить) пользователя (сотрудника или администратора) над политикой безопасности организации, введенной в системе контроля и управления доступом.

Актор: отдел безопасности.

Зависимость: является обобщением прецедентов посмотреть политику, изменить политику.

Предусловие: пользователь (сотрудник или администратор) вошел в систему с правами отдела безопасности.

Основной поток событий: данный прецедент начинает выполняться, когда пользователь (сотрудник или администратор) с правами отдела безопасности пытается совершить один из процессов ПО (посмотреть, обновить) над политикой безопасности, введенной в системе. Рассмотрим последовательность событий более подробно:

1. ПО над политикой безопасности:
   1.1. просмотр политики безопасности;
   1.2. обновление политики безопасности;
2. формируется журнальная запись о произошедшем событии.

Альтернативные потоки событий: если в процессе реализации ПО над политикой безопасности, введенной в системе, обнаружено, что один из процессов не может быть выполнен, то выдается уведомление о соответствующей ошибке.

Постусловие: если прецедент выполнен успешно, то осуществляется реализация ПО над политикой безопасности организации, введенной в системе. В противном случае, выдается уведомление о соответствующей ошибке.

Прецедент: журналирование.

Краткое описание: данный прецедент описывает процесс передачи на сервер журналирования журнальных записей, сформированных в результате выполнения операций СУО (создать, удалить, обновить) над объектами базы данных сервера доступа пользователями (сотрудниками или администраторами) с правами одного из отделов организации в системе. Кроме того, данный прецедент описывает процесс передачи журнальных записей от встроенных устройств и агентов рабочих станций на сервер журналирования.

Актор: технический отдел, отдел по работе с клиентами, отдел кадров, отдел безопасности, встроенное устройство, агенты рабочих станций.

Зависимость: нет.

Предусловие: выполнена одна из операций СУО (создать, удалить, обновить) в рамках следующих прецедентов: операции над встроенными устройствами, операции над гостями, операции над работниками, операции над картами, операции над ролями, операции над аккаунтами, операции над политиками. Или выполнен один из следующих прецедентов: вход в помещение, выход из помещения, начало сеанса с операционной системой, завершение сеанса с операционной системой.

Основной поток событий: данный прецедент начинает выполняться, когда журнальные записи, сформированные в результате выполнения операций СУО (создать, удалить, обновить) над объектами сервера доступа пользователями (сотрудниками или администраторами) с правами одного из отделов организации в системе, пересылаются на сервер журналирования. Кроме того, данный прецедент начинает выполняться, когда журнальные записи, сформированные в результате выполнения прецедентов вход в помещение, выход из помещения, начало сеанса с операционной системой, завершение сеанса с операционной системой. Рассмотрим последовательность событий более подробно:

1. получение журнальной записи, сформированной в результате выполнения операций СУО (создать, удалить, обновить) над объектами сервера доступа или выполнения прецедентов вход в помещение, выход из помещения, начало сеанса с операционной системой, завершение сеанса с операционной системой;
2. проверка журнальной записи на соответствие стандарту Syslog;
3. внесение журнальной записи в базу данных сервера журналирования.

Альтернативные потоки событий: в ситуациях, когда журнальная запись не соответствует стандарту Syslog, поля сформированной журнальной записи

преобразуются для разрешения данного несоответствия. Преобразованная журнальная запись вносится в базу данных сервера журналирования.

Постусловие: в ситуациях, когда сформированная журнальная запись соответствует стандарту Syslog, система продолжает работать в нормальном режиме. В противном случае, сформированная журнальная запись преобразуется для разрешения данного несоответствия.

Более подробно прецедент операции над встроенными устройствами (приложение А), прецедент операции над гостями (приложение Б), прецедент операции над работниками (приложение В), прецедент операции над картами (приложение Г), прецедент операции над ролями (приложение Д), прецедент операции над аккаунтами (приложение Е), прецедент операции над политиками (приложение Ж) рассмотрены в соответствующих приложениях к данной выпускной квалификационной работе.

3.3. Выбор компонентного состава

В соответствии с функциональными требованиями, каждая из рассматриваемых альтернатив должна поддерживать взаимодействие с внешними электронными компонентами: механическими замками, сканерами бесконтактных карт технологии RFID, инфракрасными датчиками движения, устройствами вывода текстовой, звуковой информации, звуковых и световых сигналов. Набор внешних электронных компонент может быть сведён в едином представлении (таблица 7).

Механический замок TowerPro SG90 потребляет 550 мА·ч [23], но только в момент открытия двери. Сканер бесконтактных карт технологии RFID Grove 125KHz RFID Reader потребляет 50 мА·ч [24] на постоянной основе. Инфракрасный датчик движения PIR Motion Sensor HC-SR501 потребляет 0.05 мА·ч [23] на постоянной основе. Устройство вывода текстовой информации DC 5V Character LCD 16x2 потребляет 100 мА·ч [25], но только при поднесении бесконтактной карты к сканеру бесконтактных карт техноло-

гии RFID. Устройство вывода звуковых сигналов DC 12mA 5V 12mm Piezo Alarm Buzzer потребляет 12 мА·ч [26], но только при обнаружении человека, вошедшего в помещение и не приложившего карту. Устройство вывода световых сигналов RGB Light-emitting Diode потребляет 20 мА·ч [26] на постоянной основе. Максимальное энергопотребление внешних электронных компонентов составляет 732,05 мА·ч. Минимальное энергопотребление внешних электронных компонентов составляет 70,05 мА·ч. Опытным путём было установлено среднее энергопотребление внешних электронных компонент, которое составляет около 200 мА·ч.

Таблица 7 – Набор внешних электронных компонентов

Внешний электронный компонент	Выбранное физическое устройство	Потребление (мА·ч)	Стоимость (руб.)
механический замок	TowerPro SG90	550 (в момент подачи сигнала)	764
сканер бесконтактных карт технологии RFID	Grove 125KHz RFID Reader	50	1249
инфракрасный датчик движения	PIR Motion Sensor HC-SR501	0.05	209
устройство вывода текстовой информации	DC 5V Character LCD 16x2	100 (в момент подачи сигнала)	347
устройство вывода звуковых сигналов	DC 12mA 5V 12mm Piezo Alarm Buzzer	12 (в момент подачи сигнала)	209
устройство вывода световых сигналов	RGB Light-emitting Diode	20	7
Итого		70.05 – 732.05 (среднее – 300)	2785

Набор внешних электронных компонентов будет единым, поэтому в методике проектирования не будет осуществляться поиск альтернатив для каждого из внешних электронных компонентов. Влияние набора внешних электронных компонентов на нефункциональные требования будет учтено при принятии оптимального с точки зрения нефункциональных требований решения. С учетом функциональных требований, на выходе методики, были сформированы альтернативы, которые могут быть сведены в едином представлении (таблица 8).

При анализе энергоэффективности отдельных компонентов и устройств использовались как источники в сети Интернет, так и эксперименты с реальным оборудованием.

Энергоэффективность альтернативы № 1, включает в себя энергопотребление Arduino Yun и набора внешних электронных компонент. Энергопотребление микроконтроллера Arduino Yun, в свою очередь, зависит от степени нагрузки процессора и может варьироваться между 200 и 250 мА·ч [27]. Таким образом, энергоэффективность альтернативы № 1 составляет 500-550 мА·ч.

Энергоэффективность альтернативы № 2, включает в себя энергопотребление Raspberry Pi B+, Wi-Pi модуль и набора внешних электронных компонентов. Минимальное энергопотребление Raspberry Pi B+ без подключенных внешних устройств составляет 600 мА·ч [28]. Потребление Wi-Pi модуля составляет 450 мА·ч [28]. Таким образом, энергоэффективность альтернативы № 2 составляет 1350 мА·ч.

Энергоэффективность альтернативы № 3, включает в себя энергопотребление Beaglebone Black, Compact USB Wi-Fi Adapter и набора внешних электронных компонент. Энергопотребление Beaglebone Black составляет 210-460 мА·ч [29]. Потребление Compact USB Wi-Fi Adapter составляет 120 мА·ч (получено экспериментально). Таким образом, энергоэффективность альтернативы № 3 составляет 780 мА·ч.

Таблица 8 – Альтернативы, выбранные при помощи методики

№	Альтернатива	Описание
1	Arduino Yun, microSD 512 MB	Внутренняя память Arduino Yun ограничена 8 MB, чего недостаточно для соответствия функциональным требованиям к программному обеспечению. Внутреннюю память Arduino Yun можно расширить с помощью microSD.
2	Raspberry Pi B+, Wi-Pi модуль	Raspberry Pi B+ не поддерживает передачу данных по беспроводному каналу передачи данных, а потому не соответствует одному из функциональных требований к аппаратному обеспечению. Wi-Pi модуль разработан специально для Raspberry Pi, чтобы нивелировать данный недостаток.
3	Beaglebone Black, Compact USB Wi-Fi Adapter	Beaglebone Black не поддерживает передачу данных по беспроводному каналу передачи данных, а потому не соответствует одному из функциональных требований к аппаратному обеспечению. Compact USB Wi-Fi Adapter разработан специально для Beaglebone Black, чтобы нивелировать данный недостаток.
4	Intel Galileo Gen 2P Board, Intel Galileo Wi-Fi Kit	Intel Galileo Gen 2P Board не поддерживает передачу данных по беспроводному каналу передачи данных, а потому не соответствует одному из функциональных требований к аппаратному обеспечению. Intel Galileo Wi-Fi Kit разработан специально для Intel Galileo Gen 2P Board, чтобы нивелировать данный недостаток.

Энергоэффективность альтернативы № 4, включает в себя энергопотребление Intel Galileo Gen 2P Board, Intel Galileo Wi-Fi Kit и набора внешних электронных компонент. Минимальное энергопотребление Intel Galileo Gen

2P Board без подключенных внешних устройств составляет 800 мА·ч [30]. Потребление Intel Galileo Wi-Fi Kit составляет около 400 мА·ч [30]. Таким образом, энергоэффективность альтернативы № 4 составляет 1400 мА·ч.

Стоимости микроконтроллеров и специфичных для них элементов сформированы исходя из официальных предложений разработчиков и их дистрибьюторов. Более дешёвые аналоги (реплики) не рассматриваются, так как невозможно гарантировать их степень совместимости с общим набором внешних компонент. Стоимость не специфичных компонентов сформирована исходя из предложений электронного магазина Amazon (http://www.amazon.com). Стоимость внешних компонентов, включая механический замок, сканер бесконтактных карт технологии RFID, инфракрасный датчик движения, устройства вывода текстовой информации, звуковых и световых сигналов составляет 2785 рублей. Рассмотрим особенности предлагаемых альтернатив, которые также влияют на общую цену:

- в стоимость альтернативы № 1 входят: Arduino Yun – 3608 рублей [31], Micro SD карта – 139 рублей [23]. Итоговая стоимость с учетом внешних электронных компонентов – 6532 рубля.
- в стоимость альтернативы № 2 входят: Raspberry Pi B+ – 1596 рублей [32], Wi-Pi модуль – 764 рубля [32]. Итоговая стоимость с учётом внешних электронных компонентов – 5145 рублей.
- в стоимость альтернативы № 3 входят: Beaglebone Black – 3469 рублей [33], Compact USB Wi-Fi Adapter - 764 рубля [23]. Итоговая стоимость с учетом внешних электронных компонентов – 7018 рублей.
- в стоимость альтернативы № 4 входят: Intel Galileo Gen 2P Board – 4302 рубля [34], Intel Galileo Wi-Fi Kit – 3123 рубля [34]. Итоговая стоимость с учётом внешних электронных компонентов – 10210 рублей.

Размеры встроенного устройства напрямую зависят от размера их самой большой части – микроконтроллеров. Толщина всех микроконтрол-

леров соответствует ограничению в три сантиметра (при непосредственном встраивании в дверь). Результаты, полученные в результате анализа альтернатив по нефункциональным требованиями, могут быть сведены в едином представлении (таблица 9).

Таблица 9 – Сравнение альтернатив по нефункциональным требованиям

	Потребление энергии (мА·ч)	Стоимость (руб.)	Размер ($мм^3$)
Arduino Yun, microSD 512 MB	550	6532	73x53x8
Raspberry Pi B+, Wi-Pi модуль	1350	5145	60x36x7
Beaglebone Black, Compact USB Wi-Fi Adapter	780	7018	86x53x7
Intel Galileo Gen 2P Board, Intel Galileo Wi-Fi Kit	1400	10210	123x72x9

Альтернатива № 1 показывает лучшую энергоэффективность при средней стоимости. Альтернатива № 2 имеет малую энергоэффективность, однако, ее стоимость значительно ниже приведенных аналогов, что даёт основания для рассмотрения и этого варианта. Альтернатива № 3 имеет энергоэффективность и стоимость аналогичную стоимости альтернативы № 1, но всё же несколько уступает ей. Таким образом, альтернативу № 3 можно далее не рассматривать. Альтернатива № 4 является наиболее дорогим и наименее энергоэффективным решением в сравнении с остальными наборами компонентов. Дальнейшее рассмотрение альтернативы № 4 нецелесообразно.

Требование энергоэффективности подразумевает, что встроенное устройство способно поддерживать функционирование в условиях выхода из строя электрической цепи, к которой подсоединено встроенное устройство, за счёт энергии резервного источника питания. Время работы от резервного источника питания для различных альтернатив зависит от емкости источника резервного питания. Для работы альтернатив № 1 и № 2 (таблица 5) от источника резервного питания на протяжении 24 часов необходимы аккумуляторы со следующими емкостями: альтернатива № 1 - 13000 мА·ч, альтернатива № 2 - 32000 мА·ч. Необходимая емкость была рассчитана на основе полученных ранее значений среднего энергопотребления.

В качестве источников резервного питания рассматриваются power bank, т.к. их размер соответствует нефункциональным требованиям. Стоимость power bank зависит от емкости и количества поддерживаемых циклов перезарядки и равна: 1041 рубль и 13876 рублей для ёмкостей в 15000 мА·ч и 40000 мА·ч [23]. Таким образом, итоговая стоимость эксплуатации альтернативы № 2 составляет 19021 рубль, если учитывать стоимость источника резервного питания. Это значительно выше, чем итоговая стоимость альтернативы № 1, которая составляет 7573 рубля.

С учетом вышесказанного, оптимальным набором компонентов защиты является альтернатива № 1. Итоговый набор компонентов встроенного устройства: Arduino Yun, microSD 512 MB, TowerPro SG90, Grove 125KHz RFID Reader, PIR Motion Sensor HC-SR501, DC 5V Character LCD 16x2, DC 12mA 5V 12mm Piezo Alarm Buzzer, RGB Light-emitting Diode, power bank 15000 мА·ч; стоимостью 7573 рубля и средним энергопотреблением 550 мА·ч.

3.4. Программно-аппаратный прототип

Программно-аппаратный прототип защищенной системы контроля и управления доступом представлен на рисунке 7:

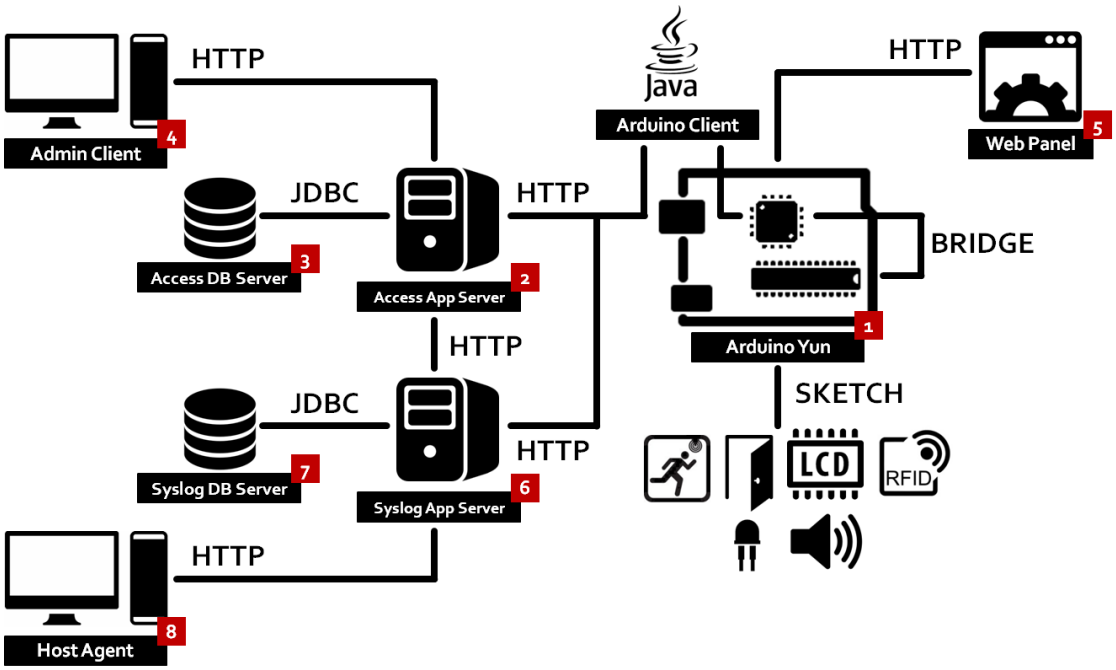

Рисунок 7 – Программно-аппаратный прототипа системы

Микроконтроллер Arduino Yun (1) состоит из двух частей:

- Процессор ATmega 32U4 (выполняет требования № 2, 3, таблица 2, раздел 1.1), управляющий через sketch [35] механическим замком, сканнером бесконтактных карт технологии RFID, текстовым экраном, инфракрасным датчиком движения, компонентами вывода световых и звуковых сигналов.
- Процессор AR9331 под управлением Linux (выполняет требования № 1, 5, таблица 2, раздел 1.1), содержит клиентское приложение (Arduino Client, выполняет требования № 4, 7, таблица 2, раздел 1.1), которое выполняет роль посредника между ATmega 32U4 и сервером приложений центрального сервера доступа (Access App Server), а также формирует журнальные записи, связанные с событиями входа пользователей в помещение и выхода пользователей из помещения.

Сервер приложений центрального сервера доступа (2) предоставляет удаленный доступ к базе данных центрального сервера доступа (Access DB Server) для клиентского приложения на микроконтроллере (Arduino Client) и

приложения для администрирования (Admin Client), а также формирует журнальные записи, связанные с работой приложения для администрирования (Admin Client).

База данных центрального сервера доступа (3) содержит в себе информацию о пользователях системы, бесконтактных картах, ролях пользователей, устройствах и правах доступа к помещениям для каждой из ролей.

Приложение для администрирования (4) осуществляет управление информацией, хранящейся в базе данных центрального сервера доступа (Access DB Server), формирует журнальные записи, связанные с действиями администратора.

Панель управления (5) используется для отображения записей локального журнала встроенного устройства, для инициализации обновления локальной базы доступа, а также для конфигурирования устройства при локальном Ethernet подключении (выполняет требования № 6, 8, таблица 2, раздел 1.1).

Сервер приложений центрально сервера журналирования (6) предоставляет удалённый доступ к базе данных центрального сервера журналирования (Syslog DB Server), а также осуществляет генерацию инцидентов безопасности на основе анализа причинно-следственных связей журнальных записей.

База данных центрального сервера журналирования (7) содержит информацию о событиях и инцидентах безопасности, происходящих в системе.

Агенты рабочих станций (8) формируют журнальные записи, связанные с событиями начала и завершения сеанса пользователя с операционной системой.

Рассмотрим элементы архитектуры системы контроля и управления доступом, а также их взаимодействие более подробно.

В процессор ATmega 32U4 (1.1) загружается код, который называется sketch. Любой sketch можно условно разделить на три части: блок инициализации, блок прошивки, блок исполнения. В блоке инициализации подключа-

ются необходимые для работы sketch библиотеки, объявляются глобальные переменные, задаются специальные обозначения для цифровых или аналоговых PIN. В блоке прошивки (setup(){}) осуществляется настройка Arduino Yun (1), ее подготовка для выполнения функционала, необходимого в блоке исполнения. Блок исполнения (loop(){}) циклически выполняет записанный в нём код, представляя собой сердце sketch, его алгоритмическое ядро.

Взаимосвязь между ATmega 32U4 (1.1) и AR9331 Linux (1.2) процессорами Arduino Yun (1) осуществляется при помощи библиотек Bridge.h и FileIO.h [35]. Библиотека Bridge.h позволяет запускать shell-команды прямо из sketch, а FileIO.h позволяет считывать файлы и записывать файлы, принадлежащие файловой системе Linux.

Запуск клиентского приложения на микроконтроллере (Arduino Client) осуществляется из sketch благодаря библиотеке Bridge.h посредством выполнения асинхронной (без ожидания завершения) shell-команды. Дальнейшее взаимодействие между sketch и клиентским приложением строится на обработке (чтение/запись) специальных текстовых (.txt) файлов. Это происходит относительно быстро благодаря использованию библиотеки FileIO.h. Запись осуществляется в специальном формате, напоминающем HTTP.

Клиентское приложение на микроконтроллере (Arduino Client) представлено jar-приложением [36]. Работу jar-приложения клиента можно разделить на два этапа: инициализация и функционирование. При инициализации происходит проверка доступности сервера приложений центрального сервера доступа (2), настройка параметров взаимодействия между процессорами AR9331 и ATmega, а также копирование идентификационных данных пользователей с правами администратора из базы данных центрального сервера доступа (3) в локальную базу данных и из неё в кэш приложения. Локальная база данных необходима на случай, если сервер приложений центрального сервера доступа (2) станет недоступен. На этапе функционирования, предусмотрено разбиение главного потока на прикладные. Каждый поток будет обрабатывать запросы, приходящие от Arduino Yun (1), с некоторой перио-

дичностью. В данный момент реализовано четыре потока: первый обрабатывает запросы на получение доступа в помещение, второй проверяет соединение с сервером приложений центрального сервера доступа (2), третий обеспечивает формирование журнальных записей, четвертый обновляет локальную базу данных с некоторой периодичностью или по запросу от панели управления (5).

Также, при помощи sketch, реализована панель управления (5) – веб-страница, позволяющая просматривать локальные журнальные записи устройства и инициировать обновления локальной базы данных. Для получения доступа к веб-странице необходимо прямое подключение к микроконтроллеру Arduino Yun (1) через Ethernet-кабель, а также прохождение процедуры аутентификации.

Сервера приложений центрального сервера доступа (2) и центрального сервера журналирования (6) представлены каталогом сервлетов Tomcat [37], на котором развернуто war-приложение, разрабатываемого в рамках фреймворка Spring [38]. Данный фреймворк имеет готовые решения в области доступа к базам данных (пакет DAO Support) и базовых требований к безопасности (пакет Spring Security).

Посредником между war-приложением и базами данных центрального сервера доступа (3) и центрального сервера журналирования (7) является пулл соединений C3P0 [39], который основан на JDBC [40]. C3P0 обеспечивает большую гибкость соединения: он позволяет распределять подключения к базе данных для разных пользователей с разными правами, а также имеет механизмы управления нагрузками.

База данных центрального сервера доступа (3) содержит в себе информацию о пользователях системы, бесконтактных картах, ролях пользователей, устройствах и правах доступа на эти устройства для каждой из ролей. База данных центрального сервера доступа (3) основана на реляционной системе управления базами данных PostgreSQL [41].

База данных центрального сервера журналирования (7) содержит информацию о событиях и инцидентах безопасности, происходящих в системе. База данных центрального сервера журналирования (7) также основана на реляционной системе управления базами данных PostgreSQL.

Приложение администратора (4) представлено jar-приложением, запуск которого осуществляет пользователь системы с правами администратора, после предварительного прохождения процедуры аутентификации путем ввода логина и пароля.

Агенты рабочих станций (8) представлены jar-приложением, которое осуществляет мониторинг сеанса пользователя с операционной системой, а также формирует соответствующие журнальные записи при успешной/неуспешной попытке входа/выхода пользователя из системы. При этом агенты рабочих станций (8) отправляют журнальные записи на сервер приложений центрального сервера журналирования (6) с информацией о параметрах входа пользователя в систему. При отсутствии сети (как правило, сеть появляется через несколько секунд после входа пользователя в систему), агенты рабочих станций (8) пытаются отправить сообщение через определенный интервал времени, вплоть до успешной отправки или выхода пользователя из системы.

4. РАССЧЕТ ТЕХНИКО-ЭКОНОМИЧЕСКИХ ПОКАЗАТЕЛЕЙ

4.1. Расчет технических показателей

Расчет технических показателей будет осуществляться в соответствии с методиками оценки систем на основе встроенных устройств, представленными в разделе 2 данной выпускной квалификационной работы.

4.1.1. Оценка защищенности

Оценка защищенности программно-аппаратного прототипа встроенного устройства системы контроля и управления доступом будет осуществляться посредством статического тестирования (раздел 2.2). При этом для автоматизации процесса статического тестирования, а также реализации предложенной методики оценки защищенности для сетей встроенных устройств было разработано специально программное обеспечение на высокоуровневом языке программирования Java (рисунок 8).

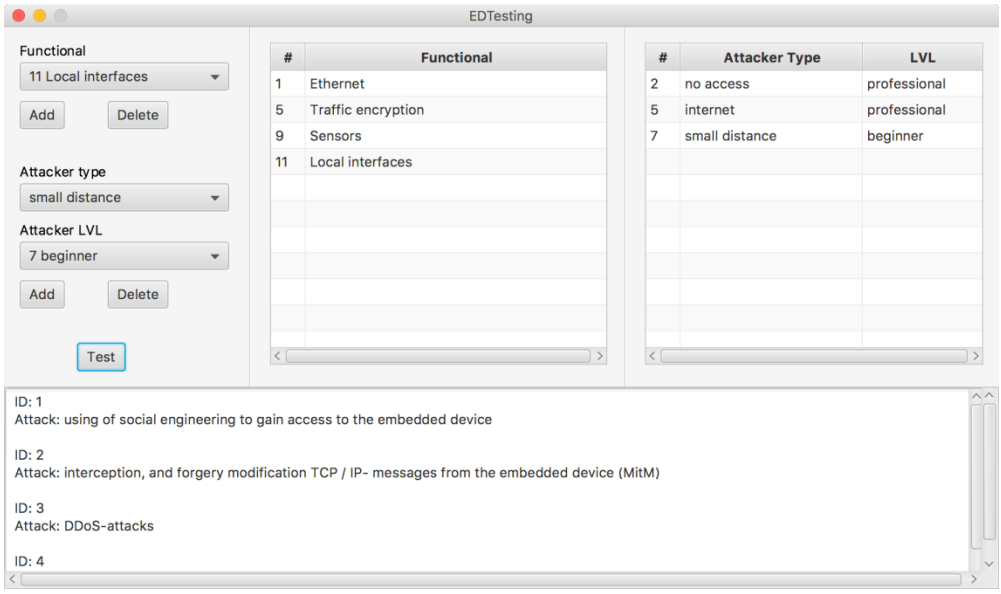

Рисунок 8 – Интерфейс пользователя

Направим на статическое тестирование набор компонентов встроенного устройства: Arduino Yun, microSD 512 MB, TowerPro SG90, Grove 125KHz RFID Reader, PIR Motion Sensor HC-SR501, DC 5V Character LCD 16x2, DC 12mA 5V 12mm Piezo Alarm Buzzer, RGB Light-emitting Diode, power bank 15000 мА·ч.

Использование разработанного прототипа защищенной системы контроля и управления доступом предполагается для ограничения доступа в заданные помещения внутри контролируемой зоны организации. При этом защита предполагается от нарушителей типа 0 и типа 1 уровня 1.

Рассмотрим возможные атаки на систему: (1) использование социальной инженерии для получения доступа к инфраструктуре и сервисам системы контроля и управления доступом; (2) перехват, модификация и подделка TCP/IP-сообщений между элементами системы посредством Ethernet-интерфейса; (3) атаки типа отказ в обслуживании на инфраструктуру и сервисы системы; (4) перехват, модификация и подделка сообщений между элементами системы посредством Wi-Fi.

Т.к. нарушители уровня 1 используют только публично доступное программное обеспечение, а также общеизвестные уязвимости, то для защиты от перечисленных атак необходимо заложить в бизнес-логику системы следующие решения: (1) обучение персонала для предотвращения атак на основе социальной инженерии; (2),(4) шифрование передаваемых между элементами системы сообщений криптографически стойким алгоритмом, а также наличие взаимной аутентификации между элементами системы; (3) настройка межсетевых экранов для элементов системы, расположенных на границе демилитаризованной зоны локальной сети организации.

Таким образом, разработанная система контроля и управления доступом, в основу бизнес-логики которой на этапе проектирования были заложены соответствующие компоненты защиты, является защищенной относительно нарушителей уровня 1, типа 0,1.

4.1.2. Оценка оперативности

Целевой функцией применения системы контроля и управления доступом для идентификации пользователей системы, а также обнаружения нарушений политики безопасности организации с учетом требования оперативно-

сти является минимизация времени $TIME_N \to min$, необходимого для проведения данных операций, при соблюдении требований к другим свойствам:

- к оперативности $P_{\text{ОП}}(TIME_N \le TIME^{\text{ДОП}}) \ge P_{\text{ОП}}^{\text{ДОП}}$, где $P_{\text{ОП}}^{\text{ДОП}} = 0.99$, допустимое время проверки идентификационных данных пользователей $TIME^{\text{ДОП}} =$ 0.5 сек для, и допустимое время для обнаружения нарушений политики безопасности организации $TIME^{\text{ДОП}} =$ 3.0 сек.
- к обоснованности $POL_N \ge \max\limits_{s \in S} POL_N^S$ и $PARAMS \ge \max\limits_{s \in S} PARAMS^S$, где POL_N и $PARAMS$ – количество обнаруженных нарушений политики безопасности организации для помещения N и учитываемых параметров для идентификации пользователя системы контроля и управления доступом соответственно, S – множество возможных состояний пользователя в системе, POL_N^S и $PARAMS^S$ – количество обнаруженных нарушений политики безопасности организации, а также учитываемых параметров для идентификации пользователя системы контроля и управления доступом для состояния пользователя $s \in S$.
- к ресурсопотреблению $P_{\text{РЕС}}(r \le R^{\text{ДОП}}) \ge P_{\text{РЕС}}^{\text{ДОП}}$, где $P_{\text{РЕС}}^{\text{ДОП}} = 0.99$, $R^{\text{ДОП}} = 0.75$ (75% от общего объема ресурсов, доступных приложениям) для следующих видов ресурсов: оперативная память, флеш-память, объем жесткого диска, использованное процессорное время.

Взаимодействие элементов системы контроля и управления доступом для идентификации пользователей системы, а именно центрального сервера доступа, центрального сервера журналирования, клиентского приложения на микроконтроллере, приложения для администрирования и агентов рабочих станций осуществляется в рамках сетевого соединения посредством HTTP сообщений. Данная технология была выбрана, т.к. сообщения надежны, легко поддаются регулированию, поддерживают асинхронное взаимодействие и обеспечивают легкую интеграцию. Сообщения формируются по принципу построения GET запросов, т.к. подобная структура устойчива к ошибкам.

Таким образом, длительность процесса идентификации пользователей системы контроля и управления доступом будет складываться из продолжительности каждого из рассматриваемых этапов:

$$TIME^{ИД} = T_1^{ИД} + T_2^{ИД} + T_3^{ИД} \quad (9)$$

где $T_1^{ИД}$ – время взаимодействия микроконтроллера со считывателем бесконтактных карт технологии RFID и средствами вывода звуковых и световых сигналов, $T_2^{ИД}$ – время подготовки микроконтроллером данных для передачи на центральный сервер доступа, $T_3^{ИД}$ – время взаимодействия между центральным сервером доступа и микроконтроллером.

Длительность процесса обнаружения нарушений политики безопасности организации также будет складываться из продолжительного каждого из этапов данного процесса:

$$TIME^{ПБ} = T_1^{ПБ} + T_2^{ПБ} + T_3^{ПБ} \quad (10)$$

где $T_1^{ПБ}$ – время процесса сбора данных от источников физического и кибернетического уровня с последующей нормализацией и предобработкой полученных данных, $T_2^{ПБ}$ – время процесса корреляции событий безопасности, полученных от модуля сбора данных, в модуле обработки событий, $T_3^{ПБ}$ – время процесса представления полученных результатов человеку-оператору в модуле аналитической обработки и визуализации данных.

Время выполнения этапов рассматривается как случайная величина, вероятность которой подчиняется нормальному закону распределения [42]. При этом для оценки времени выполнения наиболее часто применяется закон бета-распределения в интервале $[t_{min}, t_{max}]$ с плотностью распределения [43]:

$$f(t) = \begin{cases} \dfrac{(t - t_{min})^{\alpha-1}(t_{max} - t)^{\beta-1}}{(t_{max} - t_{min})^{\alpha+\beta-1}B(\alpha, \beta)}, t_{min} \le t \le t_{max}, \\ 0, t_{max} \le t \le t_{min} \end{cases} \quad (11)$$

где t_{min} и t_{max} – минимальное и максимальное время выполнения соответственно, t – величина, определяющая время выполнения, $B(\alpha, \beta)$ – функция Эйлера, $\alpha > 0$, $\beta > 0$ – параметры бета-распределения.

Ожидаемое время выполнения процесса проверки идентификационных данных пользователей, а также процесса обнаружения нарушений политики безопасности организации и их дисперсия рассчитываются с помощью двухоценочной методики [42]:

$$T_i = \frac{3T_i^{min} + 2T_i^{max}}{5}, \sigma^2(T_i) = 0.4(T_i^{max} - T_i^{min})^2 \quad (12)$$

Вероятность того, что время выполнения этапа в целом будет не выше допустимого значения $TIME^{\text{ДОП}}$, вычисляется по формуле:

$$P_{CB}(TIME \leq TIME^{\text{ДОП}}) = \Phi(Z) \quad (13)$$

где $\Phi(Z)$ – значение функции Лапласа при:

$$Z = \frac{TIME^{\text{ДОП}} - \sum_{i=1}^{n} T_i}{\sqrt{\sum_{i=1}^{n} \sigma_i^2(T_i)}} \quad (14)$$

На основе проведенных экспериментов были получены основные временные показатели этапов выполнения процессов идентификации пользователей системы контроля и управления доступом и обнаружения нарушений политики безопасности организации. Полученные значения приведены таблицах 10 и 11 соответственно.

Таблица 10 – Временные показатели процесса проверки идентификационных данных пользователей системы

Этап	T_i^{min}, мс	T_i^{max}, мс	$T_i = \frac{3T_i^{min} + 2T_i^{max}}{5}$	$\sigma^2(T_i) = 0.4(T_i^{max} - T_i^{min})^2$
1	26.80	32.20	28.96	11.664
2	300.30	320.20	308.26	158.404
3	42.10	48.20	44.54	14.884
Итого по этапу, мс			381.76	180.952

Таблица 11 – Временные показатели процесса обнаружения нарушений политики безопасности организации

Этап	T_i^{min}, мс	T_i^{max}, мс	$T_i = \frac{3T_i^{min} + 2T_i^{max}}{5}$	$\sigma^2(T_i) = 0.4(T_i^{max} - T_i^{min})^2$
1	369.20	400.60	381.76	394.384
2	620.10	680.30	644.18	1449.616
3	500.10	550.20	520.14	1004.004
Итого по этапу, мс			1546.08	2848.004

Тогда значение функции Лапласа $\Phi(Z)$ для $TIME^{\text{ДОП}} = 500$ мс для процесса проверки идентификационных данных пользователей системы контроля и управления доступом:

$$\Phi\left(\frac{TIME^{\text{ДОП}} - \sum_{i=1}^{n} T_i}{\sqrt{\sum_{i=1}^{n} \sigma_i^2(T_i)}}\right) = \left(\frac{500.00 - 381.76}{\sqrt{180.952}}\right) \cong 8.79$$

Для процесса обнаружения нарушений политики безопасности организации, функция Лапласа $\Phi(Z)$ для $TIME^{\text{ДОП}} = 3000$ мс:

$$\Phi\left(\frac{TIME^{\text{ДОП}} - \sum_{i=1}^{n} T_i}{\sqrt{\sum_{i=1}^{n} \sigma_i^2(T_i)}}\right) = \left(\frac{2000.00 - 1546.08}{\sqrt{2848.004}}\right) \cong 8.51$$

Таким образом, по значениям функции Лапласа, заданных в табличном виде для разработанного прототипа защищенной системы контроля и управления доступом вероятность выполнения процесса идентификации пользователей системы за заданное время составляет $P_{\text{ОП}}(TIME_N \leq TIME^{\text{ДОП}}) = 0.9999$, а вероятность выполнения процесса обнаружения нарушений политики безопасности организации за заданное время составляет $P_{\text{ОП}}(TIME_N \leq TIME^{\text{ДОП}}) = 0.9999$, что соответствует предъявляемым требованиям ($P_{\text{ОП}}^{\text{ДОП}} = 0.99$) к оперативности.

4.1.3. Оценка обоснованности

Во время проведения экспериментов, для идентификации пользователей системы контроля и управления доступом были использованы следующие данные для сотрудников организации: фамилия, имя и отчество; логин в операционной системе за выделенным рабочим местом; уникальный идентификатор карты. Для сотрудников с правами администратора, также использовались данные о логине в приложении для администрирования. Для идентификации гостей организации были использованы следующие данные: фамилия, имя и отчество, уникальный идентификатор карты.

Для проверки соответствия результатов обнаружения нарушений политики безопасности организации системой контроля и управления доступом заданному состоянию анализируемого помещения, в модуль обработки событий был заложен конечный автомат возможных состояний сотрудников организации с соответствующими переходами между ними (рисунок 9): S_1 – сотрудник вошел в офис; S_2 – сотрудник начал сеанс работы с операционной системой; S_3 – сотрудник завершил сеанс работы с операционной системой; S_4 – сотрудник вышел из офиса.

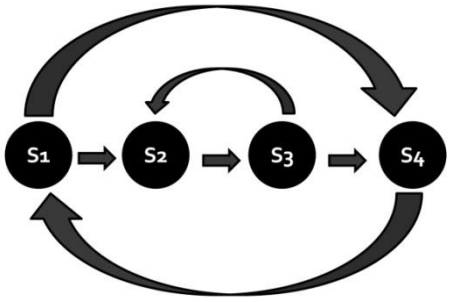

Рисунок 9 – Конечный автомат

Результаты экспериментов показали, что в течение рабочего дня, модуль обработки событий центрального сервера системы контроля и управления доступом с помощью методов на основе правил и машины конечных состояний выявлял все переходы между состояниями, нарушающие политику безопасности организации в рамках заложенного конечного автомата. Таким образом, можно сделать вывод о том, что значения обоснованности не уступает существующим аналогам и удовлетворяет требованиям.

4.1.4. Оценка ресурсопотребления

Оценка ресурсопотребления может быть проведена по ряду частных показателей. Рассмотрим каждый из них более подробно:

- использование центрального процессорного устройства

$$R_{\text{ЦП}} = \frac{Q_{\text{ЦП}}^{\text{ОБ}}}{Q_{\text{ЦП}}^{\text{ОБЩ}}} \tag{15}$$

где $Q_{\text{ЦП}}^{\text{ОБ}}$ – время центрального процессора, потраченное на процесс обнаружения нарушений политики безопасности организации и идентификации пользователей системы; $Q_{\text{ЦП}}^{\text{ОБЩ}}$ – общее доступное процессорное время;

- использование сетевого канала

$$R_{\text{СЕТЬ}} = \frac{Q_{\text{СЕТЬ}}^{\text{ОБ}}}{Q_{\text{СЕТЬ}}^{\text{ОБЩ}}} \tag{16}$$

где $Q_{\text{СЕТЬ}}^{\text{ОБ}}$ – общий объем переданных и полученных по сети данных при выполнении процесса обнаружения нарушений политики безопасности организации и идентификации пользователей системы; $Q_{\text{СЕТЬ}}^{\text{ОБЩ}}$ – максимальной возможных объем данных за тот же период;

- использование дискового пространства центрального сервера доступа, центрального сервера журналирования и микроконтроллера

$$R_{\text{ДП}} = \frac{Q_{\text{ДП}}^{\text{ОБ}}}{Q_{\text{ДП}}^{\text{ОБЩ}}} \tag{17}$$

где $Q_{\text{ДП}}^{\text{ОБ}}$ – объем дискового пространства, использованный при выполнении процесса обнаружения нарушений политики безопасности организации и идентификации пользователей системы, $Q_{\text{ДП}}^{\text{ОБЩ}}$ – общий объем дискового пространства;

- использование флеш-памяти микроконтроллера

$$R_{\text{ФП}} = \frac{Q_{\text{ФП}}^{\text{ОБ}}}{Q_{\text{ФП}}^{\text{ОБЩ}}} \tag{18}$$

где $Q_{\text{ФП}}^{\text{ОБ}}$ – объем дискового пространства, использованный при выполнении процесса обнаружения нарушений политики безопасности организации и

идентификации пользователей системы, $Q_{\text{ФП}}^{\text{ОБЩ}}$ – общий объем дискового пространства.

- использование оперативной памяти центрального сервера доступа, центрального сервера журналирования и микроконтроллера

$$R_{\text{ОП}} = \frac{Q_{\text{ОП}}^{\text{ОБ}}}{Q_{\text{ОП}}^{\text{ОБЩ}}} \tag{19}$$

где $Q_{\text{ОП}}^{\text{ОБ}}$ – объем оперативной памяти, использованный при выполнении процесса обнаружения нарушений политики безопасности организации и идентификации пользователей системы, $Q_{\text{ОП}}^{\text{ОБЩ}}$ – общий объем оперативной памяти.

Оценка ресурсопотребления соответствует заданной в требованиях, если все вышеперечисленные показатели соответствуют условию $r \leq R^{\text{ДОП}}$. Отметим, что в рамках прототипа разработанной системы контроля и управления доступом был выделен отдельный компьютер для выполнения задач центрального сервера доступа и центрального сервера журналирования, поэтому $R^{\text{ДОП}} = 0.75$ (25 % ресурсов компьютера выделяется на общие задачи операционной системы и сопутствующих программ).

При проведении экспериментов был выбран персональный компьютер, относящийся к стандартному рабочему месту программиста лаборатории проблем компьютерной безопасности ФГБУН СПИИРАН. Рассмотрим параметры данного компьютера более подробно:

- центральное процессорное устройство: Intel® Core(TM) i5-3427U CPU @1.80GHz (4 ядра);
- максимальная пропускная способность сетевого канала: 100 Мб/с;
- общий объем жесткого диска: 500 Гб;
- общий объем оперативной памяти: 4 Гб.

В процессе идентификации пользователей системы контроля и управления доступом, а также обнаружения нарушений политики безопасности организации каждое ядро центрального процессорного устройства было загру-

жено следующим образом: первое ядро – 25 %, второе ядро – 20 %, третье ядро – 17 %, четвертое ядро – 18 %. Таким образом, показатель $R_{\text{ЦП}} = 0.20$.

Сетевой канал используется при передаче идентификационных данных пользователей системы контроля и управления доступом между встроенными устройствами и центральным сервером доступа, между агентами рабочих станции и центральным сервером журналирования, между приложением для администрирования и центральным сервером доступа, а также между центральным сервером доступа и центральным сервером журналирования. В моменты пиковой нагрузки, количество пакетов, сигнализирующих о событиях, происходящих в системе, не превышала 2000 в секунду, при размере событий, не превышающем 1 Кб. Таким образом, показатель $R_{\text{СЕТЬ}} = 0.16$.

Размер исполняемого модуля со всеми необходимыми библиотеками, отвечающего за центральный сервер доступа и центральный сервер журналирования, составляет примерно 100 Мб. Таким образом, показатель использования жесткого диска $R_{\text{ЖД}} = 0.0002$.

В процессе выполнения процессов идентификации пользователей системы контроля и управления доступом, а также обнаружения нарушений политики безопасности организации, на центральном сервере доступа и журналирования использовалось не более 0.4 Гб оперативной памяти ($R_{\text{ОП}} = 0.1$).

Параметры встроенного устройства на основе микроконтроллера Arduino Yun, использованного при проведении экспериментов:

- центральное процессорное устройство: Atheros AR9331, ATmega32U4;
- максимальная пропускная способность сетевого канала: 100 Мб/с;
- общий объем жесткого диска: 512 Мб;
- общий объем оперативной памяти: 64 Мб;
- общий объем флеш-памяти: 16 Мб.

В процессе идентификации пользователей системы контроля и управления доступом, центральное процессорное устройство микроконтроллера было нагружено на 40 %. Таким образом, показатель $R_{\text{ЦП}} = 0.40$.

Размер исполняемого модуля со всеми необходимыми библиотеками, отвечающего за взаимодействие встроенного устройства с центральным сервером доступа, составляет примерно 20 Мб без учета виртуальной машины Java. Таким образом, показатель использования жесткого диска $R_{\text{ЖД}} = 0.039$.

В процессе выполнения процессов идентификации пользователей системы контроля и управления доступом на встроенном устройстве использовалось не более 24 Мб оперативной памяти ($R_{\text{ОП}} = 0.375$).

Размер исполняемого модуля со всеми необходимыми библиотеками, отвечающего за взаимодействие встроенного устройства с элементами программно-аппаратного окружения, составляет примерно 9 Мб. Таким образом, показатель использования флеш-памяти $R_{\text{ФП}} = 0.562$.

Полученные значения соответствующих показателей свидетельствуют о том, что $P_{\text{РЕС}}(r \leq R^{\text{ДОП}}) = 1$, а следовательно требование, объявленное во втором разделе, $P_{\text{РЕС}}(r \leq R^{\text{ДОП}}) \geq P_{\text{РЕС}}^{\text{ДОП}}$, где $P_{\text{РЕС}}^{\text{ДОП}} = 0.99$ выполняется. Это означает, что оценка ресурсопотребления соответствует предъявляемым требованиям.

4.2. Расчет экономических показателей

Расчет экономических показателей в данной выпускной квалификационной работе произведен в соответствии с рекомендациями методического пособия [44].

4.2.1. Определение себестоимости разработки прототипа

Перед расчетом полных затрат при разработке предлагаемого прототипа необходимо составить детализированный план работ, выполняемых на каждом этапе проектирования. При этом в основу детализированного плана работ положен календарный план выпускной квалификационной работы.

Отметим, что в соответствии с рекомендацией методического пособия, продолжительность выполняемых работ учитывалась по факту.

Результаты по каждому исполнителю могут быть сведены в едином представлении (таблица 12). Отметим, что продолжительность работ измерялась в человеко-днях (характеризует работу одного человека в течение одного рабочего дня вне зависимости от установленной продолжительности рабочего дня).

Ежемесячный оклад руководителя: 40 000 рублей (ставка старшего научного сотрудника в ФГБУН СПИИРАН), ежемесячный оклад студента – 20 000 рублей (половина ставки программиста в ФГБУН СПИИРАН).

Таблица 12 – Трудоемкость работ

№	Наименование работ	Трудоемкость, человеко-день	
		Руководитель	Студент
1	Разработка ТЗ на ВКР	2	2
2	Анализ требований ТЗ	1	1
3	Обзор и анализ существующих решений и отдельных компонентов	-	28
4	Формулирование основных требований к прототипу системы	2	8
5	Разработка методик оценки систем на основе встроенных устройств	2	10
6	Разработка программно-аппаратного прототипа системы	-	12
7	Проведение экспериментов и анализ полученных результатов	2	17
9	Оформление пояснительной записки и иллюстративного материала	-	15
Итого		9	93
Ставка, руб./день		1904.76	952.38

В каждом месяце 21 рабочий день. Таким образом, ежедневная ставка руководителя $С_Р$ и студента $С_С$ соответственно равны:

$$С_Р = \frac{40000 \text{ руб}}{21 \text{ день}} = 1904.76 \text{ руб./день} \quad (20)$$

$$С_С = \frac{20000 \text{ руб}}{21 \text{ день}} = 952.38 \text{ руб./день} \quad (21)$$

4.2.2. Расчет заработной платы

Формула расчета основной заработной платы $З_{осн.з/пл}$ исполнителей:

$$З_{осн.з/пл} = Т_р \cdot С_р + Т_с \cdot С_с \quad (22)$$

где $Т_р$, $Т_с$ – время, затраченное руководителем и студентом на проведение работ в рамках выпускной квалификационной работы; $С_р$, $С_с$ – ставка руководителя и студента.

$$З_{осн.з/пл} = 9 \cdot 1904.76 + 93 \cdot 952.38 = 105714.18 \text{ руб.}$$

Расходы на дополнительную заработную платы исполнителей

$$З_{доп.з/пл} = З_{осн.з/пл} \cdot \frac{Н_{доп}}{100} \quad (23)$$

где $Н_{доп}$ – норматив дополнительной заработной платы, при выполнении расчетов в выпускной квалификационной работе он принимается равным 14 %.

$$З_{доп.з/пл} = 105714.18 \cdot \frac{14}{100} = 14799.99 \text{ руб.}$$

Отчисления на страховые взносы на обязательно социальное, пенсионное и медицинское страхование с основной и дополнительной заработной платы исполнителей $З_{соц}$:

$$З_{соц} = (З_{осн.з./пл.} + З_{доп.з./пл.}) \cdot \frac{Н_{соц}}{100} \quad (24)$$

где $Н_{соц}$ – норматив отчислений на страховые взносы на обязательное социальное, пенсионное и медицинское страхование, при выполнении расчетов в выпускной квалификационной работе он принимается равным 30 %.

$$З_{соц} = (105714.18 + 14799.99) \cdot \frac{30}{100} = 36154.25 \text{ руб.}$$

4.2.3. Расчет затрат на материалы

Затраты на материалы $З_м$ определяются по следующей формуле:

$$З_м = \sum_{l=1}^{L} G_l Ц_l (1 + \frac{Н_{т.з.}}{100}) \quad (25)$$

где l – индекс вида сырья или материала, G_l – норма расхода i-ого материала на единицу продукции, $Ц_l$ – цена приобретения единицы l-ого материала, $Н_{т.з.}$ – норма транспортно-заготовительных расходов, при выполнении расчетов в выпускной квалификационной работе он принимается равным 10 %. Расчет затрат на материалы представлен в таблице 13.

Таблица 13 – Затраты на материалы

№	Материал	Тип (профиль, сорт, марка, размер)	Количество, ед.	Цена за единицу, руб.	Сумма на изделие, руб.
1	Бумага для офисной техники	SvetoCopy (A4, 80 г/кв.м, белизна CIE, 500 листов)	1	217	217
2	Картридж для принтера	Тонер-картридж HP 33A CF233A чер. для LJ Pro M106/M134	1	1250	1250
3	USB-флеш накопитель	Kingston Data-Traveler 100 G3 16GB USB 3.0	1	449	449
4	механический замок	TowerPro SG90	1	764	764
5	сканер бесконтактных карт технологии RFID	Grove 125KHz RFID Reader	1	1249	1249

№	Материал	Тип (профиль, сорт, марка, размер)	Количество, ед.	Цена за единицу, руб.	Сумма на изделие, руб.
6	инфракрасный датчик движения	PIR Motion Sensor HC-SR501	1	209	209
7	устройство вывода текстовой информации	DC 5V Character LCD 16x2	1	347	347
8	устройство вывода звуковых сигналов	DC 12mA 5V 12mm Piezo Alarm Buzzer	1	209	209
9	устройство вывода световых сигналов	RGB Light-emitting Diode	3	7	21
10	одноплатный компьютер	Arduino Yun	1	3608	3608
11	microSD накопитель	Kingston microSDHC Class 10, 512MB	1	139	139
12	набор соединительных проводов	Соединительные провода «папа-папа», AMP-W005, 65 шт.	1	290	290
13	макетная плата	Breadboard Half, 300x100	1	290	290
Сумма, руб.					9042
Транспортно-заготовительные расходы, руб.					904.20
Всего, руб.					9946.20

Таким образом, суммарные затраты на материалы с учетом транспортно-заготовительных расходов составляют 9946.20 руб. Необходимость в сырье, полуфабрикатах и специальном оборудовании отсутствует.

4.2.4. Затраты на содержание и эксплуатацию оборудования

Затраты на содержание и эксплуатацию оборудования определяются следующим образом:

$$З_{эо} = \sum_{i=1}^{m} C_l^{мч} t_i^{М} \quad (26)$$

где $З_{эо}$ – затраты на содержание и эксплуатацию оборудования, $C_l^{мч}$ – расчетная себестоимость одного машино-часа работы оборудования на i-ой технологической операции, $t_i^{М}$ – количество машино-часов, затрачиваемых на выполнение i-ой технологической операции.

В данной выпускной квалификационной работе будет производиться расчет стоимости потребляемой электроэнергии, поэтому в единицах измерения машино-час будет заменен на киловатт-час. Длительность выполнения выпускной квалификационной работы составляет 93 рабочих дня студента, а также 9 рабочих дней руководителя. При этом рабочий день студента длится 4 часа, а рабочий день руководителя – 8 часов. Таким образом, 372 часа работы студента и 72 часа работы руководителя соответственно.

Основными энергопотребителями при работе студента являются: рабочий компьютер – 360 Вт·ч, освещение в кабинете – 252 Вт·ч, а также аппаратный прототип системы – 3 Вт·ч. Основными энергопотребителями при работе руководителя являются: рабочий компьютер – 360 Вт·ч, а также освещение в кабинете – 252 Вт·ч. Установленный тариф составляет 4.12 руб./кВт·ч. Расчеты сведены в единую таблицу 14.

Таблица 14 – Стоимость электроэнергии

№	Потребитель	Тариф, руб./ кВт·ч	Потребление, кВт·ч	Длит. работы, час.	Суммарное потребление, кВт·ч	Затраты, руб.
1	Персональный компьютер студента	4.12	0.360	372	133.920	551.75
2	Персональный компьютер руководителя	4.12	0.360	72	25.920	106.79
4	Освещение в кабинете студента	4.12	0.252	372	93.744	386.23
5	Освещение в кабинете руководителя	4.12	0.252	72	18.000	74.16
6	Аппаратный прототип системы	4.12	0.003	372	1.116	4.60
Итого:						1123.53

4.2.5. Расходы на услуги сторонних организаций

К услугам сторонних организаций в ходе выполнения данной выпускной квалификационной работы, относится обеспечение доступа к сети Интернет. Стоимость данной услуги составляет 300 руб./мес.

Период выполнения выпускной квалификационной работы составляет 4 месяца, что означает итоговую стоимость пользования услугами доступа в Интернет в размере 1200 руб. Отметим, что из полученного результата необходимо исключить величину НДС, который при выполнении расчетов в выпускной квалификационной работе принимается равным 18 %. Рассмотрим расчетную формулу более подробно:

$$\text{С} = \frac{\text{С}_{\text{НДС}}}{1 + \text{НДС}} \tag{27}$$

$$\text{С} = \frac{1200}{1 + 0.18} = 1016.95 \text{ руб.}$$

4.2.6. Расчет амортизационных отчислений

В рамках работы над выпускной квалификационной работой используются следующие основные средства: рабочий компьютер студента и рабочий компьютер руководителя. Необходимо включить в затраты амортизационные отчисления по указанным основным средствам.

Амортизационные отчисления по i-ому основному средству за одни год определяются по следующей формуле:

$$\text{А}_i = \text{Ц}_{\text{п.н.}i} \cdot \frac{\text{Н}_{ai}}{100} \tag{28}$$

где $\text{Ц}_{\text{п.н.}i}$ – первоначальная стоимость i-ого основного средства, Н_{ai} – годовая норма амортизации i-ого основного средства.

Формула для вычисления годовой нормы амортизации имеет следующий вид:

$$\text{Н}_{ai} = \frac{\text{С}_{\text{обор.}i} - \text{С}_{\text{ликв.}i}}{\text{Т}_{\text{норм.}i} \cdot \text{С}_{\text{обор.}i}} \cdot 100 \tag{29}$$

где $\text{С}_{\text{обор.}i}$ – первоначальная стоимость -ого основного средства, $\text{С}_{\text{ликв.}i}$ – ликвидационная стоимость, составляющая 5 % от стоимости i-ого основного средства, $\text{Т}_{\text{норм.}i}$ – нормативный срок службы i-ого основного средства.

Нормативный срок службы рабочего компьютера студента, а также нормативный срок службы рабочего компьютера руководителя равны 5 лет.

Также необходимо определить время, в течение которого каждое основное средство использовалось для работы над выпускной квалификационной работой. Величина амортизационных отчислений по i-ому основному средству определяется по следующей формуле:

$$\text{А}_{i\text{ВКР}} = \text{А}_i \cdot \frac{\text{Т}_{i\text{ВКР}}}{12} \tag{30}$$

где $А_i$ – амортизационные отчисления за год по i-ому основному средству, $Т_{iВКР}$ – время, в течение которого i-ое средство использовалось для работы над выпускной квалификационной работы.

Результаты расчетов представлены в соответствующих таблицах (таблица 15 и таблица 16).

Таблица 15 – Годовая норма амортизации

№	Наименование	Тип (профиль, сорт, марка, размер)	$С_{обор.i}$	$С_{ликв.i}$	$С_{обор.i} - С_{ликв.i}$	$Т_{норм.i}$	$Н_{ai}$
1	рабочий компьютер студента	KEY GM Start G-320-8G1000	35490	1774.50	33715.50	5	19
2	рабочий компьютер руководителя	KEY GM Mid G-540-8G1000	43990	2199.50	41790.50	5	19

Таблица 16 – Расчет амортизационных отчислений

№	Наименование	Тип (профиль, сорт, марка, размер)	$Н_{ai}$	$А_i$	$Т_{iВКР}$	$А_{iВКР}$
1	рабочий компьютер студента	KEY GM Start G-320-8G1000	19	6743.10	4	2247.70
2	рабочий компьютер руководителя	KEY GM Mid G-540-8G1000	19	8358.10	4	2786.03
Итого:						5033.73

4.2.7. Накладные расходы

Накладные расходы на выполнение выпускной квалификационной работы могут быть рассчитаны по следующей формуле:

$$NR = (З_{\text{осн.з./пл.}} + З_{\text{доп.з./пл.}}) \cdot \frac{Н_{NR}}{100} \quad (31)$$

где $З_{\text{осн.з./пл.}}$ – расходы на основную заработную плату, $З_{\text{доп.з./пл.}}$ – расходы на дополнительную заработную плату, $Н_{NR}$ – норматив накладных расходов, при выполнении расчетов в выпускной квалификационной работе принимается равным 40 %

$$NR = (105714.18 + 14799.99) \cdot \frac{40}{100} = 48205{,}67 \text{ руб.}$$

4.2.8. Смета затрат

Итоговая величина затрат на разработку программно-аппаратного прототипа с указанием величины затрат по каждой из статей расходов сведена в едином представлении (таблица 17).

Таблица 17 – Смета затрат

№	Наименование статьи	Сумма, руб.
1	Расходы на оплату труда	120514.17
2	Отчисления на социальные нужды	36154.25
3	Материалы	9946.20
4	Расходы на содержание и эксплуатацию оборудования	1123.53
5	Затраты по работам, выполняемым сторонними организациями	1016.95
6	Амортизационные отчисления	5033.73
7	Накладные расходы	48205.67
Итого:		221994.50

Таким образом, итоговая величина затрат на разработку программно-аппаратного прототипа составляет 221994.50 рублей.

4.3. Выводы

Данный раздел посвящен технико-экономическому обоснованию разрабатываемого в рамках выпускной квалификационной работы программно-аппаратного прототипа защищенной системы контроля и управления доступом. Были описаны основные технические особенности разрабатываемой системы, относящиеся к функциональным возможностям и настройке системы контроля и управления доступом.

Основными конкурентными преимуществами разрабатываемого прототипа системы являются:

- защищенность системы от атак на нее за счет использования современных моделей и методик комбинирования средств защиты встроенных устройств непосредственно на этапе разработки;
- модульная архитектура системы, обеспечивающая масштабируемость и гибкость системы;
- объединение источников событий физического и кибернетического уровней для их последующей обработки с целью выявления событий безопасности, сценариев атак и аномальной активности.

Разрабатываемый прототип защищенной системы контроля и управления доступом может быть полезен для организаций, занимающихся разработкой и внедрением систем контроля и управления доступом. Кроме того, подход к разработке защищенных систем, на основе которого разрабатывается прототип защищенной системы контроля и управления доступом, а также объединение источников событий физического и кибернетического уровней в рамках системы контроля и управления доступом можно использовать в обучающих и исследовательских целях в области информационной безопасности, интернета вещей и встроенных устройств.

Себестоимость разработки составляет: 221994.50 рублей, экономическая целесообразность обусловлена техническим эффектом (функциональность прототипа расширена по сравнению со стандартными системами контроля и управления доступом), научным эффектом (для обеспечения защи-

щенности системы к атакам на нее применены на этапе разработки и проектирования системы современные модели и методики комбинирования средств защиты встроенных устройств), а также возможностью применения прототипа системы в производственной, учебной и научной сферах.

ЗАКЛЮЧЕНИЕ

В рамках выполнения выпускной квалификационной работы, все поставленные задачи были выполнены в объеме, соответствующем календарному плану и техническому заданию. При этом каждая из задач нашла отражение в соответствующем разделе пояснительной записки.

В разделе 1 были сформулированы основные функциональные и нефункциональные требования к встроенному устройству, которое легло в основу разработанной системы контроля и управления доступом, а также определена цель выпускной квалификационной работы и основные задачи, выполнение которых необходимо для ее достижения.

В разделе 2 были представлены методики оценки систем на основе встроенных устройств: методика оценки защищенности, методика оценки оперативности, методика оценки обоснованности и методика оценки ресурсопотребления. При этом методика оценки защищенности использует разработанную в рамках выпускной квалификационной работы адаптированную модель нарушителя для систем на основе встроенных устройств. Отметим, что за основу данной модели нарушителя брались уже существующие модели нарушителей, а именно модели нарушителей ФСТЭК и ФСБ России с последующим уточнением на основе особенностей предметной области.

В разделе 3 представлена архитектура разработанного прототипа защищенной системы контроля и управления доступом на основе встроенных устройств, состоящая из следующих основных элементов: (1) источников данных физического уровня, (2) источников данных кибернетического уровня, (3) модуля сбора данных, (4) модуля обработки событий, а также (5) модуля аналитической обработки и визуализации данных. Кроме того, в данном разделе для описания основных алгоритмов работы разработанного прототипа системы были теоретически изучены, а также построены следующие диаграммы прецедентов: диаграмма прецедентов для системы контроля и управления доступом, диаграмма прецедентов операций над встроенными

устройствами, диаграмма прецедентов операций над гостями, диаграмма прецедентов операций над работниками, диаграмма прецедентов операций над картами, диаграмма прецедентов операций над ролями, диаграмма прецедентов операций над аккаунтами, диаграмма прецедентов операций над политиками. Также на основе современных моделей и методик комбинирования средств защиты встроенных устройств в данном разделе был выбран следующий компонентный состав встроенного устройства для построения системы: Arduino Yun, microSD 512 MB, TowerPro SG90, Grove 125KHz RFID Reader, PIR Motion Sensor HC-SR501, DC 5V Character LCD 16x2, DC 12mA 5V 12mm Piezo Alarm Buzzer, RGB Light-emitting Diode, power bank 15000 мА·ч; стоимостью 7573 рубля и средним энергопотреблением 550 мА·ч. В заключение данного раздел был представлен разработанный программно-аппаратный прототип защищенной системы контроля и управления доступом, состоящий из следующих элементов: микроконтроллер Arduino Yun, сервер приложений центрального сервера доступа, база данных центрального сервера доступа, приложение администратора (для управления настройками системы), панель управления (для локальной настройки встроенных устройств), сервер приложений центрального сервера журналирования, база данных центрального сервера журналирования, агенты рабочих станций для мониторинга состояния сеанса пользователей с операционной системой. При этом было описано взаимодействие элементов прототипа системы контроля и управления доступом, а также основные используемые технологии.

В разделе 4 приведено технико-экономическое обоснование разработанного в рамках выпускной квалификационной работы программно-аппаратного прототипа защищенной системы контроля и управления доступом. С точки зрения технических показателей, в данном разделе представлены результаты оценки защищенности, оперативности, обоснованности, а также ресурсопотребления разработанного прототипа системы. Кроме того, сформированы выводы о соответствии данных, полученных эксперименталь-

ным путем, теоретическим ограничениям, введенным в разделе 2. Так, например, вероятность выполнения процесса идентификации пользователей системы за заданное время составляет $P_{\text{ОП}}(TIME_N \leq TIME^{\text{ДОП}}) = 0.9999$, а вероятность выполнения процесса обнаружения нарушений политики безопасности организации за заданное время составляет $P_{\text{ОП}}(TIME_N \leq TIME^{\text{ДОП}}) = 0.9999$, что соответствует предъявляемым требованиям ($P_{\text{ОП}}^{\text{ДОП}} = 0.99$) к оперативности. Также полученные значения соответствующих показателей свидетельствуют о том, что $P_{\text{РЕС}}(r \leq R^{\text{ДОП}}) = 1$, а следовательно требование $P_{\text{РЕС}}(r \leq R^{\text{ДОП}}) \geq P_{\text{РЕС}}^{\text{ДОП}}$, где $P_{\text{РЕС}}^{\text{ДОП}} = 0.99$ выполняется. Это означает, что оценка ресурсопотребления соответствует предъявляемым требованиям. Важно отметить, что по результатам оценки защищенности, разработанный прототип системы контроля и управления доступом, является защищенным относительно нарушителей уровня 1, типа 0,1 (адаптированная модель нарушителя, раздел 2.1.2). Кроме того, результаты экспериментов показали, что в течение рабочего дня, модуль обработки событий центрального сервера системы контроля и управления доступом с помощью методов на основе правил и машины конечных состояний выявлял все переходы между состояниями, нарушающие политику безопасности организации в рамках заложенного конечного автомата. Таким образом, можно сделать вывод о том, что значения обоснованности также удовлетворяет представленным требованиям. С точки зрения экономических показателей отметим, что разработанный прототип может быть полезен для организаций, занимающихся разработкой и внедрением систем контроля и управления доступом. Кроме того, подход к разработке защищенных систем, на основе которого разрабатывается прототип защищенной системы контроля и управления доступом, а также объединение источников событий физического и кибернетического уровней в рамках системы контроля и управления доступом можно использовать в обучающих и исследовательских целях в области информационной безопасности, интернета вещей и встроенных устройств.

Частично, результаты ВКР были представлены в рамках IX Санкт-Петербургской межрегиональной конференции «Информационная Безопасность Регионов России – 2015» (ИББР-2015) [45], Юбилейной XV Санкт-Петербургской Международной Конференции «Региональная информатика-2016» («РИ-2016») [46], 25-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации» [47], 9-й конференции «Информационные технологии в управлении» (ИТУ-2016) [48-49], а также в рамках международной научной школы «Управление инцидентами и противодействие целевым кибер-физическим атакам в распределенных крупномасштабных критически важных системах (IM&CTCPA 2015)» [50], организованной лабораторией проблем компьютерной безопасности ФГБУН СПИИРАН.

Кроме того, по результатам работы над выпускной квалификационной работой, был опубликован ряд работ, в том числе в изданиях, входящих в перечень ВАК и индексы РИНЦ, Web of Science и Scopus [51-55].

Также для защиты интеллектуально собственности, в Реестре программ для ЭМВ и баз данных ФГБУН ФИПС были зарегистрированы программы (приложение И, приложение К, приложение М) и база данных (приложение Л).

Коммерческие перспективы результатов выпускной квалификационной работы были апробированы в рамках конкурса «УМНИК-1С». Заявка прошла в финал конкурса, получила высокие оценки со стороны представителей жюри, относящихся к бизнесу, но не вошла в число победителей, получивших грант.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. "Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных", Федеральная служба по техническому и экспортному контролю (ФСТЭК России), 15 февраля 2008 года.

2. "Методика определения угроз безопасности информации в информационных системах", Федеральная служба по техническому и экспортному контролю (ФСТЭК России), проект, 2015 года.

3. "Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности", Федеральная служба безопасности (ФСБ России), 31 марта 2015 года, № 149/7/2/6-432.

4. Howard M. Secure systems begin with knowing your threats // 2004 - [Электронный ресурс] - Режим доступа. - URL: http://archive.devx.com/upload/free/Features/zones/security/articles/2000/10oct00/mh1000[1]-1.asp. - 2000 (дата обращения 30.05.2016).

5. Kocher P., Lee R., Mcgraw G., Ravi S. Security as a new dimension in embedded system design // Proceedings of the 41st Design Automation Conference (DAC ’04). - P. 753-760. - 2004.

6. Kommerling O., Kuhn M.G. Design principles for tamper-resistant smartcard processors // Proceedings of the USENIX Workshop on Smartcard Technology. - P. 9-20. - 1999.

7. Abraham D.G., Dolan G.M., Double G.P., Stevens J.V. Transaction security system // IBM Systems Journal. - № 30(2). - P. 206-228. - 1991.

8. Rae A.J., Wildman L.P. A Taxonomy of Attacks on Secure Devices // Department of Information Technology and Electrical Engineering, University of Queensland. Australia. - P. 251-264. - 2003.

9. Eby M., Werner J., Karsai G., Ledeczi A. Integrating Security Modeling into Embedded System Design // Proceedings of 14th Annual IEEE International Conference and Workshops on the Engineering of Computer-Based Systems (ECBS '07) . - P. 221-228. - 2007.

10. Pauli J., Xu D. Threat-Driven Architectural Design of Secure Information Systems // Proceedings of the International Conference on Enterprise Information Systems (ICEIS'05). 2005.

11. Myagmar S., Lee A.J., Yurcik W. Threat Modeling as a Basis for Security Requirements // Symposium on Requirements Engineering for Information Security (SREIS'05). 2005.

12. Serpanos D.N., Papalambrou A. Security and Privacy in Distributed Smart Cameras // Proceedings of the IEEE. - vol. 96. - № 10. - P. 1678-1687. - 2008.

13. Sastry J.K.R., Bhanu J.S., SubbaRao K. Attacking embedded systems through fault injection // 2nd National Conference on Emerging Trends and Applications in Computer Science (NCETACS). - P. 1-5. - 2011.

14. Ruiz J.F., Desnitsky V., Harjani R., Manna A., Kotenko I., Chechulin A. A Methodology for the Analysis and Modeling of Security Threats and Attacks for Systems of Embedded Components // Proceeding of the 20th International Euromicro Conference on Parallel, Distributed and Network-based Processing (PDP 2012). Garching/Munich, February, 2012. P.261-268.

15. Котенко И.В., Десницкий В.А., Чечулин А.А. Исследование технологии проектирования безопасных встроенных систем в проекте Европейского сообщества SecFutur // Защита информации. Инсайд, 2011, № 3, С.68-75.

16. Десницкий В.А., Котенко И.В., Чечулин А.А. Конфигурирование защищенных систем со встроенными и мобильными устройствами // Вопросы защиты информации, № 2, 2012. С.20-28.

17. Kruegel C, Valeur F., Vigna G. Intrusion Detection and Correlation: Challenges and Solutions. University of California, Santa Barbara, USA: Springer, 2005. P.29-33.

18. Sadoddin R., Ghorbani A. Alert Correlation Survey: Framework and Techniques // Proceedings of the 4th Annual Conference on Privacy, Security and Trust (PST), 2006, P.6-15.

19. Muller A. Event Correlation Engine. Master's Thesis, Swiss Federal Institute of technology, Zurich, 2009, P. 165. – URL: https://www.open.ch/_pdf/internships/EventCorrelationEngine_AndreasMueller.pdf (дата обращения: 29.11.2016).

20. Tagelsir H., Izzeldin E., Osman M. An improved framework for intrusion alert correlation // Proceedings of the World Congress on Engineering 2012 Volume I, 2012. 5 p.

21. Tiffany M. A survey of event correlation techniques and related topics. 2002. – URL: http://www.tiffman.com/netman/netman.html (дата обращения: 29.11.2016).

22. Denise W. Guerer, Khan I., Ogler R., Keffer R. An artificial intelligence approach to network fault management. SRI International, 1996, 10 p. – URL: http://www.academia.edu/8460871/An_Artificial_Intelligence_Approach_to_Network_Fault_Management (дата обращения: 29.11.2016).

23. Интернет-сервис Amazon. – URL: http://www.amazon.com (дата обращения: 29.11.2016).

24. Магазин электроники. – URL: http://seeedstudio.com/ (дата обращения: 29.11.2016).

25. Энергоэффективность DC 5V Character LCD 16x2. – URL: http://melt.com/ (дата обращения: 29.11.2016).

26. Магазин электроники. – URL: http://nettigo.pl/ (дата обращения: 29.11.2016).

27. Официальный форум для разработчиков платформы Arduino. – URL: http://forum.arduino.cc/ (дата обращения: 29.11.2016).

28. Официальный форум для разработчиков платформы Raspberry Pi: – URL: https://www.raspberrypi.org/forums/ (дата обращения: 29.11.2016).

29. Официальный форум для разработчиков платформы Beaglebone. – URL: https://beagleboard.org/discuss (дата обращения: 29.11.2016)

30. Официальное сообщество для разработчиков платформы Intel Galileo. – URL: https://communities.intel.com/community/tech/galileo/ (дата обращения: 29.11.2016).

31. Официальный продавец микроконтроллеров платформы Arduino. – URL: http://store.arduino.cc/ (дата обращения: 29.11.2016).

32. Официальный продавец одноплатных компьютеров платформы Raspberry Pi. – URL: http://alliedelec.com/ (дата обращения: 29.11.2016).

33. Официальный продавец одноплатных компьютеров платформы Beaglebone. – URL: https://adafruit.com/ (дата обращения: 29.11.2016).

34. Официальный продавец одноплатных компьютеров платформы Intel Galileo. – URL: http://mouser.com/ (дата обращения: 29.11.2016).

35. Официальная справка для разработчиков платформы Arduino. – URL: http://arduino.cc/en/Reference/ (дата обращения: 29.11.2016).

36. Архив с приложением на языке Java. – URL: http://docs.oracle.com/javase/7/docs/technotes/tools/windows/jar.html (дата обращения: 29.11.2016).

37. Веб-сервер Apache Tomcat. – URL: http://tomcat.apache.org/ (дата обращения: 29.11.2016).

38. Фреймворк с открытым исходных кодом Spring Framework. – URL: http://projects.spring.io/spring-framework/ (дата обращения: 29.11.2016).

39. Пулл соединений C3p0 pooling. – URL: http://mchange.com/projects/c3p0/ (дата обращения: 29.11.2016).

40. Взаимодействие Java-приложений с базой данных (JDBC). – URL: http://www.oracle.com/technetwork/java/javase/jdbc/index.html (дата обращения: 29.11.2016).

41. Свободно распространяемая объектно-реляционная система управления базами данных PostgreSQL. – URL: https://www.postgresql.org/ (дата обращения: 29.11.2016).

42. Balzarotti D., Monga M., Sicari S. Assessing the risk of using vulnerable components // Quality of protection: security measurments and metrics, Advances in Information Security 23. Springer, New York, 2006. P.65-77.

43. Основы теории управления в системах военного назначения. Часть 2. // Под ред. А.Ю. Рунеева и И.В. Котенко. – СПб.: ВУС, 2000. – 158 стр.

44. Алексеева О.Г. Методические указания по экономическому обоснованию выпускных квалификационных работ бакалавров: Метод. указа-ния, СПб.: Изд-во СПбГЭТУ “ЛЭТИ”, 2013.

45. Левшун Д.С., Чечулин А.А., Коломеец М.В., Котенко И.В. Архитектура системы контроля и управления доступом в помещения на основе бесконтактных смарт-карт // IX Санкт-Петербургская межрегиональная конференция "Информационная безопасность регионов России" (ИБРР-2015). 28-30 октября 2015 г. Материалы конференции. СПб.: СПОИСУ, 2015. С. 76.

46. Левшун Д.С., Чечулин А.А., Котенко И.В. Защищенное межконтроллерное взаимодействие на базе протокола I2C // Юбилейная XV Санкт-Петербургская Международная Конференция “Региональная информатика-2016” (“РИ-2016”). 26-28 октября 2016 г. Материалы конференции. СПб., 2016. С. 169-170.

47. Левшун Д.С., Чечулин А.А., Котенко И.В. Архитектура комплексной системы безопасности // Методы и технические средства обеспечения безопасности информации. Материалы 25-й научно-технической конференции. 4-7 июля 2016 года. Санкт-Петербург. Издательство Политехнического университета. 2016. С.53-54.

48. Булгаков М.В., Левшун Д.С. Основные проблемы обеспечения защиты линий связи систем физической безопасности // Материалы 9-й конференции "Информационные технологии в управлении" (ИТУ-2016). 4-6 октября 2016 г. СПб.: ОАО "Концерн "ЦНИИ "Электроприбор", 2016. С.665-669.

49. Левшун Д.С. Методика интеграции системы контроля и управления доступом в комплексную систему безопасности // Материалы 9-й конференции "Информационные технологии в управлении" (ИТУ-2016). 4-6 октября 2016 г. СПб.: ОАО "Концерн "ЦНИИ "Электроприбор", 2016. С.735-739.

50. Левшун Д.С., Коломеец М.В., Опыт разработки распределенной системы охраны периметра на основе элементов сети Интернета вещей // Международная научная школа "Управление инцидентами и противодействие целевым

кибер-физическим атакам в распределенных крупномасштабных критически важных системах (IM&CTCPA 2015)", СПИИРАН, Санкт-Петербург, 26-28 ноября 2015, http://www.comsec.spb.ru/imctcpa15/.

51. Котенко И.В., Левшун Д.С., Чечулин А.А., Бушуев С.Н. Корреляция событий в комплексной системе киберфизической безопасности // Сборник докладов XIX Международной конференции по мягким вычислениям и измерениям (SCM'2016). Том 2. СПб.: Издательство СПбГЭТУ «ЛЭТИ». – 2016. – С.327-331.

52. Десницкий В.А., Чечулин А.А., Котенко И.В., Левшун Д.С., Коломеец М.В. Комбинированная методика проектирования защищенных встроенных устройств на примере системы охраны периметра // Труды СПИИРАН. 2016. Вып. 5(48). С. 5-31.

53. Vasily Desnitsky, Andrey Chechulin, Igor Kotenko, Dmitry Levshun, Maxim Kolomeec. Application of a Technique for Secure Embedded Device Design Based on Combining Security Components for Creation of a Perimeter Protection System. 24th Euromicro International Conference on Parallel, Distributed, and Network-Based Processing (PDP 2016). Heraklion, Crete, Greece, February, 2016. IEEE Computer Society. 2016. P. 609-616.

54. Vasily Desnitsky, Dmitry Levshun, Andrey Chechulin and Igor Kotenko. Design Technique for Secure Embedded Devices: Application for Creation of Integrated Cyber-Physical Security System. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), Vol.7, No.2, June, 2016. P.60-80. http://jowua.yolasite.com/vol7no2.php.

55. Igor Kotenko, Dmitry Levshun, Andrey Chechulin. Event correlation in the integrated cyber-physical security system. Proceedings of the 2016 XIX IEEE International Conference on Soft Computing and Measurements (SCM-2016), IEEE, St. Petersburg, Russia, May 2016. P.484-486.

Приложение А. Диаграмма прецедентов операций над встроенными устройствами

Рассмотрим экземпляры (создать встроенное устройство, удалить встроенное устройство, посмотреть встроенное устройство, получить список состояния встроенных устройств, обновить встроенное устройство) прецедента операции над встроенными устройствами более подробно (рисунок 10).

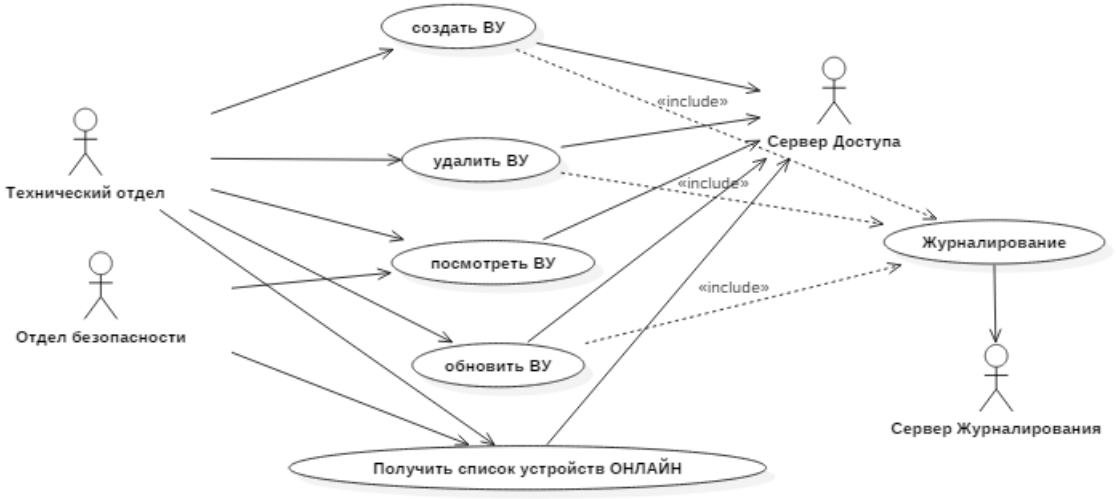

Рисунок 10 – Диаграмма прецедентов операций над ВУ

Прецедент: создать встроенное устройство.

Краткое описание: данный прецедент описывает процесс создания (ввода в эксплуатацию) встроенного устройства в системе контроля и управления доступом.

Актор: технический отдел.

Зависимость: является экземпляром прецедента операции над встроенными устройствами.

Предусловие: пользователь (сотрудник или администратор) вошел в систему с правами технического отдела.

Основной поток событий: данный прецедент начинает выполняться, когда сотрудник технического отдела хочет создать (ввести в эксплуатацию) встроенное устройство. Рассмотрим последовательность событий более подробно:

1. задается IP-адрес устройства и его спецификация;

2. формируется журнальная запись о произошедшем событии.

Альтернативные потоки событий: при совпадении задаваемого IP-адреса встроенного устройства с IP-адресом уже существующего встроенного устройства, выводится уведомление о соответствующей ошибке.

Постусловие: если прецедент выполнен успешно, то создается (вводится в эксплуатацию) встроенное устройство, а также отображается уникальный идентификатор, присвоенный встроенному устройству. В противном случае, новое устройство не создается (не вводится в эксплуатацию).

Прецедент: удалить встроенное устройство.

Краткое описание: данный прецедент описывает процесс удаления (вывода из эксплуатации) встроенного устройства из системы.

Актор: технический отдел.

Зависимость: является экземпляром прецедента операции над встроенными устройствами.

Предусловие: пользователь (сотрудник или администратор) вошел в систему с правами технического отдела.

Основной поток событий: данный прецедент начинает выполняться, когда сотрудник технического отдела хочет удалить (вывести из эксплуатации) встроенное устройство. Рассмотрим последовательность событий более подробно:

1. вводится уникальный идентификатор удаляемого (выводимого из эксплуатации) встроенного устройства;
2. формируется журнальная запись о произошедшем событии.

Альтернативные потоки событий: при отсутствии в системе встроенного устройства с запрашиваемым уникальным идентификатором, выводится уведомление о соответствующей ошибке.

Постусловие: если прецедент выполнен успешно, то выводится уникальный идентификатор удаленного (выведенного из эксплуатации) встроенного устройства, в то время как встроенное устройство удаляется из системы кон-

троля и управления доступом. В противном случае, устройство не удаляется (не выводится из эксплуатации).

Прецедент: посмотреть встроенные устройства.

Краткое описание: данный прецедент описывает процесс просмотра встроенных устройств, введенных в эксплуатацию в системе контроля и управления доступом.

Актор: технический отдел, отдел безопасности.

Зависимость: является экземпляром прецедента операции над встроенными устройствами.

Предусловие: пользователь (сотрудник или администратор) вошел в систему с правами технического отдела и/или отдела безопасности.

Основной поток событий: данный прецедент начинает выполняться, когда сотрудник технического отдела или отдела безопасности хочет просмотреть введенные в эксплуатацию встроенные устройства. Рассмотрим последовательность событий более подробно:

1. поиск встроенных устройств по IP-адресу;
2. поиск встроенных устройств по уникальному идентификатору;
3. поиск встроенных устройств по спецификации;
4. комбинированный поиск встроенных устройств.

Альтернативные потоки событий: если в результате поиска введенных в эксплуатацию встроенных устройств с заданными при поиске параметрами не обнаружено ни одного встроенного устройства, то выводится уведомление о соответствующей ошибке.

Постусловие: если прецедент выполнен успешно, то выводится полная информация о введенных в эксплуатацию встроенных устройствах, соответствующих заданным параметрам, а именно: уникальный идентификатор, спецификация и IP-адрес встроенного устройства. В противном случае, выводится уведомление о соответствующей ошибке.

Прецедент: получить список состояния встроенных устройств.

Краткое описание: данный прецедент описывает процесс просмотра всех встроенных устройств.

Актор: технический отдел, отдел безопасности.

Зависимость: является экземпляром прецедента операции над встроенными устройствами.

Предусловие: пользователь (сотрудник или администратор) вошел в систему с правами технического отдела и/или отдела безопасности.

Основной поток событий: данный прецедент начинает выполняться, когда сотрудник технического отдела или отдела безопасности хочет просмотреть информацию обо всех встроенных устройствах. Рассмотрим последовательность событий более подробно:

1. поиск встроенных устройств по IP-адресу;
2. поиск встроенных устройств по уникальному идентификатору;
3. поиск встроенных устройств по спецификации;
4. комбинированный поиск встроенных устройств.

Альтернативные потоки событий: если в результате поиска встроенных устройств не обнаружено ни одного встроенного устройства, то выводится уведомление о соответствующей ошибке.

Постусловие: если прецедент выполнен успешно, то выводится полная информация о встроенных устройствах, соответствующих заданным параметрам, а именно: уникальный идентификатор, спецификация и IP-адрес встроенного устройства. В противном случае, выводится уведомление о соответствующей ошибке.

Прецедент: обновить встроенное устройство.

Краткое описание: данный прецедент описывает процесс изменения информации о встроенном устройстве.

Актор: технический отдел.

Зависимость: является экземпляром прецедента операции над встроенными устройствами.

Предусловие: пользователь (сотрудник или администратор) вошел в систему с правами технического отдела.

Основной поток событий: данный прецедент начинает выполняться, когда пользователь хочет изменить информацию о встроенном устройстве. Рассмотрим последовательность событий более подробно:

1. изменение IP-адреса встроенного устройства;
2. изменение спецификации встроенного устройства;
3. формируется журнальная запись о произошедшем событии.

Альтернативные потоки событий: если при изменении встроенного устройства осуществляется попытка изменения IP-адреса встроенного устройства на IP-адрес другого встроенного устройства, то выдается уведомлении о соответствующей ошибке.

Постусловие: если прецедент выполнен успешно, то информация о встроенном устройстве изменяется. В противном случае, выдается уведомление о соответствующей ошибке.

Приложение Б. Диаграмма прецедентов операций над гостями

Рассмотрим экземпляры (создать гостя, освободить карту гостя, обновить гостя, посмотреть актуальных гостей, посмотреть историю посещений) прецедента операции над гостями более подробно (рисунок 11).

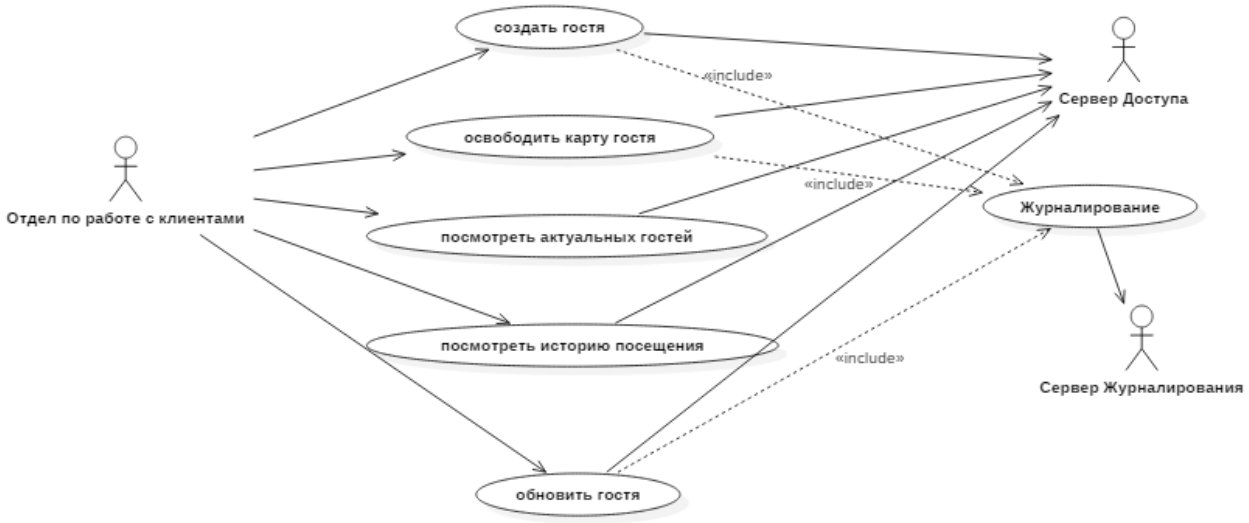

Рисунок 11 – Диаграмма прецедентов операций над гостями

Прецедент: создать гостя.

Краткое описание: данный прецедент описывает процесс создания (регистрации) пользователя с правами гостя в системе контроля и управления доступом.

Актор: отдел по работе с клиентами.

Зависимость: является экземпляром прецедента операции над гостями.

Предусловие: пользователь (сотрудник или администратор) вошел в систему с правами отдела по работе с клиентами.

Основной поток событий: данный прецедент начинает выполняться, когда пользователь (сотрудник или администратор) с правами отдела по работе с клиентами пытается создать (зарегистрировать) пользователя с правами гостя. Рассмотрим последовательность событий более подробно:

1. задается имя пользователя с правами гостя;

2. задается уникальный идентификатор смарт-карты, которая будет выдана пользователю с правами гостя;
3. фиксируется время окончания доступа по выданной смарт-карте;
4. формируется журнальная запись о произошедшем событии.

Альтернативные потоки событий: если карта, задаваемая при создании (регистрации) пользователя с правами гостя занята или не существует, то выдается уведомление о соответствующей ошибке. Новый пользователь с правами гостя не создается (регистрируется).

Постусловие: если прецедент выполнен успешно, то в системе создается (регистрируется) пользователь с правами гостя. При этом выводится уникальный идентификатор созданного (зарегистрированного) пользователя с правами гостя. В противном случае, выдается уведомление о соответствующей ошибке.

Прецедент: освободить карту гостя.

Краткое описание: данный вариант использования описывает освобождение карты пользователя с правами гостя в системе контроля и управления доступом.

Актор: отдел по работе с клиентами.

Зависимость: является экземпляром прецедента операции над гостями.

Предусловие: пользователь (сотрудник или администратор) вошел в систему с правами отдела по работе с клиентами.

Основной поток событий: данный прецедент начинает выполняться, когда пользователь (сотрудник или администратор) с правами отдела по работе с клиентами пытается освободить (отвязать от пользователя с правами гостя) смарт-карту в системе. Рассмотрим последовательность событий более подробно:

1. задается уникальный идентификатор смарт-карты, которая будет освобождена (отвязана от пользователя с правами гостя);
2. формируется журнальная запись о произошедшем событии.

Альтернативные потоки событий: если карта, выбранная для освобождения (отвязки от пользователя с правами гостя) не существует, то выдается уведомление о соответствующей ошибке.

Постусловие: если прецедент выполнен успешно, то карта отвязывается от гостя и отмечается в системе как свободная. В противном случае, выдается уведомление о соответствующей ошибке.

Прецедент: обновить гостя.

Краткое описание: данный прецедент описывает процесс изменения данных о пользователе с правами гостя в системе контроля и управления доступом.

Актор: отдел по работе с клиентами.

Зависимость: является экземпляром прецедента операции над гостями.

Предусловие: пользователь (сотрудник или администратор) вошел в систему с правами отдела по работе с клиентами.

Основной поток событий: данный прецедент начинает выполняться, когда пользователь (сотрудник или администратор) с правами отдела по работе с клиентами пытается изменить данные о пользователе с правами гостя в системе. Рассмотрим последовательность событий более подробно:

1. задается уникальный идентификатор пользователя с правами гостя, данные о котором необходимо изменить;
2. задается новое имя пользователя с правами гостя;
3. задается новый уникальный идентификатор смарт-карты для пользователя с правами гостя;
4. задается новое время окончания доступа по смарт-карте, выданной пользователю с правами гостя;
5. формируется журнальная запись о произошедшем событии.

Альтернативные потоки событий: если не существует пользователя с правами гостя, уникальный идентификатор которого был бы равен заданному, то выдается уведомление о соответствующей ошибке.

Постусловие: если прецедент выполнен успешно, то данные о пользователе с правами гостя изменяются. В противном случае, выдается уведомление о соответствующей ошибке.

Прецедент: посмотреть актуальных гостей.

Краткое описание: данный прецедент описывает процесс просмотра пользователем (сотрудником или администратором) с правами отдела по работе с клиентами актуальных пользователей с правами гостя в системе.

Актор: отдел по работе с клиентами.

Зависимость: является экземпляром прецедента операции над гостями.

Предусловие: пользователь (сотрудник или администратор) вошел в систему с правами отдела по работе с клиентами.

Основной поток событий: данный прецедент начинает выполняться, когда пользователь (сотрудник или администратор) с правами отдела по работе с клиентами хочет посмотреть актуальных пользователей с правами гостя в системе. Рассмотрим последовательность событий более подробно:

1. поиск по уникальному идентификатору карты;
2. поиск по уникальному идентификатору пользователя с правами гостя;
3. поиск по имени пользователя с правами гостя;
4. комбинированный поиск.

Альтернативные потоки событий: если в процессе поиска пользователей с правами гостя при заданных параметрах в результате поиска ничего не было обнаружено, то выдается уведомление о соответствующей ошибке.

Постусловие: если прецедент выполнен успешно, то выводится информация о пользователях с правами гостя, удовлетворяющих заданным параметрам. В частности, отображается уникальный идентификатор пользователя с правами гостя, имя пользователя с правами гостя, время начала и окончания предоставления доступа пользователю с правами гостя, а также уникальный идентификатор смарт-карты, выданной пользователю с правами гостя. В противном случае, выдается уведомление о соответствующей ошибке.

Прецедент: посмотреть историю посещений.

Краткое описание: данный прецедент описывает процесс просмотра пользователем (сотрудником или администратором) с правами отдела по работе с клиентами истории посещений пользователей с правами гостя в системе.

Актор: отдел по работе с клиентами.

Зависимость: является экземпляром прецедента операции над гостями.

Предусловие: пользователь (сотрудник или администратор) вошел в систему с правами отдела по работе с клиентами.

Основной поток событий: данный прецедент начинает выполняться, когда пользователь (сотрудник или администратор) с правами отдела по работе с клиентами хочет посмотреть историю посещений пользователей с правами гостя в системе. Рассмотрим последовательность событий более подробно:

1. поиск по уникальному идентификатору карты;
2. поиск по уникальному идентификатору пользователя с правами гостя;
3. поиск по имени пользователя с правами гостя;
4. комбинированный поиск.

Альтернативные потоки событий: если в процессе поиска посещений пользователей с правами гостя при заданных параметрах в результате поиска не было обнаружено ни одного посещения пользователя с правами гостя, то выдается уведомление о соответствующей ошибке.

Постусловие: если прецедент выполнен успешно, то выводится информация о пользователях с правами гостя, удовлетворяющих заданным параметрам. В частности, отображается уникальный идентификатор пользователя с правами гостя, имя пользователя с правами гостя, время начала и окончания предоставления доступа пользователю с правами гостя, а также уникальный идентификатор смарт-карты, выданной пользователю с правами гостя. В противном случае, выдается уведомление о соответствующей ошибке.

Приложение В. Диаграмма прецедентов операций над работниками

Рассмотрим экземпляры (создать работника, удалить работника, посмотреть работника, обновить работника) прецедента операции над работниками более подробно (рисунок 12).

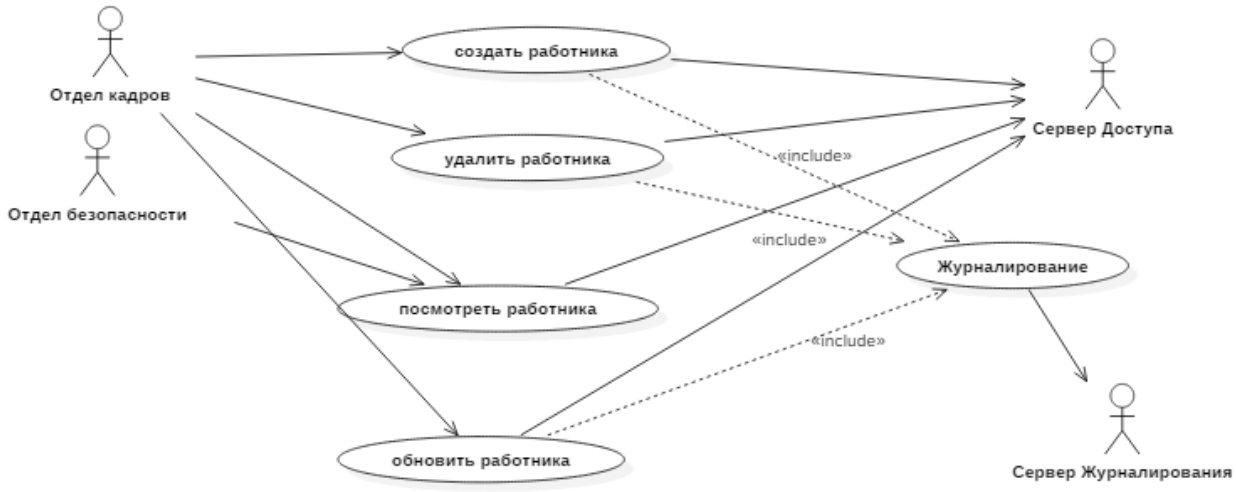

Рисунок 12 – Диаграмма прецедентов операций над работниками

Прецедент: создать работника.

Краткое описание: данный прецедент описывает процесс создания пользователя с правами сотрудника или администратора в системе контроля и управления доступом.

Актор: отдел кадров.

Зависимость: является экземпляром прецедента операции над работниками.

Предусловие: пользователь (сотрудник или администратор) вошел в систему с правами отдела кадров.

Основной поток событий: данный прецедент начинает выполняться, когда пользователь (сотрудник или администратор) с правами отдела кадров пытается создать (зарегистрировать) пользователя с правами сотрудника или администратора в системе. Рассмотрим последовательность событий более подробно:

1. задается имя пользователя с правами сотрудника или администратора;

2. задается уникальный идентификатор смарт-карты, выдаваемой пользователю с правами сотрудника или администратора;
3. формируется журнальная запись о произошедшем событии.

Альтернативные потоки событий: если в процессе создания пользователя с правами сотрудника или администратора, осуществляется попытка выдать новому пользователю смарт-карту, уникальный идентификатор которой занят или не существует, то выдается уведомление о соответствующей ошибке.

Постусловие: если прецедент выполнен успешно, то создается (регистрируется) пользователь с правами сотрудника или администратора. При этом выводится уникальный идентификатор, присвоенный новому пользователю. В противном случае, выдается уведомление о соответствующей ошибке.

Прецедент: удалить работника.

Краткое описание: данный прецедент описывает процесс удаления пользователя с правами сотрудника или администратора в системе контроля и управления доступом.

Актор: отдел кадров.

Зависимость: является экземпляром прецедента операции над работниками.

Предусловие: пользователь (сотрудник или администратор) вошел в систему с правами отдела кадров.

Основной поток событий: данный прецедент начинает выполняться, когда пользователь (сотрудник или администратор) с правами отдела кадров пытается создать (зарегистрировать) пользователя с правами сотрудника или администратора в системе. Рассмотрим последовательность событий более подробно:

1. задается уникальный идентификатор пользователя (сотрудника или администратора), которого необходимо удалить из системы;
2. формируется журнальная запись о произошедшем событии.

Альтернативные потоки событий: если в процессе удаления пользователя с правами сотрудника или администратора, осуществляется попытка удалить

пользователя, уникальный идентификатор которого не существует, то выдается уведомление о соответствующей ошибке.

Постусловие: если прецедент выполнен успешно, то из системы удаляется пользователь с правами сотрудника или администратора. При этом выводится уникальный идентификатор, принадлежавший данному пользователю. В противном случае, выдается уведомление о соответствующей ошибке.

Прецедент: посмотреть работника.

Краткое описание: данный прецедент описывает процесс просмотра информации о пользователях с правами сотрудника или администратора в системе контроля и управления доступом.

Актор: отдел кадров или отдел безопасности.

Зависимость: является экземпляром прецедента операции над работниками.

Предусловие: пользователь (сотрудник или администратор) вошел в систему с правами отдела кадров или отдела безопасности.

Основной поток событий: данный прецедент начинает выполняться, когда пользователь (сотрудник или администратор) с правами отдела кадров или отдела безопасности осуществляет поиск информации о пользователях с правами сотрудника или администратора в системе. Рассмотрим последовательность событий более подробно:

1. поиск по уникальному идентификатору пользователя (сотрудника или администратора;
2. поиск по имени пользователя (сотрудника или администратора);
3. поиск по уникальному идентификатору смарт-карты, выданной пользователю (сотруднику или администратору;
4. поиск по роли пользователя (сотрудника или администратора);
5. комбинированный поиск.

Альтернативные потоки событий: если в процессе поиска информации о пользователях с правами сотрудника или администратора, в результате поис-

ка не обнаружено пользователей, удовлетворяющих заданным параметрам, то выдается уведомление о соответствующей ошибке.

Постусловие: если прецедент выполнен успешно, то выводится информация о пользователях с правами сотрудника или администратора. В частности, отображается информация об уникальном идентификаторе пользователя, имени пользователя, а также роли пользователя в системе. В противном случае, выдается уведомление о соответствующей ошибке.

Прецедент: обновить работника.

Краткое описание: данный прецедент описывает процесс изменения информации о пользователе с правами сотрудника или администратора в системе контроля и управления доступом.

Актор: отдел кадров.

Зависимость: является экземпляром прецедента операции над работниками.

Предусловие: пользователь (сотрудник или администратор) вошел в систему с правами отдела кадров.

Основной поток событий: данный прецедент начинает выполняться, когда пользователь (сотрудник или администратор) с правами отдела кадров пытается изменить информацию о пользователе с правами сотрудника или администратора в системе. Рассмотрим последовательность событий более подробно:

1. задается уникальный идентификатор пользователя (сотрудника или администратора), информацию о котором необходимо изменить в системе;
2. задается новое имя пользователя (сотрудника или администратора), информацию о котором необходимо изменить в системе;
3. задается новый уникальный идентификатор смарт-карты для замены выданной пользователю (сотруднику или администратору), информацию о котором необходимо изменить в системе;

4. задается новая роль пользователя (сотрудника или администратора), информацию о котором необходимо изменить в системе;
5. формируется журнальная запись о произошедшем событии.

Альтернативные потоки событий: если в процессе изменения информации о пользователях с правами сотрудника или администратора, в результате поиска не обнаружено пользователя с заданным уникальным идентификатором, то выдается уведомление о соответствующей ошибке.

Постусловие: если прецедент выполнен успешно, то информация о пользователе с правами сотрудника или администратора изменяется. В частности, может быть изменения информация об имени пользователя, роли пользователя в системе, а также уникальном идентификаторе смарт-карты, принадлежащей пользователю. В противном случае, выдается уведомление о соответствующей ошибке.

Приложение Г. Диаграмма прецедентов операций над картами

Рассмотрим экземпляры (посмотреть свободные карты, удалить карту, создать карту) прецедента операции над картами более подробно (рисунок 13).

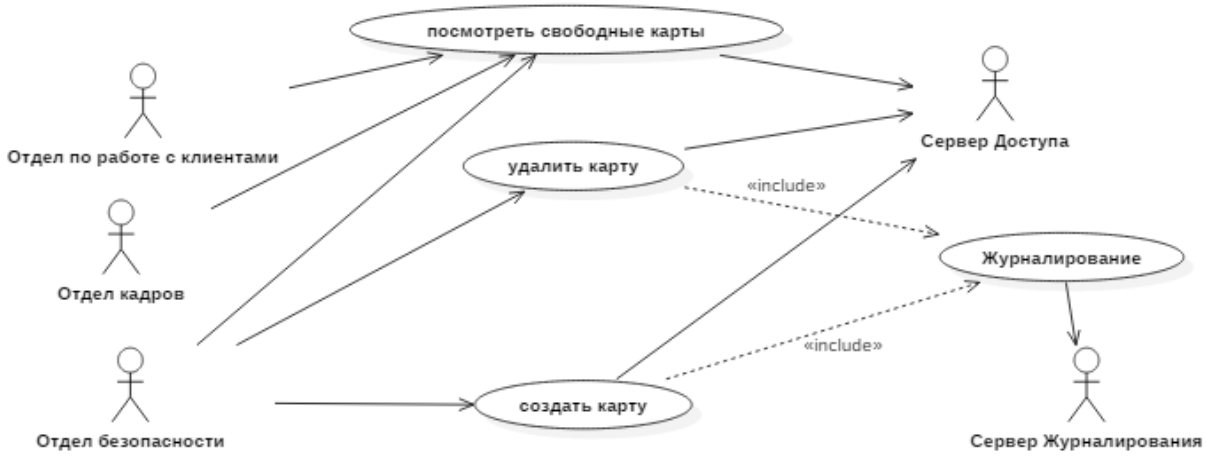

Рисунок 13 – Диаграмма прецедентов операций над картами

Прецедент: посмотреть свободные карты.

Краткое описание: данный прецедент описывает процесс просмотра информации о свободных уникальных идентификаторах смарт-карт, зарегистрированных в системе контроля и управления доступом.

Актор: отдел по работе с клиентами, отдел кадров, отдел безопасности.

Зависимость: является экземпляром прецедента операции над картами.

Предусловие: пользователь (сотрудник или администратор) вошел в систему с правами отдела по работе с клиентами, или отдела кадров, или отдела безопасности.

Основной поток событий: данный прецедент начинает выполняться, когда пользователь (сотрудник или администратор) с правами отдела по работе с клиентами, или отдела кадров, или отдела безопасности осуществляет поиск информации о свободных уникальных идентификаторах смарт-карт, зарегистрированных в системе. Рассмотрим последовательность событий более подробно:

1. поиск по уникальному идентификатору смарт-карты;
2. вывод всех смарт-карт, отмеченных в качестве свободных.

Альтернативные потоки событий: если в процессе поиска информации о свободных уникальных идентификаторах смарт-карт, в результате поиска не обнаружено смарт-карт с заданными параметрами, то выдается уведомление о соответствующей ошибке.

Постусловие: если прецедент выполнен успешно, то информация о свободных уникальных идентификаторах смарт-карт отображается. В противном случае, выдается уведомление о соответствующей ошибке.

Прецедент: удалить карту.

Краткое описание: данный прецедент описывает процесс удаления информации о смарт-картах, зарегистрированных в системе контроля и управления доступом.

Актор: отдел безопасности.

Зависимость: является экземпляром прецедента операции над картами.

Предусловие: пользователь (сотрудник или администратор) вошел в систему с правами отдела безопасности. Смарт-карта, информация о которой удаляется, не привязана к пользователю системы.

Основной поток событий: данный прецедент начинает выполняться, когда пользователь (сотрудник или администратор) с правами отдела безопасности пытается удалить информацию о смарт-картах, зарегистрированных в системе. Рассмотрим последовательность событий более подробно:

1. задается уникальный идентификатор смарт-карты, информацию о которой необходимо удалить из системы;
2. формируется журнальная запись о произошедшем событии.

Альтернативные потоки событий: если в процессе удаления информации о смарт-картах, в результате поиска не обнаружено смарт-карт с заданными параметрами или смарт-карта с заданными параметрами привязана к пользователю системы, то выдается уведомление о соответствующей ошибке.

Постусловие: если прецедент выполнен успешно, то информация о смарт-картах удаляется из системы. В противном случае, выдается уведомление о соответствующей ошибке.

Прецедент: создать карту.

Краткое описание: данный прецедент описывает процесс создания (регистрации) смарт-карты в системе контроля и управления доступом.

Актор: отдел безопасности.

Зависимость: является экземпляром прецедента операции над картами.

Предусловие: пользователь (сотрудник или администратор) вошел в систему с правами отдела безопасности.

Основной поток событий: данный прецедент начинает выполняться, когда пользователь (сотрудник или администратор) с правами отдела безопасности пытается создать (зарегистрировать) смарт-карту в системе. Рассмотрим последовательность событий более подробно:

1. задается уникальный идентификатор смарт-карты, информацию о которой необходимо зарегистрировать в системе;
2. формируется журнальная запись о произошедшем событии.

Альтернативные потоки событий: если в процессе создания (регистрации) смарт-карты в системе, обнаружено, что смарт-карта с заданными параметрами уже существует (зарегистрирована) в системе, то выдается уведомление о соответствующей ошибке.

Постусловие: если прецедент выполнен успешно, то информация о смарт-карте регистрируется в системе. В противном случае, выдается уведомление о соответствующей ошибке.

Приложение Д. Диаграмма прецедентов операций над ролями

Рассмотрим экземпляры (создать роль, удалить роль, посмотреть роль, обновить роль) прецедента операции над ролями более подробно (рисунок 14).

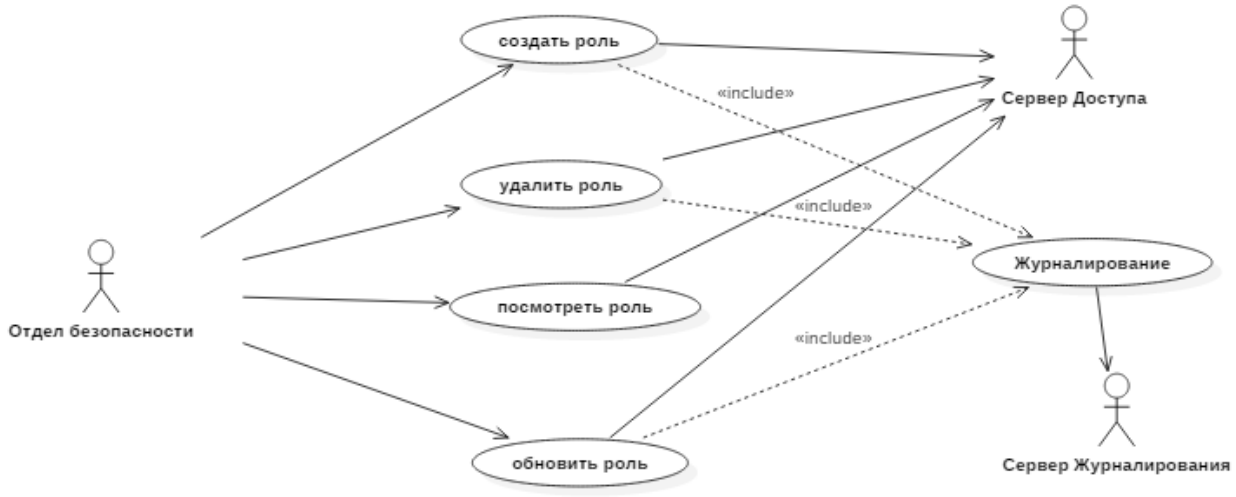

Рисунок 14 – Диаграмма прецедентов операций над ролями

Прецедент: создать роль.

Краткое описание: данный прецедент описывает процесс создания роли пользователей в системе контроля и управления доступом.

Актор: отдел безопасности.

Зависимость: является экземпляром прецедента операции над ролями.

Предусловие: пользователь (сотрудник или администратор) вошел в систему с правами отдела безопасности.

Основной поток событий: данный прецедент начинает выполняться, когда пользователь (сотрудник или администратор) с правами отдела безопасности пытается создать новую роль пользователей в системе. Рассмотрим последовательность событий более подробно:

1. задается название новой роли, информацию о которой необходимо зарегистрировать в системе;
2. формируется журнальная запись о произошедшем событии.

Альтернативные потоки событий: если в процессе создания новой роли в системе обнаружено, что роль с заданными параметрами уже существует (зарегистрирована) в системе, то выдается уведомление о соответствующей ошибке.

Постусловие: если прецедент выполнен успешно, то информация о новой роли регистрируется в системе. В противном случае, выдается уведомление о соответствующей ошибке.

Прецедент: посмотреть роль.

Краткое описание: данный прецедент описывает процесс поиска информации о ролях пользователей, зарегистрированных в системе контроля и управления доступом.

Актор: отдел безопасности.

Зависимость: является экземпляром прецедента операции над ролями.

Предусловие: пользователь (сотрудник или администратор) вошел в систему с правами отдела безопасности.

Основной поток событий: данный прецедент начинает выполняться, когда пользователь (сотрудник или администратор) с правами отдела безопасности осуществляет поиск информации о ролях пользователей, зарегистрированных в системе. Рассмотрим последовательность событий более подробно:

1. поиск по уникальному идентификатору роли;
2. поиск по названию роли;
3. комбинированный поиск.

Альтернативные потоки событий: если в процессе поиска информации о ролях пользователей в системе, обнаружено, что роль с заданными параметрами не существует (не зарегистрирована) в системе, то выдается уведомление о соответствующей ошибке.

Постусловие: если прецедент выполнен успешно, то информация о ролях пользователей, удовлетворяющих заданным параметрам, отображается в системе. В частности, отображается информация об уникальном идентифика-

торе и названии роли. В противном случае, выдается уведомление о соответствующей ошибке.

Прецедент: удалить роль.

Краткое описание: данный прецедент описывает процесс удаления роли из системы контроля и управления доступом.

Актор: отдел безопасности.

Зависимость: является экземпляром прецедента операции над ролями.

Предусловие: пользователь (сотрудник или администратор) вошел в систему с правами отдела безопасности.

Основной поток событий: данный прецедент начинает выполняться, когда пользователь (сотрудник или администратор) с правами отдела безопасности пытается удалить информацию о роли, зарегистрированной в системе. Рассмотрим последовательность событий более подробно:

1. задается уникальный идентификатор роли, информацию о которой необходимо удалить из системы;
2. формируется журнальная запись о произошедшем событии.

Альтернативные потоки событий: если в процессе создания (регистрации) смарт-карты в системе, обнаружено, что роль с заданными параметрами уже используется в качестве роли хотя бы одного из пользователей системы, то выдается уведомление о соответствующей ошибке.

Постусловие: если прецедент выполнен успешно, то информация о смарт-карте регистрируется в системе. В противном случае, выдается уведомление о соответствующей ошибке.

Прецедент: обновить роль.

Краткое описание: данный прецедент описывает процесс изменения информации о ролях пользователей, зарегистрированных в системе контроля и управления доступом.

Актор: отдел безопасности.

Зависимость: является экземпляром прецедента операции над ролями.

Предусловие: пользователь (сотрудник или администратор) вошел в систему с правами отдела безопасности.

Основной поток событий: данный прецедент начинает выполняться, когда пользователь (сотрудник или администратор) с правами отдела безопасности пытается изменить информацию о ролях пользователей, зарегистрированных в системе. Рассмотрим последовательность событий более подробно:

1. задается уникальный идентификатор роли, информацию о которой необходимо изменить;
2. задается новое название роли, информацию о которой необходимо изменить;
3. формируется журнальная запись о произошедшем событии.

Альтернативные потоки событий: если в процессе изменения информации о ролях пользователей в системе, обнаружено, что роль с заданными параметрами принадлежит хотя бы одному из пользователей системы, то выдается уведомление о соответствующей ошибке.

Постусловие: если прецедент выполнен успешно, то информация о ролях пользователей, удовлетворяющих заданным параметрам, изменяется в системе. В противном случае, выдается уведомление о соответствующей ошибке.

Приложение Е. Диаграмма прецедентов операций над аккаунтами

Рассмотрим экземпляры (создать аккаунт, удалить аккаунт, посмотреть аккаунт, обновить аккаунт) прецедента операции над аккаунтами более подробно (рисунок 15).

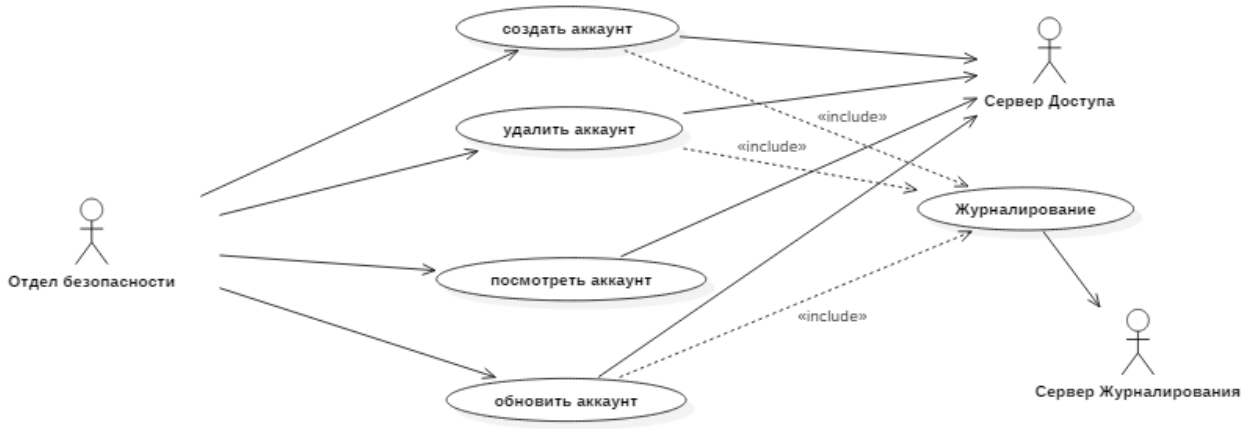

Рисунок 15 – Диаграмма прецедентов операций над аккаунтами

Прецедент: создать аккаунт.

Краткое описание: данный прецедент описывает процесс создания (регистрации) аккаунта пользователя с правами сотрудника или администратора в системе контроля и управления доступом.

Актор: отдел безопасности.

Зависимость: является экземпляром прецедента операции над аккаунтами.

Предусловие: пользователь (сотрудник или администратор) вошел в систему с правами отдела безопасности.

Основной поток событий: данный прецедент начинает выполняться, когда пользователь (сотрудник или администратор) с правами отдела безопасности пытается создать (зарегистрировать) аккаунт пользователя с правами сотрудника или администратора в системе. Рассмотрим последовательность событий более подробно:

1. задается уникальный идентификатор пользователя (сотрудника или администратора);

2. задается пара логин/пароль для пользователя (сотрудника или администратора);
3. задается отдел пользователя (сотрудника или администратора);
4. формируется журнальная запись о произошедшем событии.

Альтернативные потоки событий: если в процессе создания (регистрации) аккаунта пользователей в системе, обнаружено, что не введены данные о логине/пароле пользователя или не назначен отдел, то выдается уведомление о соответствующей ошибке.

Постусловие: если прецедент выполнен успешно, то создается (регистрируется) аккаунт пользователя в системе. При этом в системе отображается информация об уникальном идентификаторе созданного (зарегистрированного) аккаунта пользователя. В противном случае, выдается уведомление о соответствующей ошибке.

Прецедент: удалить аккаунт.

Краткое описание: данный прецедент описывает процесс удаления информации об аккаунте пользователя с правами сотрудника или администратора из системы контроля и управления доступом.

Актор: отдел безопасности.

Зависимость: является экземпляром прецедента операции над аккаунтами.

Предусловие: пользователь (сотрудник или администратор) вошел в систему с правами отдела безопасности.

Основной поток событий: данный прецедент начинает выполняться, когда пользователь (сотрудник или администратор) с правами отдела безопасности пытается удалить информацию об аккаунте пользователя с правами сотрудника или администратора из системы. Рассмотрим последовательность событий более подробно:

1. задается уникальный идентификатор пользователя (сотрудника или администратора), информацию об аккаунте которого необходимо удалить из системы;

2. формируется журнальная запись о произошедшем событии.

Альтернативные потоки событий: если в процессе удаления информации об аккаунте пользователя в системе, обнаружено, что аккаунта с уникальным идентификатором, указанным в качестве параметра для удаления, не существует, то выдается уведомление о соответствующей ошибке.

Постусловие: если прецедент выполнен успешно, то информация об аккаунте пользователя удаляется из системы. При этом в системе отображается информация об уникальном идентификаторе аккаунта, информация о котором была удалена. В противном случае, выдается уведомление о соответствующей ошибке.

Прецедент: посмотреть аккаунт.

Краткое описание: данный прецедент описывает процесс поиска информации об аккаунтах пользователей с правами сотрудника или администратора в системе контроля и управления доступом.

Актор: отдел безопасности.

Зависимость: является экземпляром прецедента операции над аккаунтами.

Предусловие: пользователь (сотрудник или администратор) вошел в систему с правами отдела безопасности.

Основной поток событий: данный прецедент начинает выполняться, когда пользователь (сотрудник или администратор) с правами отдела безопасности осуществляет поиск информации об аккаунтах пользователей с правами сотрудника или администратора в системе. Рассмотрим последовательность событий более подробно:

1. поиск по уникальному идентификатору пользователя (сотрудника или администратора);
2. поиск по уникальному идентификатору аккаунта пользователя (сотрудника или администратора);
3. поиск по логину аккаунта пользователя (сотрудника или администратора);

4. поиск по отделу/отделам аккаунта пользователя (сотрудника или администратора);
5. комбинированный поиск.

Альтернативные потоки событий: если в процессе поиска информации об аккаунтах пользователей в системе, обнаружено, что аккаунтов, соответствующих заданным параметрам, не существует, то выдается уведомление о соответствующей ошибке.

Постусловие: если прецедент выполнен успешно, то информация об аккаунтах пользователей отображается в системе. В частности, при выводе результатов поиска, отображается уникальный идентификатор аккаунта, информация о логине аккаунта, имя пользователя, уникальный идентификатор пользователя, отделы аккаунта. В противном случае, выдается уведомление о соответствующей ошибке.

Прецедент: обновить аккаунт.

Краткое описание: данный прецедент описывает процесс изменения информации об аккаунте пользователя с правами сотрудника или администратора в системе контроля и управления доступом.

Актор: отдел безопасности.

Зависимость: является экземпляром прецедента операции над аккаунтами.

Предусловие: пользователь (сотрудник или администратор) вошел в систему с правами отдела безопасности.

Основной поток событий: данный прецедент начинает выполняться, когда пользователь (сотрудник или администратор) с правами отдела безопасности пытается изменить информацию об аккаунте пользователя с правами сотрудника или администратора в системе. Рассмотрим последовательность событий более подробно:

1. задается уникальный идентификатор аккаунта пользователя (сотрудника или администратора), информацию об аккаунте которого необходимо изменить в системе;

2. задается новый пароль аккаунта пользователя (сотрудника или администратора), информацию об аккаунте которого необходимо изменить в системе;
3. задается новый логин аккаунта пользователя (сотрудника или администратора), информацию об аккаунте которого необходимо изменить в системе;
4. задается новый состав отделов аккаунта пользователя (сотрудника или администратора), информацию об аккаунте которого необходимо изменить в системе;
5. формируется журнальная запись о произошедшем событии.

Альтернативные потоки событий: если в процессе изменения информации об аккаунте пользователя в системе, обнаружено, что аккаунта с уникальным идентификатором, указанным в качестве параметра для изменения, не существует, то выдается уведомление о соответствующей ошибке.

Постусловие: если прецедент выполнен успешно, то информация об аккаунте пользователя изменяется в системе. В противном случае, выдается уведомление о соответствующей ошибке.

Приложение Ж. Диаграмма прецедентов операций над политиками

Рассмотрим экземпляры (изменить политику, посмотреть политику) прецедента операции над политиками более подробно (рисунок 16).

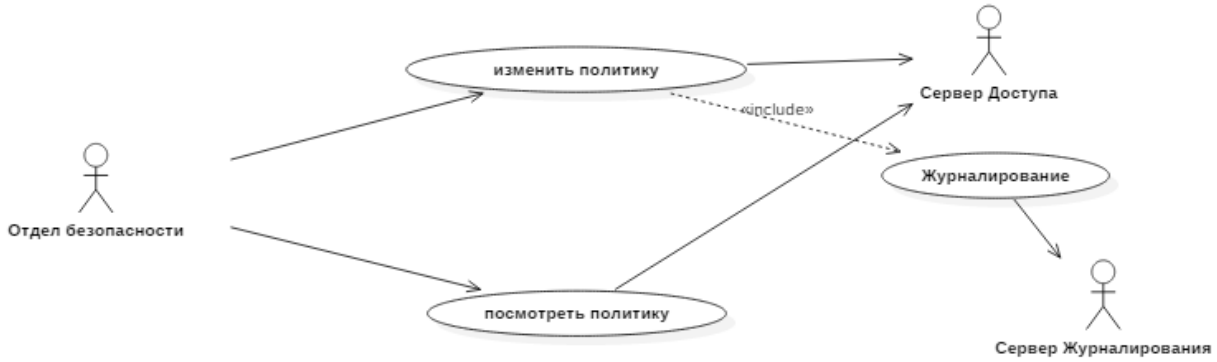

Рисунок 16 – Диаграмма прецедентов операций над политиками

Прецедент: посмотреть политику.

Краткое описание: данный прецедент описывает процесс поиска информации о политике безопасности, установленной в системе контроля и управления доступом.

Актор: отдел безопасности.

Зависимость: является экземпляром прецедента операции над политиками.

Предусловие: пользователь (сотрудник или администратор) вошел в систему с правами отдела безопасности.

Основной поток событий: данный прецедент начинает выполняться, когда пользователь (сотрудник или администратор) с правами отдела безопасности осуществляет поиск о политике безопасности, установленной в системе. Рассмотрим последовательность событий более подробно:

1. поиск по уникальному идентификатору роли пользователя в системе;
2. поиск по уникальному идентификатору встроенного устройства;
3. комбинированный поиск.

Альтернативные потоки событий: если в процессе поиска информации о политике безопасности, установленной в системе, обнаружено, что информа-

ции, удовлетворяющей заданным параметрам, не существует, то выдается уведомление о соответствующей ошибке.

Постусловие: если прецедент выполнен успешно, то информация о политике безопасности, установленной в системе, отображается. В частности, при выводе результатов поиска, отображается уникальный идентификатор роли и ее наименование, уникальный идентификатор встроенного устройства, его IP-адрес и спецификация, а также информация о наличии или отсутствии прав у роли на доступ к помещению (через встроенное устройство). В противном случае, выдается уведомление о соответствующей ошибке.

Прецедент: изменить политику.

Краткое описание: данный прецедент описывает процесс изменения политики безопасности, установленной в системе контроля и управления доступом.

Актор: отдел безопасности.

Зависимость: является экземпляром прецедента операции над политиками.

Предусловие: пользователь (сотрудник или администратор) вошел в систему с правами отдела безопасности.

Основной поток событий: данный прецедент начинает выполняться, когда пользователь (сотрудник или администратор) с правами отдела безопасности пытается изменить политику безопасности, установленную в системе. Рассмотрим последовательность событий более подробно:

1. задается уникальный идентификатор роли пользователя в системе;
2. задается уникальный идентификатор встроенного устройства в системе;
3. задается новое значение (наличие или отсутствие) прав доступа роли пользователя к помещению (через встроенное устройство);
4. формируется журнальная запись о произошедшем событии.

Альтернативные потоки событий: если в процессе изменения информации о политике безопасности, установленной в системе, обнаружено, что части

политики, соответствующей заданным параметрам, не существует, то выдается уведомление о соответствующей ошибке.

Постусловие: если прецедент выполнен успешно, то информация о политике безопасности, установленной в системе, изменяется. В противном случае, выдается уведомление о соответствующей ошибке.

Приложение И. Прошивка встроенного устройства системы контроля и управления доступом в помещения на основе бесконтактных смарт-карт

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2015662137

Прошивка встроенного устройства системы контроля и управления доступом в помещения на основе бесконтактных смарт-карт

Правообладатель: ***Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН) (RU)***

Авторы: ***Левшун Дмитрий Сергеевич (RU),***
Чечулин Андрей Алексеевич (RU)

Заявка № **2015619114**
Дата поступления **01 октября 2015 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***17 ноября 2015 г.***

Руководитель Федеральной службы
по интеллектуальной собственности

Г.П. Ивлиев

Приложение К. Система поддержки и управления доступом к базе данных системы контроля и управления доступом в помещения на основе бесконтактных смарт-карт

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2016612543

«Система поддержки и управления доступом к базе данных системы контроля и управления доступом в помещения на основе бесконтактных смарт-карт»

Правообладатель: ***Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН) (RU)***

Авторы: ***Левшун Дмитрий Сергеевич (RU), Чечулин Андрей Алексеевич (RU), Котенко Игорь Витальевич (RU)***

Заявка № **2015619124**

Дата поступления **01 октября 2015 г.**

Дата государственной регистрации в Реестре программ для ЭВМ ***01 марта 2016 г.***

Руководитель Федеральной службы по интеллектуальной собственности

Г.П. Ивлиев

Приложение Л. База данных сервера журналирования защищенной системы контроля и управления доступом для модели Умного дома

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации базы данных

№ 2016621608

База данных сервера журналирования защищенной системы контроля и управления доступом для модели Умного дома

Правообладатель: ***Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН) (RU)***

Авторы: ***Левшун Дмитрий Сергеевич (RU),***
Чечулин Андрей Алексеевич (RU)

Заявка № **2016621268**
Дата поступления **29 сентября 2016 г.**
Дата государственной регистрации
в Реестре баз данных ***29 ноября 2016 г.***

Руководитель Федеральной службы
по интеллектуальной собственности

Г.П. Ивлиев

Приложение М. Компонент, реализующий сетевой уровень межконтроллерного взаимодействия на базе протокола I2C

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2016663951

Компонент, реализующий сетевой уровень межконтроллерного взаимодействия на базе протокола I2C

Правообладатель: ***Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН) (RU)***

Авторы: ***Левшун Дмитрий Сергеевич (RU), Чечулин Андрей Алексеевич (RU), Котенко Игорь Витальевич (RU)***

Заявка № **2016660118**
Дата поступления **29 сентября 2016 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***20 декабря 2016 г.***

Руководитель Федеральной службы по интеллектуальной собственности

Г.П. Ивлиев