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

Институт информационных технологий и телекоммуникаций
Кафедра информационной безопасности автоматизированных систем

Утверждена распоряжением по институту
От «02» марта 2020 г. № 013-р/12.00

Допущена к защите
«18» июня 2020 г.
Зав. кафедрой информационной безопасности автоматизированных систем
канд. техн. наук, профессор
А. Ф. Чипига

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

РАЗРАБОТКА СПОСОБА ВЗАИМНОЙ АУТЕНТИФИКАЦИИ С ИСПОЛЬЗОВАНИЕМ СВОЙСТВ ФИЗИЧЕСКИ НЕКЛОНИРУЕМЫХ ФУНКЦИЙ НА ОСНОВЕ МИКРОСХЕМ СТАТИЧЕСКОЙ ПАМЯТИ

Рецензенты:
Козлов Сергей Ильич
заведующий сектором по защите информации и специальной работе Министерства энергетики промышленности и связи СК

Выполнил:
Моторикин Денис Вадимович
Студент 5 курса, группы ИБС-с-о-15-1 специальности 10.05.03 «Информационная безопасность автоматизированных систем» специализация «Защищенные автоматизированные системы управления» очной формы обучения

Нормоконтролер:
Гиш Татьяна Александровна
доцент кафедры информационной безопасности автоматизированных систем

Научный руководитель:
Новикова О. В.
канд. физ.-мат. наук, доцент кафедры информационной безопасности автоматизированных систем

Дата защиты:
« _____» _____ 2020 г.

Оценка: _____

Ставрополь, 2020 г.

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

Институт информационных технологий и телекоммуникаций
Кафедра информационной безопасности автоматизированных систем

Утверждена распоряжением по институту
От «02» марта 2020 г. № 013-р/12.00

Допущена к защите
«18» июня 2020 г.
Зав. кафедрой информационной безопасности автоматизированных систем
канд. техн. наук, профессор
А. Ф. Чипига
(подпись)

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ (ДИПЛОМНОМУ ПРОЕКТУ) НА ТЕМУ:

РАЗРАБОТКА СПОСОБА ВЗАИМНОЙ АУТЕНТИФИКАЦИИ С ИСПОЛЬЗОВАНИЕМ СВОЙСТВ ФИЗИЧЕСКИ НЕКЛОНИРУЕМЫХ ФУНКЦИЙ НА ОСНОВЕ МИКРОСХЕМ СТАТИЧЕСКОЙ ПАМЯТИ

Автор дипломного проекта 17.06.2020 г. Моторикин Денис Вадимович
подпись

Специальность 10.05.03 Информационная безопасность автоматизированных систем

Специализация Защищенные автоматизированные системы управления

Группа ИБС-с-о-15-1

Руководитель проекта 17.06.2020 г. О. В. Новикова
подпись

Консультантыы по разделам:
Безопасность и экологичность проекта О. В. Новикова

Организационно-экономический раздел О. В. Новикова

Нормоконтролер Т. А. Гиш

Ставрополь, 2020 г.

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

Институт информационных технологий и телекоммуникаций
Кафедра информационной безопасности автоматизированных систем
Специальность 10.05.03 Информационная безопасность автоматизированных систем
Специализация Защищенные автоматизированные системы управления

«УТВЕРЖДАЮ»
Зав. кафедрой информационной безопасности автоматизированных систем, канд. техн. наук, профессор
Чипига А. Ф.
«13» декабря 2019 г.

ЗАДАНИЕ НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ РАБОТУ
(ДИПЛОМНЫЙ ПРОЕКТ)

Студент Моторикин Денис Вадимович группа ИБС-с-о-15-1
1. Тема Разработка способа взаимной аутентификации с использованием свойств физически неклонируемых функций на основе микросхем статической памяти
Утверждена распоряжением по институту № 013-р/12.00 от «02» марта 2020 г.
2. Срок представления проекта к защите «18» июня 2020 г.
3. Исходные данные для проектирования массив данных с 7 микросхем статической памяти
4. Содержание пояснительной записки:
4.1 Анализ достоинств и недостатков технологий и средств обеспечения идентификации и аутентификации в системах контроля и управления доступом.
4.2 Анализ свойств физически неклонируемых функций СОЗУ и определение оптимальной длины вектора инициализации алгоритма взаимной аутентификации на основе ФНФ.
4.3 Разработка алгоритмов исследования статической ОЗУ и взаимной аутентификации на основе свойств физически неклонируемых функций СОЗУ.
4.4 Безопасность и экологичность проекта
4.5 Организационно-экономический раздел
4.6 Другие разделы проекта
5. Перечень графического материала
Дата выдачи задания « 13 » декабря 2019 г.
Руководитель проекта _____ О. В. Новикова
подпись

Консультанты по разделам:
безопасность и экологичность проекта _____ О. В. Новикова
подпись

организационно-экономический раздел _____ О. В. Новикова
подпись

Задание принял к исполнению «13» декабря 2019 г. _____ Д. В. Моторикин
подпись

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

Институт информационных технологий и телекоммуникаций
Кафедра информационной безопасности автоматизированных систем
Специальность 10.05.03 Информационная безопасность автоматизированных систем
Специализация Защищенные автоматизированные системы управления

КАЛЕНДАРНЫЙ ПЛАН

Фамилия, имя, отчество Моторикин Денис Вадимович
Тема ВКР Разработка способа взаимной аутентификации с использованием свойств физически неклонируемых функций на основе микросхем статической памяти
Руководитель канд. физ.-мат. наук Новикова О. В.
Консультанты безопасность и экологичность работы канд. физ.-мат. наук Новикова О. В.
организационно-экономический раздел канд. физ.-мат. наук Новикова О. В.

№	Наименование этапов выпускной квалификационной работы	Срок выполнения работы	Примечание
1.	Подбор и анализ научно-технической литературы по теме исследования	13.12.19 – 31.01.20	
2.	Анализ достоинств и недостатков технологий и средств обеспечения идентификации и аутентификации в системах контроля и управления доступом	01.02.20 – 16.02.20	
3.	Анализ свойств физически неклонируемых функций СОЗУ и определение оптимальной длины вектора инициализации алгоритма взаимной аутентификации на основе ФНФ	17.02.20 – 08.03.20	
4.	Разработка алгоритмов исследования статической ОЗУ и взаимной аутентификации на основе свойств физически неклонируемых функций СОЗУ	09.03.20 – 30.03.20	
5.	Оценка безопасности и экологичности работы, оценка технико-экономической эффективности работы	31.04.20 – 19.05.20	
6.	Оформление пояснительной записки	20.05.20 – 05.06. 20	
7.	Подготовка доклада и презентационного материала	06.06.20 – 12.06.20	
8.	Представление выпускной квалификационной работы на кафедру, предварительная защита, брошюровка пояснительной записки, получение допуска к защите.	12.06.20 – 18.06.20	

Научный руководитель _____ Новикова О. В.
подпись

Зав. кафедрой _____ Чипига А. Ф.
подпись

«13» декабря 2019 г.

Содержание

Введение

В настоящее время информационная безопасность одна из важнейших задач необходимая для функционирования предприятия. Защита от воздействий из вне становится более совершенней, что заставляет злоумышленников пытаться использовать внутренние уязвимости организаций.

Основным методами реализации внутренних уязвимостей является социальная инженерия, поскольку человеческий фактор всегда может повлиять на защищенность системы. Одной из возможных целей злоумышленника является проникновение в контролируемую зону, чтобы получить прямой доступ к оборудованию или реализовать иные угрозы. Поскольку контролируемая зона на предприятиях защищается системами контроля и управления доступом(СКУД), в неё становится довольно сложно попасть, не имея идентификатора, такого как touch memory или smart-card. Однако, угроза проникновения в контрольную зону, при установленной системе контроля и управлением доступом, не исчезает. Зачастую в системах СКУД используется однофакторный не защищённый идентификатор. Данный идентификатор являются пассивными элементами, которые будут передавать данные любому контроллеру, без предварительной проверки, вследствие чего очень легко произвести дубликат. Наличие дубликата идентификатора в руках злоумышленника упрощает задачу по проникновению в контролируемую зону предприятия.

Для того чтобы обезопасить идентификатор предлагается способ защиты карт доступа от несанкционированного изготовления дубликата, как взаимная аутентификации с использованием свойств физически неклонируемых функций(PUF) на основе микросхем статической оперативной памяти.

Физически неклонируемая функция (Physical Unclonable Function, PUF) – это функция построенная на уникальной физической структуре объекта , которую можно просто проанализировать, но крайне сложно смоделировать или воспроизвести. Уникальность физической структуры объекта, на основе которой формируется PUF, происходит из того что объект состоит из множества

случайных компонентов, возникающих в ходе производства. Данные компоненты неконтролируемы в ходе производственного процесса. PUF – это физическая система, которая при воздействии на неё (запросе) порождает уникальный и непредсказуемый ответ.

Принцип действия взаимной аутентификации с использованием свойств физически неклонируемых функций на основе микросхем статической памяти, заключается в том, что контроллер, получив от карты доступа случайно сгенерированный набор данных и зная параметры карты доступа сможет вычислить уникальный для карты доступа и сессии авторизации ответ. Карта доступа также вычислит ответ, которой при совпадении с ответом контроллера подтвердит то, что контроллер является действительным и можно передавать данные для авторизации карты доступа. И благодаря тому, что точной копии статической оперативной памяти воссоздать невозможно, параметры для каждой карты доступа будут уникальными.

В дипломном проекте рассмотрена тема: «Разработка способа взаимной аутентификации с использованием свойств физически неклонируемых функций на основе микросхем статической памяти». Предлагаемое в данном проекте решение может быть использовано для обеспечения защиты от несанкционированного изготовления дубликата карт доступа в системах контроля и управления доступом для организации контролируемой зоны предприятия.

Актуальность данного проекта объясняется не только современными тенденциями разработок более надежных методов аутентификации, но и необходимостью разработки методов, которые будут более эффективны и менее затратные для организации аутентификации.

В проекте предлагается повысить безопасность карт доступа, не используя блочные алгоритмы шифрования, а использовать уникальные свойства статической оперативной памяти, которые невозможно воспроизвести.

Разработанность: в дипломном проекте разработан новый способ обеспечения взаимной аутентификации карты доступа и котроллера доступа, исключающий изготовления дубликата карты доступа.

Цель: разработка способа взаимной аутентификации на основе свойств физически неклонируемых функции статического оперативно запоминающего устройства (СОЗУ).

Задачи:

1. Исследовать возможность использования любой СОЗУ в качестве PUF;
2. Разработать алгоритм определения оптимальной длины вектора инициализации.
3. Разработать алгоритм взаимной аутентификации, основанный на свойствах физически не клонируемости функций статической ОЗУ, учитывая известность работы алгоритма злоумышленнику и его попыток провести анализ карты доступа и просушки открытого канала обмена данными между картой доступа и контроллером доступа.

Объект: модель защищенной карты доступа на основе свойств физически неклонируемых функций микросхем статической оперативной памяти.

Предмет: способ взаимной аутентификации карты доступа и контроллера доступа на основе свойств физически неклонируемых функций микросхем статической оперативной памяти.

Методологические основы проекта: способы аутентификации в современных системах связи.

Информационную базу проекта составляют результаты научных исследований в области PUF, стандарты и нормативные документы по протоколам аутентификациям в системах СКУД.

Дипломный проект состоит из введения, пяти глав, заключения и списка используемой литературы. Во введении представлены постановка задачи, актуальность темы дипломного проекта, цель и основные задачи проекта, объект и предмет исследования, методологическая основа проекта и информационная база проекта.

В первой главе проведен анализ достоинств и недостатков существующих технологий и средств обеспечения идентификации аутентификации в системах контроля и управления доступом. Построена модель угроз для систем СКУД.

Проанализированы основные угрозы защиты информации. Описаны шаги решения актуальных угроз.

Во второй главе проанализированы свойства физически неклонируемых функций (ФНФ) на основе статической ОЗУ. В третьей главе описаны разработанные алгоритмы исследования СОЗУ и взаимной аутентификации на основу ФНФ статической ОЗУ. В четвертой главе описана безопасность и экологичность проекта. В пятой главе произведено технико-экономическое обоснование созданного проекта. В заключении приведены общие выводы о проделанной работе и рекомендуемые направления по дальнейшей разработке темы.

1. Анализ достоинств и недостатков технологий и средств обеспечения идентификации и аутентификации в системах контроля и управления доступом

1.1. Анализ систем на основе односторонней аутентификации с использованием контактных ключей

При организации системы контроля и управления доступом одним из вариантов её реализации является использование системы с контактным ключом. Примером такой системы могут послужить электронные ключи Dallas Touch Memory, также известные как электронные идентификаторы iButton.

Основой электронного ключа Touch Memory является герметичный корпус, выполненный в виде таблетки диаметром 16 мм, верхняя крышка которого электрически изолирована от нижней части. При этом верхняя крышка является контактом данных, а нижняя – общим контактом. Внутри корпуса размещается кремниевый чип (микросхема).

Таблетка Touch Memory выступает в качестве пассивного идентификатора, поскольку и питание, и опрос осуществляются через контроллер СКУД.

Принцип работы интерфейса Touch Memory заключается в использовании интерфейса iButton для связи между контроллером и считывателем. Контроллер эмулирует поведение ключа и контактора. Таким образом осуществляется возможность использовать простую схему передачи данных. Также это позволяет лучше защитить идентификатор от считывания.

Для обмена данными между считывателем и контроллером используется всего одна двунаправленная сигнальная линия, на которой по времени отсутствия напряжения определяется содержимое бита данных.

В качестве считывателя выступает контактор, при соприкосновении которого с идентификатором происходит передача на контроллер уникального 48-битного номера и на основании полученных данных принятие решения о допуске или отказе в доступе.

Достоинства электронных ключей Dallas Touch Memor:

- небольшой размер;
- простой и быстрый обмен данными по протоколу 1-Wire;
- идентификация по касанию;

Недостатки электронных ключей Dallas Touch Memory:

- недостаточная защищенность ключа от изготовления дубликата;
- низкая помехоустойчивость протокола Touch Memory;
- отсутствие контроля целостности линии.

Данные ключи легко компрометируются ввиду не защищенности уникального номера, так как ключ является пассивным идентификатором и передает уникальный номера любому подходящему считывателю.

1.2. Анализ систем на основе односторонней аутентификации с использованием бесконтактных ключей

Для организации системы контроля и управления доступом также применяются системы, где в качестве идентификатора используется бесконтактные ключи. Рассмотрим такие системы на примерах Proximity и MIFARE.

У карт доступа наблюдается схожая схема фазы аутентификации. Контроллер излучает переменное электромагнитное поле стандартной частоты, что активирует карту доступа. Далее карта передаёт необходимую для аутентификации информацию. И на основе полученной информации контроллер определяет открыть доступ или отказать в выдаче доступа к защищаемому помещению. Можно заметить, что фаза аутентификации проходит в 3 этапа:

1. Активации карты доступа.
2. Передачи данных.
3. Приятие решение о доступе.

Схема фазы аутентификации, представлена на рисунке 1.1.

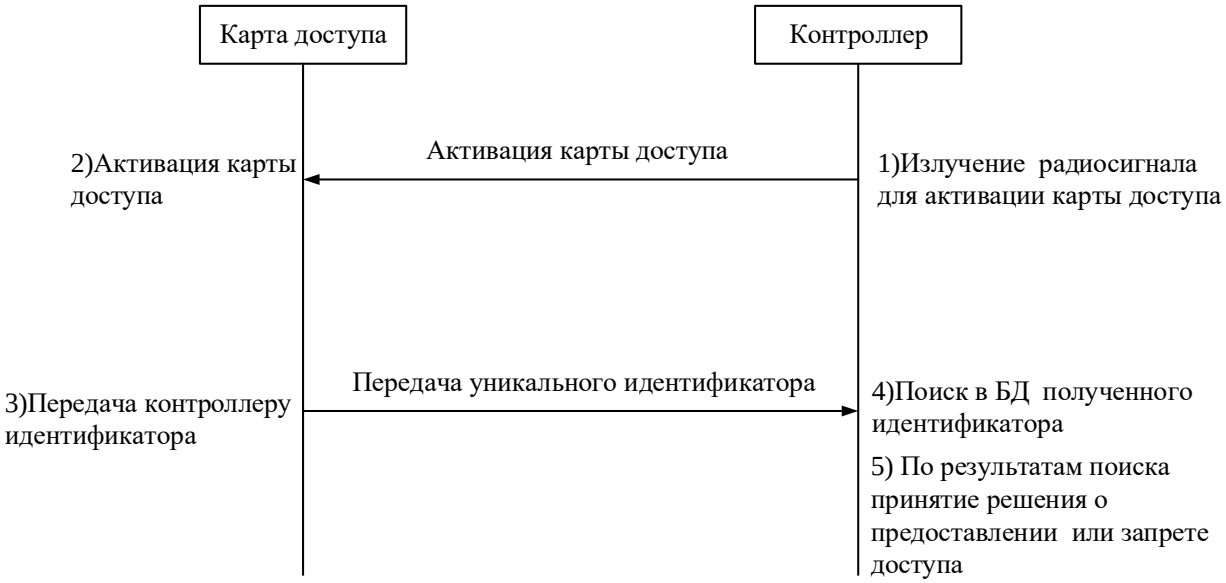

Рисунок 1.1 – Схема фазы аутентификации

Бесконтактная карта доступа Proximity, работает на частоте 125 кГц. Радиус действия карты составляет от 6 до 50 сантиметров.

Proximity карты поддерживают различные способы идентификации, помимо стандартной технологии бесконтактной идентификации, карта поддерживает способы: идентификация по фото, штрих-коду и др.

Внутри каждой пассивной карты доступа размещена электронная микросхема. В состав микросхемы входит приемник, передатчик и процессор, в памяти которого записывается и хранится идентификационный код карты. Каждый Proximity-считыватель постоянно излучает радиосигнал. При попадании в зону действия этого излучения Proximity карта активизируется и посылает в ответ сигнал, содержащий ее уникальный код доступа.

Активация карты доступа и последующая передача кода считывателю производятся за счет приема и накопления Proximity картой высокочастотной энергии, излучаемой считывателем. Считывание кода с карты происходит без непосредственного контакта на определенном расстоянии от считывателя, которое определяется мощностью передатчика считывателя. При этом позиционирование Proximity карты относительно считывателя не имеет значения.

Общими недостатками СКУД, использующих Proximity карты является:

1. Передача серийного номера на считывающее устройство в незашифрованном виде. При необходимости его можно легко перехватить, а затем записать в другую карту.

2. Сложность обеспечения совместимости карт, изготовленных по различным технологиям, с конкретными считывающими устройствами.

3. Уменьшение скорости обмена информацией в процессе прохождения аутентификации, которое происходит при внедрении в Proximity карты или считывающие устройства дополнительных степеней защиты.

MIFARE ещё один представитель кард доступа основанный на технологии RFID (Radio Frequency IDentification, радиочастотная идентификация) – способ автоматической идентификации объектов, в котором посредством радиосигналов считываются или записываются данные, хранящиеся в RFID-метках (карте доступа) работающих на частоте 13,56 МГц. Карта хранит информацию на встроенным микрочипу и памяти.

Внутри карты MIFARE расположены микрочип и индуктивная антенна, которая одновременно служит и для передачи информации, и для питания карты.

Стандартная карта MIFARE запрограммирована с уникальным 32-битным серийным номером. Это случайное число и не содержит код объекта. Доступ к памяти карты защищен. Чтение и запись возможна только при знании ключей доступа, а передаваемые между картой и считывателем данные защищены. Карта MIFARE имеет память для хранения значений.

Карта MIFARE может быть запрограммирована с несколькими учетными данными, что добавляет дополнительное авторизацию между устройством чтения карт и программным обеспечением устройства чтения карт.

Карты доступа MIFARE имеют уязвимости в своей защите. В 2008 году исследовательской группой голландского университета Радбау были опубликованы 3 статьи, касающиеся взлома карт Mifare Classic. Также в ноябре 2010 года группой исследователей в области безопасности из Рурского университета была опубликована статья детально описывающая атаку на карты Mifare DESFire.

1.3. Разработка модели угроз для систем СКУД

Модель угроз строится для информационной системы контроля и управления доступом, имеющей открытый радиочастотный канала связи для получения данных от идентификатора. Выявлено, что информационная система включает в себя считыватель, идентификатор (карта доступа), контроллер доступа, замки. В системе содержатся персональные данные, которые могут хранится как в базе данных контроллера СКУД, так и записаны в карту доступа. Персональные данные служат для определения, кто и когда пытался получить доступ к защищаемой зоне.

Модель угроз построена в соответствии с нормативно-правовыми актами Российской Федерации:

– Федеральный закон РФ от 27.07.2006 года № 152-ФЗ «О персональных данных»;

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

– Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Основу модели угроз составили методические документы Федеральной службы по техническому и экспортному контролю Российской Федерации:

– Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008 год;

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

На первом этапе определена исходная защищенность информационной инфраструктуры, с использованием модели ФСТЭК для информационных систем, которые содержат персональные данные.

Анализ информации о системе позволил выявить показатели исходной защищенности, которые отображены в таблице 1.1.

Таблица 1.1 – Показатели исходной защищенности Технические и эксплуатационные

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
1. По территориальному размещению: локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий;	-	+	-
2. По наличию соединения с сетями общего пользования: ИСПДн, имеющая одноточечный выход в сеть общего пользования;	-	+	-
3. По встроенным (легальным) операциям с записями баз персональных данных: запись, удаление, сортировка;	-	+	-
4. По разграничению доступа к персональным данным: ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн;	-	+	-
5. По наличию соединений с другими базами ПДн иных ИСПДн: ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн	+	-	-
6. По уровню обобщения (обезличивания) ПДн: ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;	-	+	
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн безпредварительной обработки: ИСПДн, не предоставляющая никакой информации.	+	-	-

Согласно таблице 1.1 и методике ФСТЭК сделан вывод, что информационная система имеет средний уровень исходной защищенности, так как не менее 70% характеристик соответствуют уровню не ниже «средний». Показатель исходной защищенности равен Y1=5.

С учетом наличия прав доступа и возможностей по доступу к информации или к компонентам информационной системы для информационной системы персональных данных, имеющей подключение к сетям связи общего пользования по кабельным линиям связи, а также съёмным носителям информации нарушители подразделяются на два типа:

– внешние нарушители – лица, не имеющие права доступа к информационной системе, ее отдельным компонентам и реализующие угрозы безопасности информации из-за границ информационной системы;

– внутренние нарушители – лица, имеющие право постоянного или разового доступа к информационной системе, ее отдельным компонента.

Внутренние нарушители включают в себя сотрудников, администраторов и инженеров информационной системы. Также лицами, относящихся к категории внутренних нарушителей относятся персонал по администрированию программно-аппаратных средств, установке и наладке компонентов СКУД, а также лица имеющие персональные идентификаторы для доступа в защищаемые помещения.

К внешним нарушителям могут быть отнесены бывшие сотрудники организации, внешние субъекты.

Нарушители имеют высокий потенциал, если обладают знанием структуры информационной системы, квалификацией, ресурсами и мотивацией.

Коэффициент вероятности реализации угрозы определяется экспертным путем исходя внешних условий. Коэффициент вероятности реализации (Y2) определяется по 4 градациям:

– маловероятно – отсутствуют объективные предпосылки для осуществления угрозы (Y2=0);

– низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют её реализацию (Y2=2);

– средняя вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры безопасности недостаточны (Y2=5);

– высокая вероятность – объективные предпосылки для реализации угрозы существуют и меры обеспечения безопасности не приняты (Y2=10).

Для выявления возможных угроз безопасности ИСПДн имеющей подключение к сетям связи общего пользования по кабельным линиям связи проанализирован Банк данных угроз ФСТЭК и на основе исходных данных об информационной системе выделены угрозы, отображенные в таблице 1.2.

Таблица 1.2 – Вероятность реализации угроз безопасности

№	Угроза	Коэффициент
1	УБИ .003: Угроза анализа криптографических алгоритмов и их реализации	2
2	УБИ.008: Угроза восстановления и/или повторного использования аутентификационной информации	5
3	УБИ.027: Угроза искажения вводимой и выводимой на периферийные устройства информации	0
4	УБИ.034: Угроза использования слабостей протоколов сетевого/локального обмена данными	5
5	УБИ.073: Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети	5
6	УБИ.074: Угроза несанкционированного доступа к аутентификационной информации	5
7	УБИ.086: Угроза несанкционированного изменения аутентификационной информации	5
8	УБИ.100: Угроза обхода некорректно настроенных механизмов аутентификации	2
9	УБИ.104: Угроза определения топологии вычислительной сети	2
10	УБИ.107: Угроза отключения контрольных датчиков	0
11	УБИ.128: Угроза подмены доверенного пользователя	5
12	УБИ.139: Угроза преодоления физической защиты	0
13	УБИ.152: Угроза удаления аутентификационной информации	5
14	УБИ.156: Угроза утраты носителей информации	5
15	УБИ.160: Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	5
16	УБИ.176: Угроза нарушения технологического и производственного процесса из-за временных задержек, вносимых средством защиты	5
17	УБИ.185: Угроза несанкционированного изменения параметров настройки средств защиты информации	2
18	УБИ.216: Угроза получения несанкционированного доступа к приложениям, установленным на Smart-картах	5

Оценка возможности реализации и опасности угроз.

Опираясь на результаты оценки уровня защищенности (Y1) и вероятности реализации угрозы (Y2), непосредственно определяется коэффициент реализуемости угрозы (Y) и возможность реализации угрозы.

Коэффициент реализуемости угрозы Y определяется соотношением:

$$Y = \frac{(Y_1 + Y_2)}{20} \qquad (1.1)$$

С помощью расчётов по формуле (1.1) коэффициент реализуемости угрозы определяется по следующим диапазонам:

– 0 > Y > 0,3 – низкая возможность реализации угрозы;

– 0,3 > Y > 0,6, то средняя возможность реализации угрозы;

– 0,6 > Y > 0,8, то высокая возможность реализации угрозы;

– Y > 0,8, то очень высокая возможность реализации угрозы.

Так же осуществляется оценка опасности, определяемая с помощью опроса специалистов по показателям опасности с тремя значениями:

– низкая опасность – когда реализация угрозы вероятно приведёт к незначительным негативным последствиям для субъектов персональных данных;

– средняя опасность – когда реализация угрозы вероятно приведёт к негативным последствиям для субъектов, персональных данных;

– высокая опасность – когда реализация угрозы вероятно приведёт к значительным негативным последствиям для субъектов персональных данных.

Таблица 1.3 – Оценка возможности реализации и опасности угроз

№	Угроза безопасности	Коэффициент реализуемости угрозы (Y)	Возможность реализации угрозы	Оценка опасности угрозы
1	УБИ .003: Угроза анализа криптографических алгоритмов и их реализации	0.35	средняя	средняя
2	УБИ.008: Угроза восстановления и/или повторного использования аутентификационной информации	0.5	средняя	высокая
3	УБИ.027: Угроза искажения вводимой и выводимой на периферийные	0.25	низкая	низкая

	устройства информации			
4	УБИ.034: Угроза использования слабостей протоколов сетевого/локального обмена данными	0.5	средняя	высокая
5	УБИ.073: Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети	0.5	средняя	средняя
6	УБИ.074: Угроза несанкционированного доступа к аутентификационной информации	0.5	средняя	высокая
7	УБИ.086: Угроза несанкционированного изменения аутентификационной информации	0.5	средняя	высокая
8	УБИ.100: Угроза обхода некорректно настроенных механизмов аутентификации	0.35	средняя	средняя
9	УБИ.104: Угроза определения топологии вычислительной сети	0.35	средняя	низкая
10	УБИ.107: Угроза отключения контрольных датчиков	0.25	низкая	низкая
11	УБИ.128: Угроза подмены доверенного пользователя	0.5	средняя	высокая
12	УБИ.139: Угроза преодоления физической защиты	0.25	низкая	низкая
13	УБИ.152: Угроза удаления аутентификационной информации	0.5	средняя	высокая
14	УБИ.156: Угроза утраты носителей информации	0.5	средняя	высокая
15	УБИ.160: Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	0.5	средняя	высокая
16	УБИ.176: Угроза нарушения технологического/производственного процесса из-за временны́х задержек, вносимых средством защиты	0.5	средняя	средняя
17	УБИ.185: Угроза несанкционированного изменения параметров настройки средств защиты информации	0.35	средняя	высокая
18	УБИ.216: Угроза получения несанкционированного доступа к приложениям, установленным на Smart-картах	0.5	средняя	средняя

Составим перечень актуальных угроз. Для того, чтобы отнести угрозы к актуальным или неактуальным, необходимо следовать правилам, приведенными в методике определения актуальных угроз безопасности персональных данных при их обработке в информационных системах, утвержденной ФСТЭК России 14.02.2008, отображенных в таблице 1.4.

Таблица 1.4 – Перечень актуальных угроз

Возможность реализации угрозы	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

Характеристики актуальности угроз (ФСТЭК России 14.02.2008).

Таблица 1.5 – Определение актуальности угроз

№	Угроза безопасности	Актуальность угрозы
1	УБИ .003: Угроза анализа криптографических алгоритмов и их реализации	актуальная
2	УБИ.008: Угроза восстановления и/или повторного использования аутентификационной информации	актуальная
3	УБИ.027: Угроза искажения вводимой и выводимой на периферийные устройства информации	неактуальная
4	УБИ.034: Угроза использования слабостей протоколов сетевого/локального обмена данными	актуальная
5	УБИ.073: Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети	актуальная
6	УБИ.074: Угроза несанкционированного доступа к аутентификационной информации	актуальная
7	УБИ.086: Угроза несанкционированного изменения аутентификационной информации	актуальная
8	УБИ.100: Угроза обхода некорректно настроенных механизмов аутентификации	актуальная
9	УБИ.104: Угроза определения топологии вычислительной сети	неактуальная
10	УБИ.107: Угроза отключения контрольных датчиков	неактуальная

Продолжение таблицы 1.5

11	УБИ.128: Угроза подмены доверенного пользователя	актуальная
12	УБИ.139: Угроза преодоления физической защиты	неактуальная
13	УБИ.152: Угроза удаления аутентификационной информации	актуальная
14	УБИ.156: Угроза утраты носителей информации	актуальная
15	УБИ.160: Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	актуальная
16	УБИ.176: Угроза нарушения технологического/производственного процесса из-за временных задержек, вносимых средством защиты	актуальная
17	УБИ.185: Угроза несанкционированного изменения параметров настройки средств защиты информации	актуальная
18	УБИ.216: Угроза получения несанкционированного доступа к приложениям, установленным на Smart-картах	актуальная

Список актуальных угроз:

– угроза анализа криптографических алгоритмов и их реализации;

– угроза восстановления и/или повторного использования аутентификационной информации;

– угроза использования слабостей протоколов сетевого/локального обмена данными;

– угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети;

– угроза несанкционированного доступа к аутентификационной информации;

– угроза несанкционированного изменения аутентификационной информации;

– угроза обхода некорректно настроенных механизмов аутентификации;

– угроза подмены доверенного Пользователя;

– угроза удаления аутентификационной информации;

– угроза утраты носителей информации;

– угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации;

– угроза нарушения технологического/производственного процесса из-за временных задержек, вносимых средством защиты;

– угроза несанкционированного изменения параметров настройки средств защиты информации;

– угроза получения несанкционированного доступа к приложениям, установленным на Smart-картах.

Стоит отметить что, имеется угроза, которая не описана в Банке данных угроз ФСТЭК. Данная угроза заключается в возможности скрытом копировании пассивных идентификаторов (носителя информации), без необходимости кражи носителя информации.

1.4.Анализ существующих способов защиты от актуальных угроз

Меры обеспечения защиты информации от выявленных угроз, принимаемые обладателем информации, должны обеспечивать эффективное и своевременное выявление и блокирование (нейтрализацию) угроз безопасности информации, в результате реализации которых возможно наступление негативных последствий (ущерба).

Меры противодействия актуальным угрозам приведены в таблице 1.6.

Таблица 1.6 – Способы перекрытия угроз

№	Актуальная угроза	Мера противодействия
1	УБИ .003: Угроза анализа криптографических алгоритмов и их реализации	Применять надёжные криптографические алгоритмы с использование рекомендуемой длины ключа шифрования
2	УБИ.008: Угроза восстановления и/или повторного использования аутентификационной информации	Очистка оперативной памяти после успешной авторизации
3	УБИ.034: Угроза использования слабостей протоколов сетевого/локального обмена данными	Настройка служб безопасности , устраняющие уязвимости протоколов
4	УБИ.073: Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети	Регламент, запрещающий доступ к оборудованию.

Продолжение таблицы 1.6

5	УБИ.074: Угроза несанкционированного доступа к аутентификационной информации	Разграничение доступа к базам данных, использование алгоритмов шифрования и очистка оперативной памяти после завершения сеанса
6	УБИ.086: Угроза несанкционированного изменения аутентификационной информации	Разграничение доступа к базам данных и использование алгоритмов шифрования
7	УБИ.100: Угроза обхода некорректно настроенных механизмов аутентификации	Настройка оборудования при котором блокируются неподдерживаемые данные и действия
8	УБИ.128: Угроза подмены доверенного пользователя	Разграничение доступа к базам данных и использование алгоритмов шифрования
9	УБИ.152: Угроза удаления аутентификационной информации	Разграничение доступа к базам данных и использование алгоритмов шифрования ,а также резервирование данных с баз данных
10	УБИ.156: Угроза утраты носителей информации	Шифрование носителей информации, регистрация и контроль наличия всех носителей информации
11	УБИ.160: Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	Шифрование носителей информации, регистрация и контроль наличия всех носителей информации
12	УБИ.176: Угроза нарушения технологического/производственного процесса из-за временных задержек, вносимых средством защиты	Запись в журнал безопасности , информирование администратора о аномальной активности
13	УБИ.185: Угроза несанкционированного изменения параметров настройки средств защиты информации	Разграничение доступа к СЗИ и использование алгоритмов шифрования
14	УБИ.216: Угроза получения несанкционированного доступа к приложениям, установленным на Smart-картах	Защита приложений методами шифрования и защита от нестандартных команд

Для того чтобы устранить угрозу в скрытом съёме информации с карт доступа необходимо организовать защиту карты доступа в виде алгоритма взаимной аутентификации при которой карта доступа не будет передавать данные пока, другая сторона не подтвердит, что является легитимным контроллером.

Рассмотрим другие способы защиты аутентификация.

Многофакторная аутентификация это один из способов позволяющий повысить надёжность аутентификации в системах контроля и управления доступом. В рамках этого метода для успешной аутентификации система будет требовать от 2 и более факторов для идентификации, что существенно затруднит злоумышленнику преодолеть систему контроля и управления доступом.

При этом факторами, с помощью которых можно идентифицировать объект представлены на рисунке 1.2.

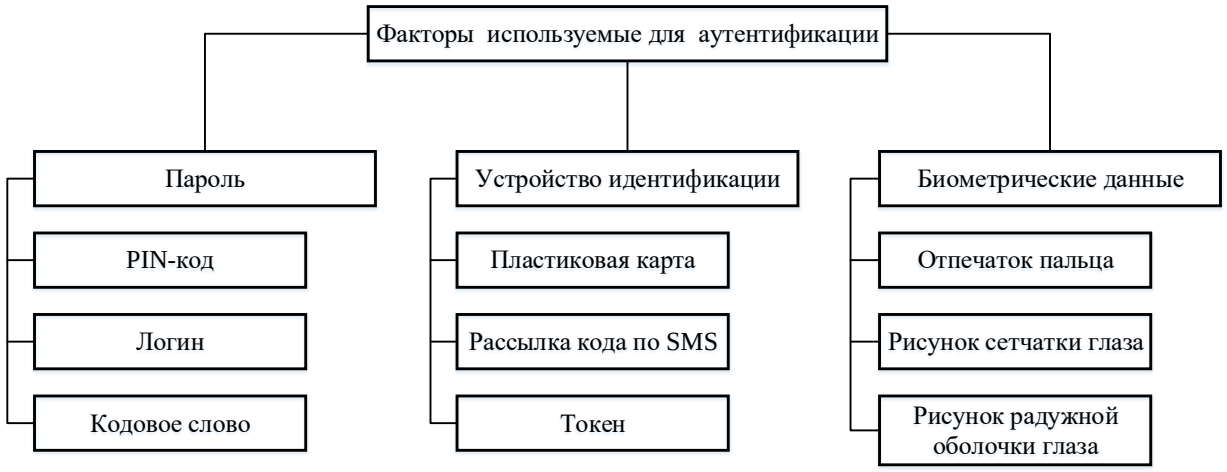

Рисунок 1.2 – Факторы аутентификации

Наиболее распространены системы двухфакторной аутентификации, использующие в своей работе два фактора идентификации личности из трех, приведенных выше.

Методы двухфакторной авторизации повышают безопасность использования бесконтактные карты. Поскольку СКУД, построенные на основе этих методов требуют не только наличия карты, которую можно скомпрометировать, но и введения ПИН-кода (пароля), известного только владельцу карты.

Кроме того, вместо использования пароля можно использовать биометрические методы аутентификации, являющиеся ещё один из возможных способов построения двухфакторной аутентификации. Применение сочетаний двух факторов, распознавание отпечатка пальцев, радужной оболочки глаза или других биометрических данных, а также карты доступа. Сочетание этих факторов также обеспечивает надежную аутентификацию СКУД. Это обуславливается сложность реализации более 2-х факторов аутентификации.

Многофакторная аутентификации также имеет ряд недостатков таких как значительная денежная затрата на дополнительные оборудование для реализации других факторы аутентификации помимо карты доступа, сложность монтажа

таких систем, а также времени, затрачиваемого пользователем для успешной аутентификации.

Помимо многофакторной аутентификации, для обеспечения защищенности карт доступа используют криптографические методы, использующие симметричные блочные алгоритмы шифрования 3DES, AES, где один и тот же ключ используется как для шифрования, так и для дешифровки сообщения, при чем длина ключа фиксированная.

Triple DES (3DES) – симметричный алгоритм блочного шифрования с троекратным шифрованием с 3 различными ключами по 56 бит. Данные при этом разбиваются на блоки фиксированной длины, размер блока равный 64 битам, каждый из которых шифруется отдельно. Triple DES обладает достаточно низкой производительностью.

AES – симметричный алгоритм блочного шифрования с размером блока 128 бит и переменной длины ключа от 128 до 256 бит.

AES имеет хорошую устойчивость к атакам на реализацию, при которых злоумышленник пытается декодировать зашифрованное сообщение, анализируя внешние проявления алгоритма, в том числе уровень энергопотребления и время выполнения. AES можно легко защитить от таких атак, поскольку он опирается в основном на булевы операции. Однако AES имеет недостаток в виду высокой вычислительной нагрузки.

Помимо шифрования и двухфакторной аутентификации существую методы взаимной аутентификации. Данный метод позволяет избежать повторного воспроизведения информации. Это достигается тем что карта доступа вместо простой передачи информации для осуществления аутентификации, предоставляет считывателю, уникальный номер CSN и сгенерированный 16-битный случайный номер.

В ответ контроллер, используя Hash функцию, создает диверсификационный ключ, который должен совпасть с ключом, записанным на карте. Если ключи совпали, карта и контроллер обмениваются 32-битными откликами, после чего контроллер определяет есть ли у карты доступ.

Помимо традиционных способов защиты карт доступа, описанных выше существуют решения, обеспечивающие дополнительный уровень безопасности при передаче данных от идентификатора к считывателю.

Примером такого решения может служить технология Secure Identity Object (SIO), обеспечивающая многоуровневую защиту данных и представляет собой электронный контейнер для хранения данных в любом из форматов карт.

Данная технология построена на принципе кодирования карты с привязкой к уникальному идентификатору носителя UID с последующим заверением записанной информации электронной подписью. Присвоение UID и наличие электронной подписи исключают возможность копирования информации и взлома защиты карты. SIO может применяться на любых картах доступа, в том числе на смарт-картах и мобильных устройствах.

1.5. Выводы

В ходе анализа существующих методов организации системы контроля и управления доступом были рассмотрены технологий RFID и бесконтактные карты доступа Proximity, MIFARE, а также контактная система Dallas touch memory.

Замечено, что большинство систем уязвимы к атакам на копирование ключа (смарт-карты), но в свою очередь их можно защитить с помощью криптографических алгоритмов, которые могут обеспечить защиту от неправомерного копирование карты доступа, но основные алгоритмы, используемые для защиты карт доступа такие как 3DES и AES, имеют недостатки в виде оказываемой нагрузки при шифровании.

Рассмотрен метод двухфакторной аутентификации, который обеспечит надёжность системы контроля и управление доступом, но сложность монтажа и большие денежные затраты для организации дополнительного метода аутентификации таких как ввод PIN-кода или биометрические методы аутентификации является недостатком таких систем. Так же процесс идентификации станет более сложным и продолжительным по сравнению с

обычной системой контроля и управление доступом с использование карт или ключей доступа.

Ещё одним способом защиты карты доступа от неправомерного копирования является метод взаимной аутентификации. При взаимной аутентификации карта доступа прежде чем передать данные для аутентификации, должна удостоверится что контроллер является легитимным. Взаимная аутентификация достигается наличием общего секрета между картой и контролером, который передается по открытому канала в защищенном виде.

На основе изученных данных предлагается разработать алгоритм взаимной аутентификации в системе управления и контроля доступом на основе физически не клонируемых функциях статической ОЗУ, этот метод не потребует больших денежных затрат по сколько контроллер СКУД будет обладать данными об уникальной структуре статической оперативной памяти карты доступа, которую можно будет легко сканировать, но крайне сложно воспроизвести. Такой метод позволит избавится от необходимости использовать симметричные блочные шифры в качестве защиты данных для аутентификации, а также применения сложной и затратной в установке двухфакторной аутентификации.

2. Анализ свойств физически неклонируемых функций СОЗУ и определение оптимальной длины вектора инициализации алгоритма взаимной аутентификации на основе ФНФ

2.1. Анализ основных физически не клонируемых функций в рамках разработки алгоритма взаимной аутентификации на основе ФНФ

Физически неклонируемая функция (Physical Unclonable Function,PUF) – это функция, воплощённая в физической структуре, которую просто оценить, но трудно охарактеризовать, смоделировать или воспроизвести. Физическая структура, содержащая PUF, состоит из множества случайных компонентов. Эти случайные компоненты вводятся в ходе производственного процесса и неконтролируемы. Ввиду этого система на основе PUF, при воздействии на неё порождает уникальный, но непредсказуемый ответ. PUF во многом схож с хеш-функцией, и так же является необратимой функцией.

PUF обладают свойством неклонируемости благодаря тому, что каждый PUF имеет уникальный и непредсказуемый ответ. Два PUFa, созданные в результате одних и тех же производственных процессов, будут обладать разным поведением.

PUF обладает двумя важными свойствами такими как, практически невозможным воссозданием физическую копию PUF и невозможности создания точной математической модели PUF, то есть вычисления отклик, при наличии точных данных о параметрах запроса и другие пары запросов-откликов. Эти качества вместе и называются неклонируемостью.

В PUF могут использоваться различные источники физической случайности. Различают PUF, в которых произвольность вносится внешними факторами и те, в которых она присуще, внутренним факторам физической системы.

Существуют различные виды PUF такие как: оптический PUF, PUF покрытия, кремниевые PUF, магнитные PUF, PUF статической оперативной памяти.

Оптический PUF состоит из прозрачного материала, в котором содержатся случайно распределённые светоотражающие частицы. Когда лазерный пучок освещает материал создаётся случайная интерференционная картина, которая образуется при взаимной интерференции когерентных волн, имеющих случайные сдвиги фаз и/или случайный набор интенсивностей. Данная картина является функцией внутренней структуры PUF, длины волны лазера, угла падения луча.

PUF покрытия может быть создан на верхнем слое интегральных микросхем. Полученные в процессе массового изготовления микросхемы отличаются неповторяющимся набором электрических характеристик, что может быть использовано в системах безопасности как гарантированно не поддающийся копированию идентификационный признак.

Кремниевые PUF используют случайные вариации задержек в проводниках и затворах полевых транзисторов. Устанавливаются условия гонки в электрической цепи и два переключения распространяются по различным путям и выясняется, какой из них придет первым. Арбитр, обычно реализованный как триггер, дает 1 или 0 в зависимости от того, какой переход завершится первым. Когда схему по одинаковым маскам производят на разных чипах, логические функции, реализуемые в электрических цепях, различаются у каждого чипа из-за случайной вариации задержек.

Магнитные PUF существуют на картах с магнитной полосой. Физическая структура магнитного носителя, используемого в картах, производится путём смешения миллиардов частиц феррита бария в пасту в процессе производства. Частицы имеют различную форму и размер. Затем паста наносится на принимающий слой. Частицы ложатся случайным образом. Заставить частицы лечь точно также во второй раз физически невозможно из-за неточности процесса, огромного числа частиц и случайной геометрии частиц.

PUF статической оперативной памяти (SRAM) полагается на отклонения, которые неизбежно существуют для материалов, используемых при изготовлении аппаратуры. Они производят для данного входа – выход, который будет отличным для разных образцов данного оборудования, таким образом, препятствуя созданию точной копии данного продукта. Эти PUF представлены на всех интегральных схемах, имеющих статическую память. Они позволяют создавать идентификатор, который является свойством данной микросхемы, а не хранить его в цифровом виде.

Идентификатор строится на основе состояния памяти в результате включения питания и/или сброса состояния статических запоминающих устройств (SRAM) значение, изначально хранимое в каждом из элементов памяти (0 или 1), является уникальным и случайным. Запросом в данной PUF является включение/выключение питания, а ответом – наблюдаемое состояние каждого из элементов памяти, которое уникально характеризует интегральную схему, на которой PUF реализована.

Из всех описанных выше физически не клонируемых функций для организации работы алгоритма взаимной аутентификации более приемлемым является PUF на основе СОЗУ, ввиду возможности внедрения её в карту доступа, а также из-за высокой скорости запроса и отклика.

2.2. Исследование статистического распределения значений физически не клонируемых функций на основе СОЗУ

В ходе исследования СОЗУ было замечено, что только для части ячеек СОЗУ их состояние после включения питающего напряжения является действительно случайным и зачастую приближается к равномерному распределению. Остальные ячейки устойчиво принимают значение состояния 0 или 1. Из этого следует, что количество случайных значений ячеек СОЗУ при включении питания является ограниченным, а также следует, что в СОЗУ имеются стабильные ячеек.

В ходе исследования статистического распределения значений ячеек СОЗУ, были использованы в качестве исследуемых образцов семь микросхем статической оперативной памяти HM62256 от разных производителей. Схема экспериментальной установки представлена на рисунке 2.1.

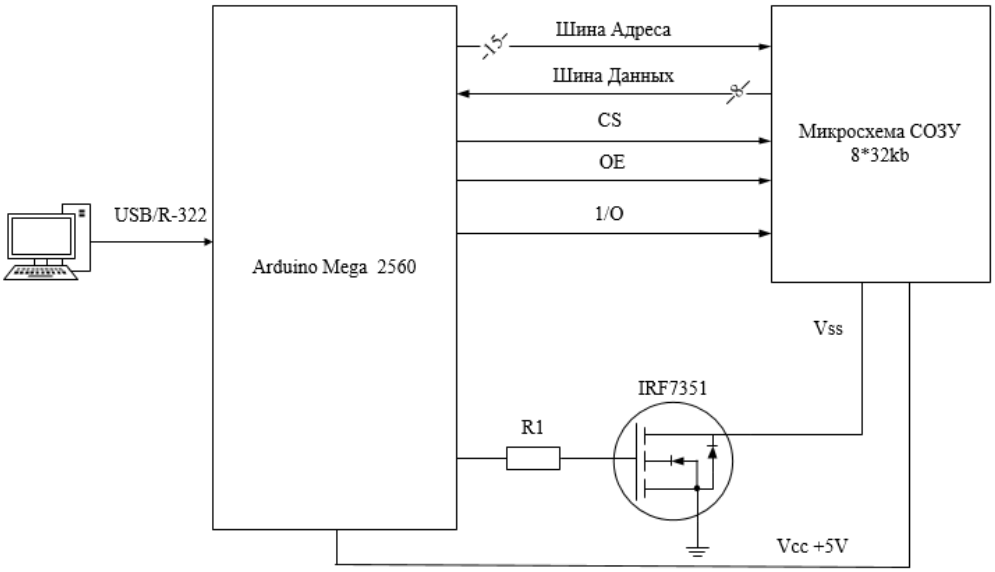

Рисунок 2.1 – Схема экспериментальной установки

Она состоит из универсального модуля Arduino Mega на базе процессора Atmel 2560, микросхем статического ОЗУ, быстросъемной панели для микросхем памяти, транзисторного ключа для управления электропитанием устройства. Опрос каждой микросхемы памяти выполнялся 100 раз через 100 мс после включения электропитания.

Для реализации алгоритма взаимной аутентификации на основе статической ОЗУ будет формироваться вектор инициализации, содержащий помимо случайных ячеек, также стабильные ячеек, которые необходимы для аутентификации. Для вектора инициализации и ключевой информации отсутствие стабильных ячеек приведет к невозможности их использования такой СОЗУ.

В криптографических алгоритмах под вектором инициализации понимают – блок некоторых данных, необходимый для начала шифрования в некоторых режимах блочных шифров. В алгоритме взаимной аутентификации под вектором инициализации понимается блок некоторых данных, необходимый для начала вычисления общего секрета.

Стабильные ячейки – ячейки памяти, которые в ходе включения и выключения электропитания сохраняют одно и тоже значения.

Таким образом, для реализации алгоритма возникает ряд задач, направленных на уменьшение предсказуемости вектора инициализации, а также определение минимальной длины вектора инициализации для надежного обнаружения смещения вектора инициализации в образе памяти.

В ходе исследования были построены карты распределения значений в ячейках памяти для 100 измерений. Продемонстрированы карты наиболее характерных образцов № 1, № 2 и № 6, представленных на рисунках 2.2 – 2.4.

По оси абсцисс отложены адреса ячеек, по оси ординат – номер измерения. Цветом на каждой карте показано значение в ячейке памяти в диапазоне от 0 до 255. Сплошные вертикальные линии на рисунках указывают на стабильные значения, цвет указывает на значение в данной ячейке. Прерывистые вертикальные линии характеризуют нестабильные ячейки.

Псевдослучайное чередование сплошных и прерывистых линий, а также разный цвет сплошных линий является важной характеристикой идеальной физически неклонируемой функции, предлагаемой к использованию в устройстве взаимной аутентификации.

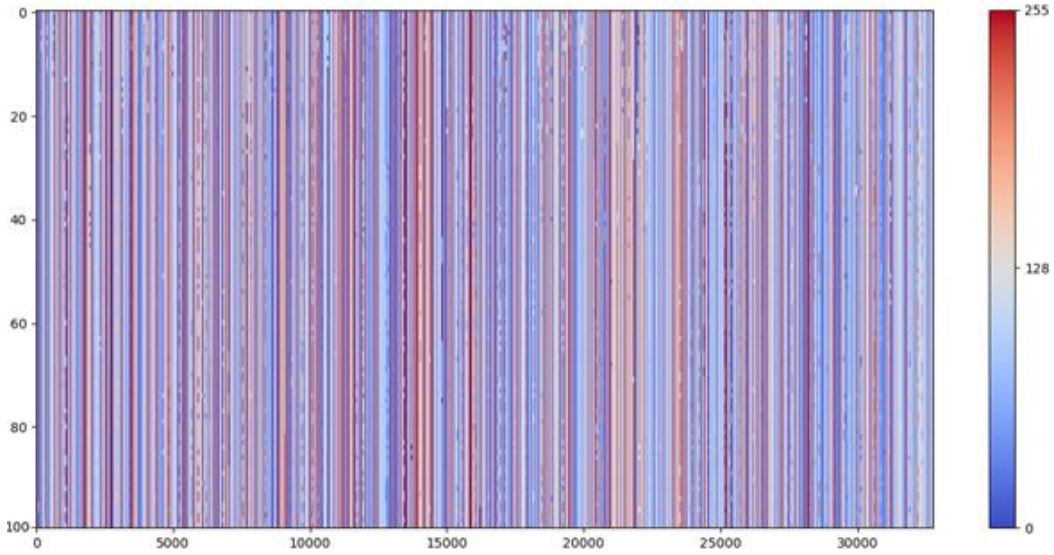

Рисунок 2.2 – Карта распределения значений в ячейках памяти образца СОЗУ № 1 для 100 измерений

Образец СОЗУ № 1 показал достаточно случайное распределение значений в ячейках, а также наличие в СОЗУ стабильных ячеек.

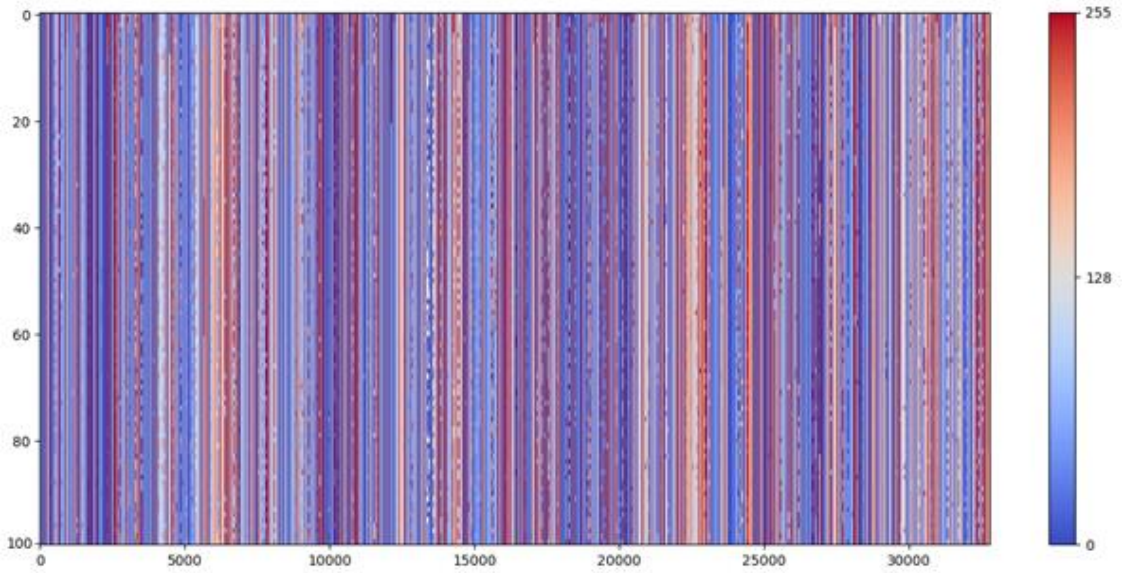

Рисунок 2.3 – Карта распределения значений в ячейках памяти образца СОЗУ № 2 для 100 измерений

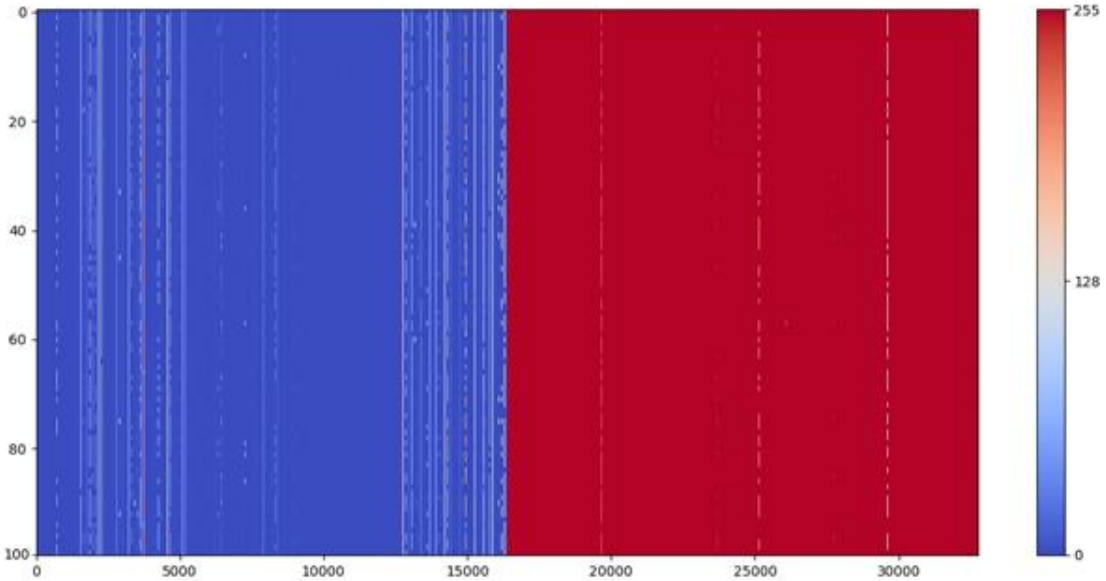

Рисунок 2.4 – Карта распределения значений в ячейках памяти образца СОЗУ № 6 для 100 измерений

В образце СОЗУ № 2 распределение значений в ячейках хуже, чем в образце СОЗУ № 1, наблюдаются периодически повторяющиеся области с преобладанием

нулевых и единичных значений, но при это значения в ячейках достаточно случайно распределены. Также в образце СОЗУ № 2 имеются стабильные ячейки.

В образце СОЗУ № 6 имеют две выраженные области преобладания значений «0» и «255». А также значительное преобладание стабильных ячеек над случайными ячейками, что увеличивает предсказуемость вектора инициализации.

Другие образцы имеют схожую картину с представленными картам. Образцы СОЗУ № 3 и № 4 имеют схожую картину с образцом СОЗУ № 2, а образцы СОЗУ № 5 и № 7 имеют схожую картину с образцом СОЗУ № 6.

2.3. Определение оптимальной длины вектора инициализации для алгоритма взаимной аутентификации на основе СОЗУ

В ходе определения оптимальной длины вектора инициализации были рассмотрены ячейки памяти образцов СОЗУ с семи микросхем. Были сняты 100 снимков значений ячеек памяти по 32 кбайт с 7 образцов СОЗУ. Было определено количество стабильных ячеек, максимальное расстояние между стабильными ячейками, а также какие значения и их количество из диапазона от 0 до 255 принимали стабильные ячейки.

Максимальное расстояние между стабильными ячейками – наибольшее количество нестабильных ячеей между двумя стабильными.

В ходе исследования было замечено что количество стабильных ячеек на разных СОЗУ сильно различаются, как и распределение значений в этих ячейках. Также замечено, что чем больше стабильных ячеек к общему количество ячеек, тем больше длина вектора инициализации необходимого для однозначного совпадения вектора инициализации и образа СОЗУ, на основе которого был построен вектор инициализации. Это связано с тем что чем больше стабильных ячеек, тем выше плотность распределения стабильных ячеек.

На рисунке 2.5 представлено количество стабильных ячеек на разных СОЗУ.

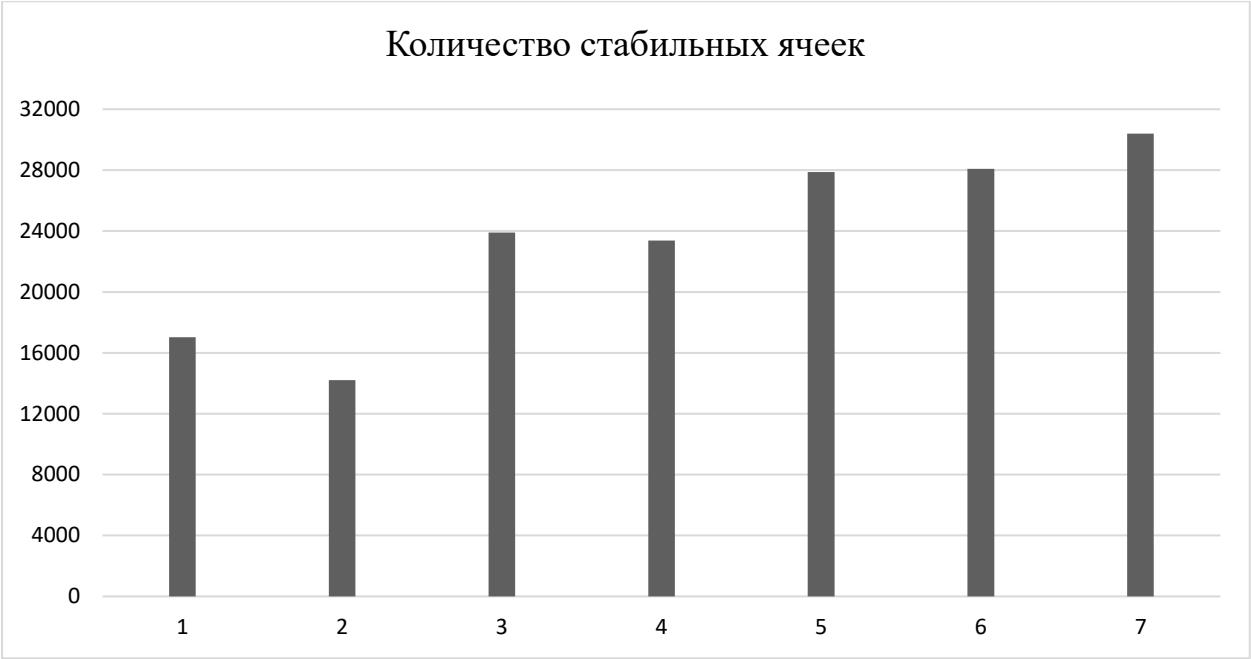

Рисунок 2.5 – Количество стабильных ячеек на разных СОЗУ

Исследовано количество уникальных значений из диапазона от 0 до 255 которые принимают стабильные ячейки памяти. На рисунке 2.6 представлено количество уникальных значений, которые принимали стабильные ячейки памяти разных СОЗУ.

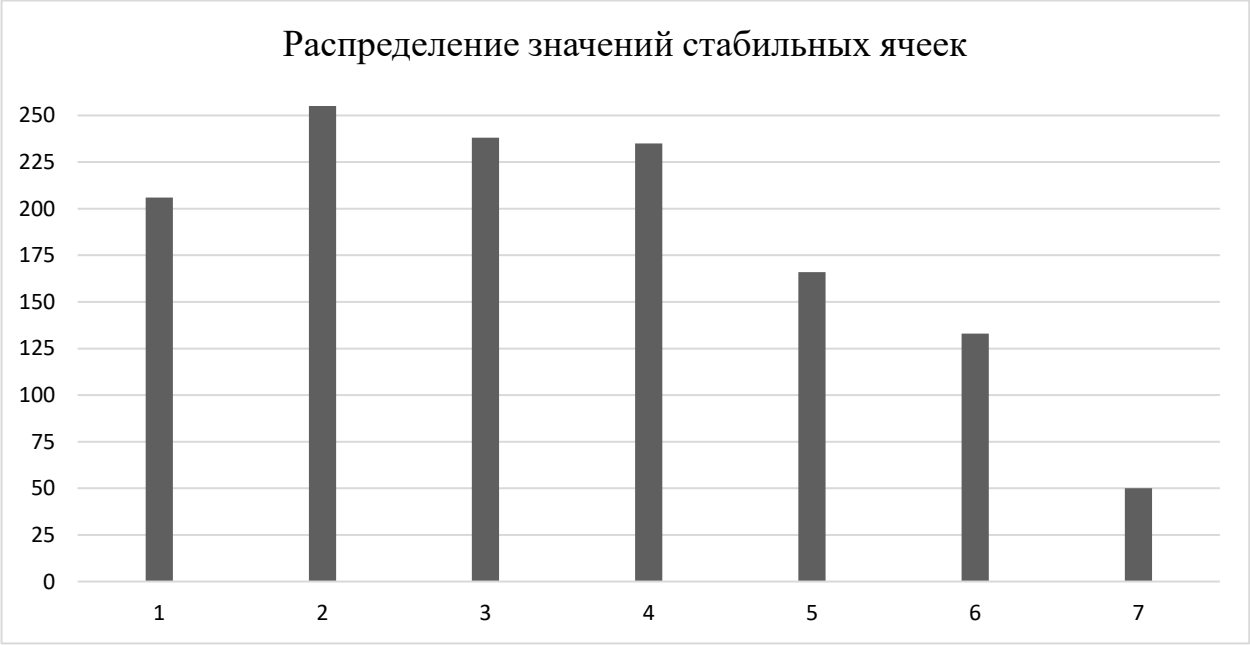

Рисунок 2.6 – Количество уникальных значений, которые принимали стабильные ячейки памяти разных СОЗУ

Было установлено, что чем меньше уникальных значений принимают стабильные ячейки, тем больше длина вектора инициализации необходимого для однозначного совпадения вектора инициализации и фрагмента образа СОЗУ, на основе которого был построен вектор инициализации.

Далее рассмотрена частота повторяемости значений среди стабильных ячеек разных образцов СОЗУ. В рассмотренных СОЗУ наблюдается, что из 7 образцов все кроме 1 имели резкое преобладания одного или двух значений в стабильных ячейках. Частота повторяемости значений, представлены на рисунках 2.7-2.13.

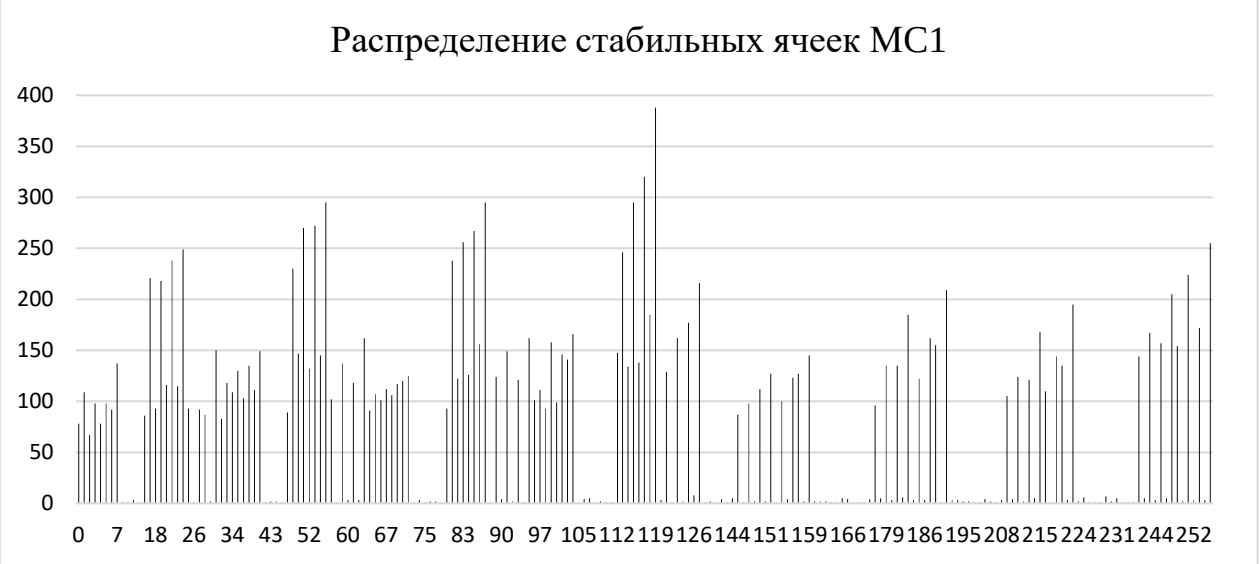

Рисунок 2.7 – Частота повторяемости значений стабильных ячеек микросхемы № 1

Распределение значений в стабильных ячейках у образца 1 достаточно равномерное, что благоприятно влияет на длину векторе инициализации, поскольку вероятность появления уникальных комбинаций ячеек становится выше. Также у данного образца стабильные ячейки принимают 206 значений из 256 возможных, что также благоприятно влияет на длину вектора инициализации. Данный образец СОЗУ показал наилучший показатель длины вектора инициализации из рассмотренных образцов.

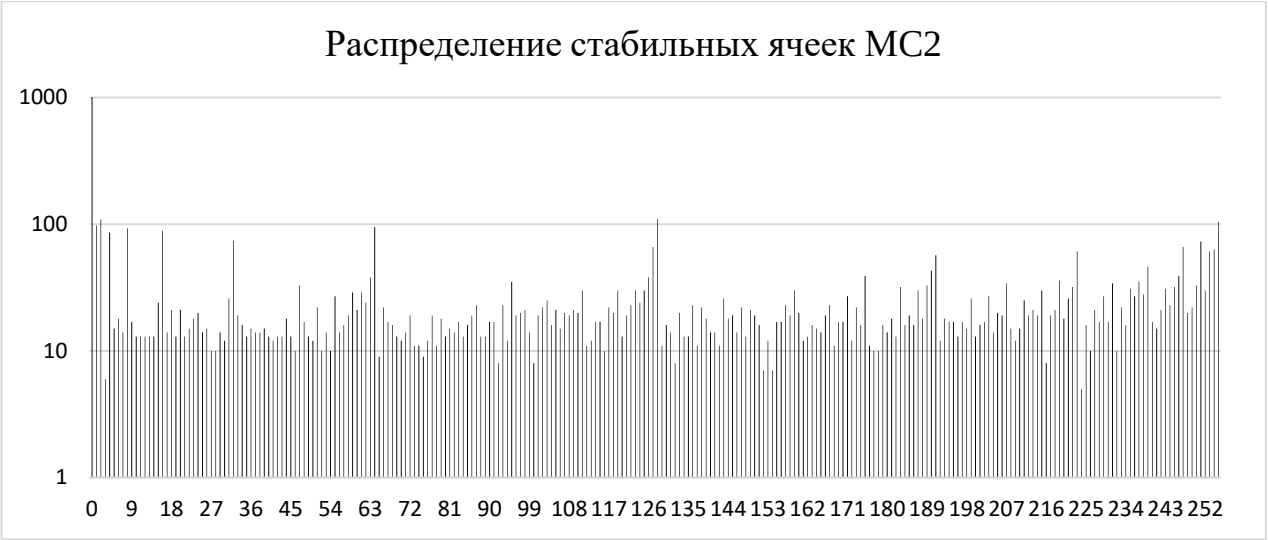

Рисунок 2.8 – Частота повторяемости значений стабильных ячеек микросхемы № 2

У образца 2 наблюдается преобладания значения 0 в стабильных ячейках, что негативно влияет на вектор инициализации. Но распределение оставшихся значений компенсирует преобладание 0 в стабильных ячейках.

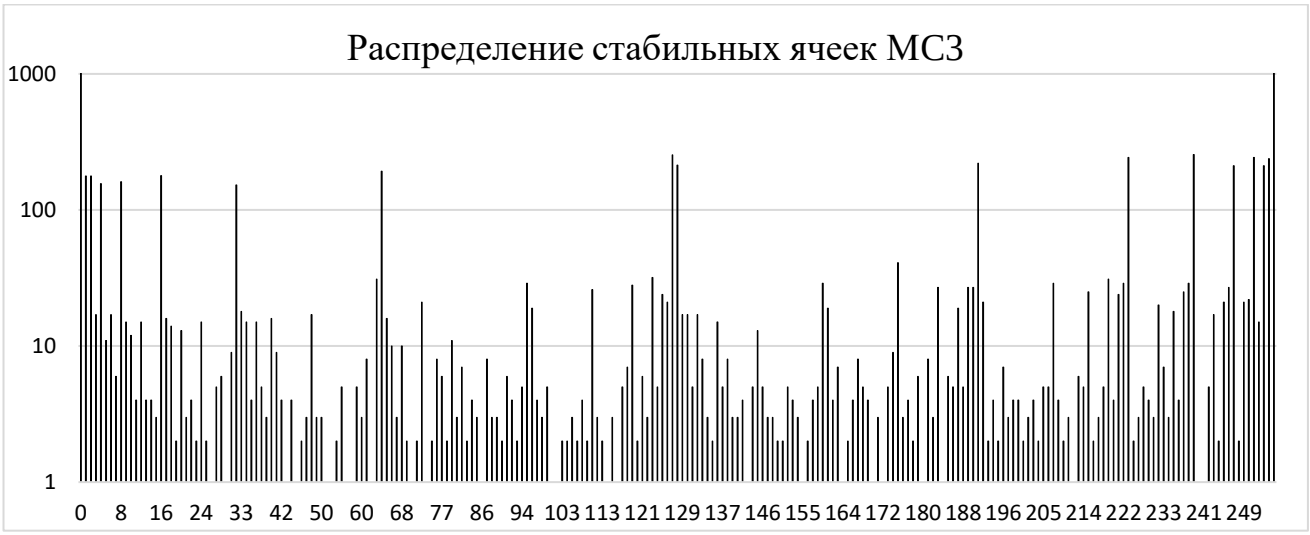

Рисунок 2.9 – Частота повторяемости значений стабильных ячеек микросхемы № 3

У образца № 3 наблюдается преобладания двух значений 0 и 255, что более негативно влияет на вектор, чем преобладание 1 значения, как у образца № 2.

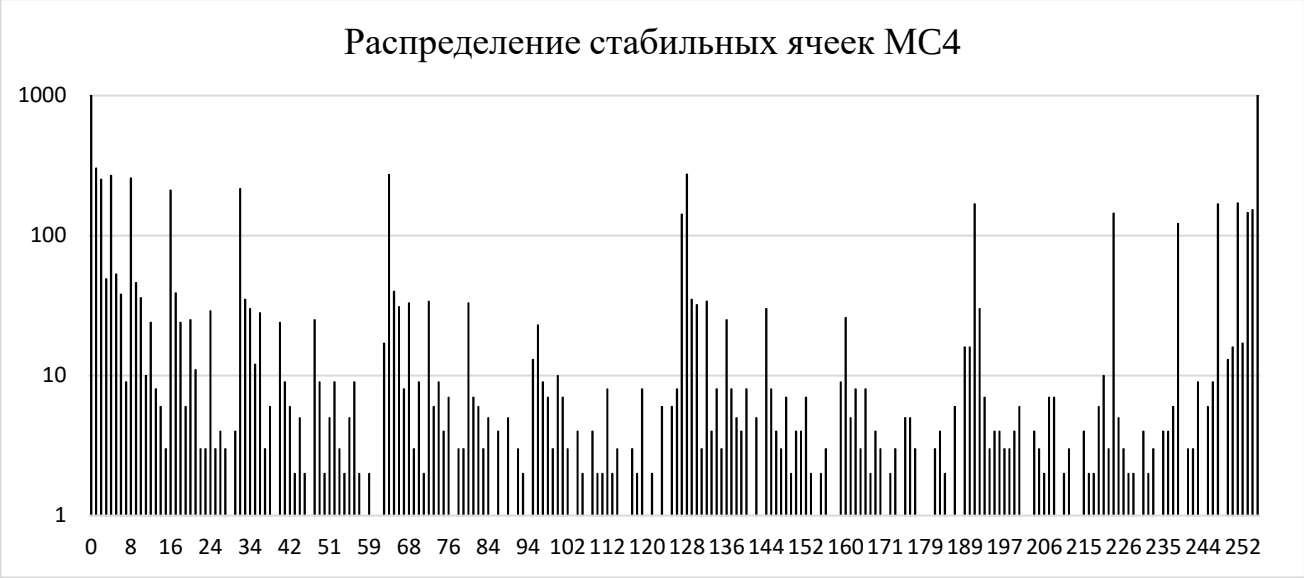

Рисунок 2.10 – Частота повторяемости значений стабильных ячеек микросхемы № 4

У образца № 4 наблюдается также, как и у образца № 3 преобладания значений 0 и 255 среди стабильных ячеек. Но оба образца имеют достаточно хорошее распределение значений.

Рисунок 2.11 – Частота повторяемости значений стабильных ячеек микросхемы № 5

У образца № 5 наблюдается значительное преобладания значений 0 и 255 при снижении общего количества значений, принимаемых стабильными ячейками. Вследствие чего наблюдается более стремительное увеличение длины

вектора инициализации, необходимой для однозначного совпадения с образом СОЗУ, чему у образцов 3 и 4.

Рисунок 2.12 – Частота повторяемости значений стабильных ячеек микросхемы № 6

У образца № 6, как и у образца № 5 наблюдается схожая картина с распределением значений стабильных ячейках и числом уникальных значений принимаемыми стабильными ячейками.

Рисунок 2.13 – Частота повторяемости значений стабильных ячеек микросхемы № 7

У образца № 7 наблюдается значительное преобладания значений 0 и 255 и самое маленькое число уникальных значений, принимаемых стабильными ячейками среди всех образцов. Вследствие чего данная СОЗУ имеет самую большую длину вектора инициализации.

На основе полученных данных составлена таблица 2.1, где можно увидеть, как различные параметры стабильных ячеей влияют на длину вектора инициализации.

Таблица 2.1 – Данные исследования стабильных ячеек

	МС 1	МС 2	МС 3	МС 4	МС 5	МС 6	МС 7
Количество стабильных ячеей	17016	14205	23896	23374	27883	28089	30389
Максимальное расстояние между стабильными ячейками	15	26	9	8	7	6	4
Количество значений принимаемых из диапазона 0-255 в стабильных ячейках	206	255	238	235	166	133	50
Стабильный вектор инициализации	28	58	90	60	412	186	1040

Из таблицы 2.1 видно, что наименьшую длину вектора инициализации имеет микросхема № 1, а наибольшую микросхема № 7.

Вектор инициализации микросхемы № 7 имеет длину 3,17% от общего количества ячеек, из чего следует что это негативно сказывается на эффективности и безопасности алгоритма аутентификации.

2.4. Выводы

В ходе анализа данных по стабильным ячейкам 7 различных микросхем замечено, что чем больше соотношение стабильных ячеек к общему числу ячеек, тем больше длина вектора инициализации необходимого для однозначного определения в ходе сравнения.

Так же видно, что чем меньше уникальных значений из диапазона от 0 до 255 принимают стабильные ячейки тем больше длина вектора инициализации необходимого для однозначного определения в ходе сравнения.

Так же влияние на длину вектора инициализации оказывает максимальное расстояние между стабильными ячейками, длина вектора не может быть меньше этого числа, а также чем меньше длина максимального расстояния между стабильными ячейками, тем меньше среднее расстояние между стабильными ячейками, а значит более плотно расположены стабильных ячеей что в месте с неравномерным распределением значений ячеек ,где может преобладать одно значения повышает вероятность встречи одинаковых комбинаций стабильных ячеек. Из-за чего для однозначного совпадения значения необходимо увеличить длину вектора инициализации.

В ходе исследования было замечено что наиболее равномерным распределением значений среди стабильных ячеек показала образец № 1, где нет сильного преобладания отдельных значений, а вместе с этим образец № 1 имеет 52 % стабильных ячеек от общего числа ячеек, при задействованных 206 уникальных значениях из 256. При этих параметрах эта микросхема имеет наименьшую оптимальную длину вектора инициализации равную 28 ячейкам.

Образцы № 2 показали размер оптимального вектора инициализации ~ 2 раза больше чем образец № 1. Это связано с тем, что образец № 2 при задействовании всех 256 значений в стабильных ячейках, обладал максимальным расстояния между стабильными ячейками равным 26 и чётко выраженно преобладание значение 0, что составило 59 % от общего количества стабильных ячеек. Из-за чего оптимальная длина вектора инициализации возросла до 58 ячеек.

Образец № 4 также показал показали размер оптимального вектора инициализации ~ 2 раза больше чем образец № 1. Это связано с тем, что при задействовании 235 значений из 256 в стабильных ячейках, было чётко выраженно преобладание значений 0 и 255, где встречаемость 0 составила 53%, а

встречаемость 255 составила 25%, из-за чего длина оптимального вектора инициализации возросла до 60 ячеек.

Образец № 3 показал результат оптимальной длины вектора хуже, чем рассмотренные ранее образцы, где при схожих параметрах с образцом № 4, но с увеличением повторяемости значения 0 до 61% вектор инициализации вырос до 90 ячеек.

С плохими характеристиками представлены образцы № 5–7, где при увели общего числа стабильных ячеек и уменьшении максимального расстояния между стабильными ячейка, распределение значений было неравномерно. Среди значений стабильных ячеек значительно преобладали значений 0 и 255, и при это количество значений, задействованных из 256, составило для образца № 5 – 166 значений, для образца № 6 – 133 значений и для образца № 7 – 50 значений. Вследствие чего резко увеличилась оптимальная длина вектора инициализации, где для образца № 6 необходимо 186 ячеек, для образца № 5 необходимо 412 ячеек и для образца № 7 необходимо 1040 ячеек.

На основе этого можно сделать вывод что не каждая микросхема может применятся в устройствах аутентификации СКУД на основе статического ОЗУ, поскольку повлиять на параметры СОЗУ не представляется возможным ввиду конструкторских особенностей и определенных условий окружающей среды.

Большой процент повторений одного или нескольких значений, а также высокая плотность значений ведет к повышению вероятности появлений одинаковых комбинаций стабильных ячеек, что влечет в свою очередь увеличение длины вектора инициализации и увеличению количества информации, предаваемого по открытому каналу. В свою очередь это приведет к увеличению вероятности компрометации карт доступа на основе статического ОЗУ.

3. Разработка алгоритмов исследования статической ОЗУ и взаимной аутентификации на основе свойств физически неклонируемых функций СОЗУ

3.1. Разработка алгоритма исследования статической ОЗУ для определения длины вектора инициализации

В ходе исследования оптимальной длины вектора инициализации было выявлено, что не каждая СОЗУ имеет подходящие параметры для использования в качестве ФНФ для алгоритма взаимной аутентификации. Это об условлено тем, что у некоторых СОЗУ среди стабильных ячеек в значительной степени преобладают одно или несколько значений из 256 возможны. Вследствие чего необходимо проводить исследование каждой СОЗУ, что бы выявить следующие аспекты:

- подходит ли СОЗУ в качестве ФНФ, то есть отсутствие большого преобладания определенных значений;
- определить количество стабильных ячеек и их позицию;
- определить максимально расстояние между стабильными ячейками;
- определить оптимальную длину вектора инициализации.

Для проведения исследования необходимо записать результат опросов микросхемы памяти, выполненных 100 раз через 100 мс после включения электропитания.

Следующим этапом необходимо сравнить каждую ячейку памяти с значением в других ста опросах. По результатам сравнений ячейки, которые принимали одно и тоже значение во всех ста опросах является стабильными. Далее строится матрица стабильных значений, для этого значения всех ячеек последовательно записываются и индексируется номером ячейки. Ячейкам, которое не являются стабильными, присваивается значение 0, а индекс обнуляется. В случае если значение стабильной ячейки будет 0, то наличие не 0 индекса будет говорить, что это стабильная ячейка. Полученная матрица будет

является образом стабильных ячеек необходимой для дальнейшего исследования СОЗУ и работы алгоритма взаимной аутентификации.

В матрице необходимо определить максимальное расстояние между стабильными ячейками (R) – наибольшее количество нестабильных ячеей между двумя стабильными, в дальнейшем пустая область. Данный параметр показывает меньше какого значения не может быть длина вектор инициализации. Исходя из возможности того, что при формировании вектора инициализации, будет выбрана пустая область, где количество стабильных ячеек будет минимально, поэтому минимальная длина вектора будет определятся, как $L=2^1 \times R$, где R – максимальное расстояние между стабильными ячейками.

Поскольку стабильные ячейки перемещены с нестабильными ячейками, а вектор инициализации будет формироваться по случайному фрагменту памяти, то минимальная длина равная $L=2^1 \times R$, может быть недостаточной. Поэтому для определения оптимальной длины вектора инициализации необходимо выполнить алгоритмы поиска и проверки длины вектора.

Алгоритм поиска длины происходит в 2 этапа. Первый этап поиска приемлемой длины вектора инициализации заключается в поиске верхнего граничного значения по формуле $L=2^n \times R$,где R– максимальное расстояние между стабильными ячейками , а n – номер текущей итерации. Начиная с первой итерации и до тех пор, пока проверка не будет завершена успешно значение n будет увеличивается на единицу, вследствие чего будет увеличиваться значение верхнего граничного значения. В случае успешной проверки, верхнее граничное значение не будет увеличиваться, а, следовательно, Длина последней итерации будет является верхним граничным значением. Длина предпоследней итерации станет нижним граничным значением, на этом первый этап завершается. На втором этапе в качестве оптимальной длины будет приниматься среднее арифметическое между верхним граничным значением и нижним граничным значением. В случае если средне арифметическое представляет собой десятичную дробь, то дробная часть отбрасывается, а целя часть увеличивается на единицу.

Данное значение длины также будет проверено, и в случае успешной проверки станет верхним граничным значением, а в случае неудачной проверки станет нижним граничным значением. Второй этап будет повторятся до тех пор, пока верхнее и нижнее граничные значение не примкнут друг к другу, то есть разница между ними не будет превышать 1. И получившееся значение верхней границы будет оптимальной длиной вектора инициализации.

Алгоритм проверки длины вектора инициализации состоит из 2-х циклов. Первый цикл будет формировать векторы инициализации заданной длины из образа памяти СОЗУ поставив указатель начиная с 1 ячейки памяти. Сформировав вектор, будет вызваться 2 цикл проверки, по завершении которого в случае успешной проверки указатель 1 цикла сдвинется вперед на 1 позицию и последовательность действий повторится вновь до тех пор, пока указатель не дойдет до позиции ячейки образа памяти СОЗУ равной 32768-L, где L–длина проверяемого вектора, или неудачного завершения цикла проверки.

Второй цикл проверки будет вызывается для сравнение полученного вектора с матрицей стабильных ячеек. Поставив указатель начиная с 1 ячейки матрицы будет формироваться фрагментом матрицы равным по величине вектор инициализации. Затем у фрагмента будет вычислено количество стабильных ячеек и вектор будет сравниваться с фрагментом матрицы. Если в результате сравнения количество совпадений фрагмента и вектора равно количеству стабильных ячеей, то фиксируется совпадение, и указатель в матрице сдвигается на 1 позицию вперед. Если совпадений не было выявлено, то указатель в матрице так же сдвигается на 1 позицию вперед. Данный цикл будет повторятся пока указатель не достигнет, позиции ячейки равной 32768-L ячейки, где L-длина проверяемого вектора. В конце каждого прохода будет вывялятся минимум 1 совпадение. Если в ходе прохода цикла будет выявлено больше одного совпадения, то проверка признается неудачной и длина считается не подходящей. Проверка считается успешной если в ходе каждого из 32768-L прохода было выявлено по 1 совпадению вектора и матрицы.

Блок-схема алгоритма поиска длины вектора представлена на рисунке 3.1.

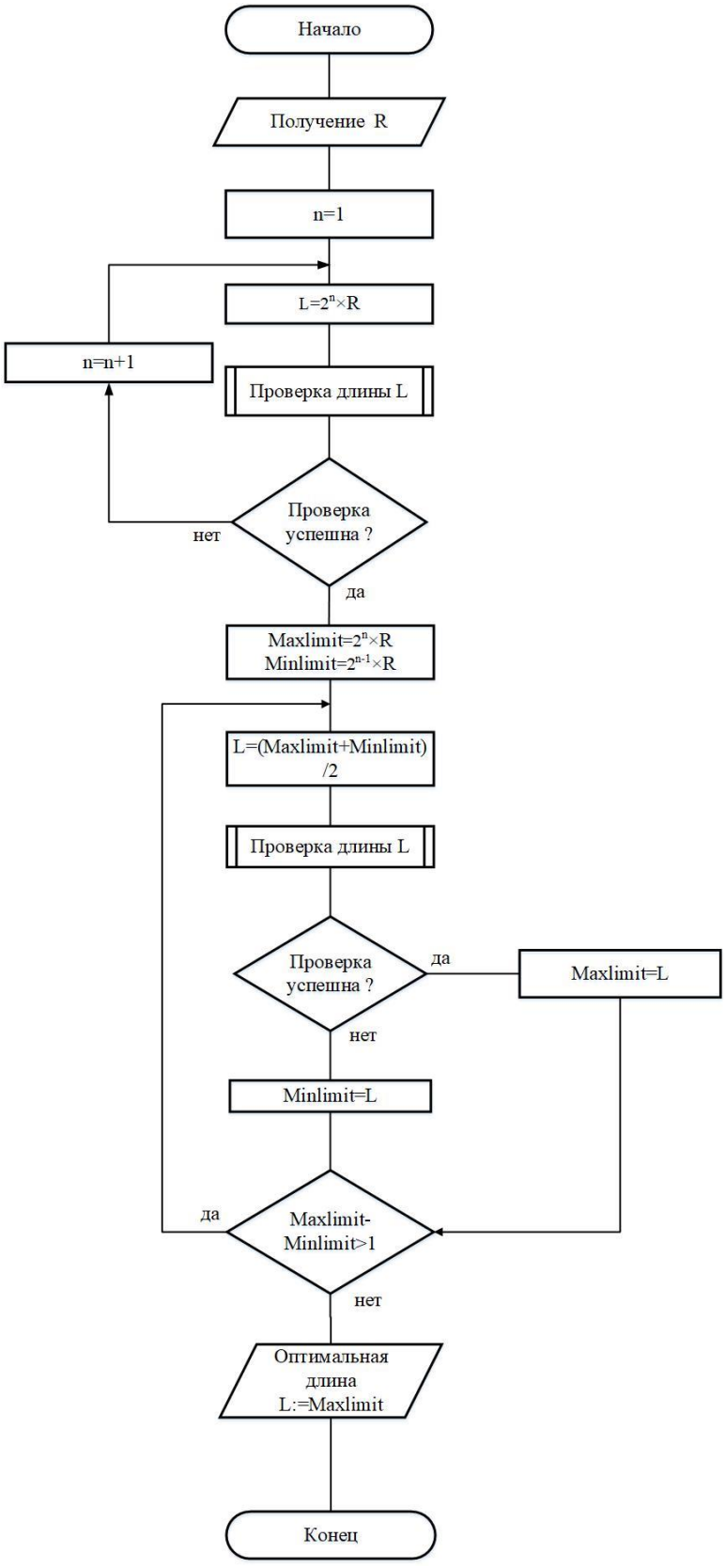

Рисунок 3.1 – Блок-схема алгоритма поиска длины вектора

Блок-схема алгоритма проверки длины вектора представлена на рисунке 3.2.

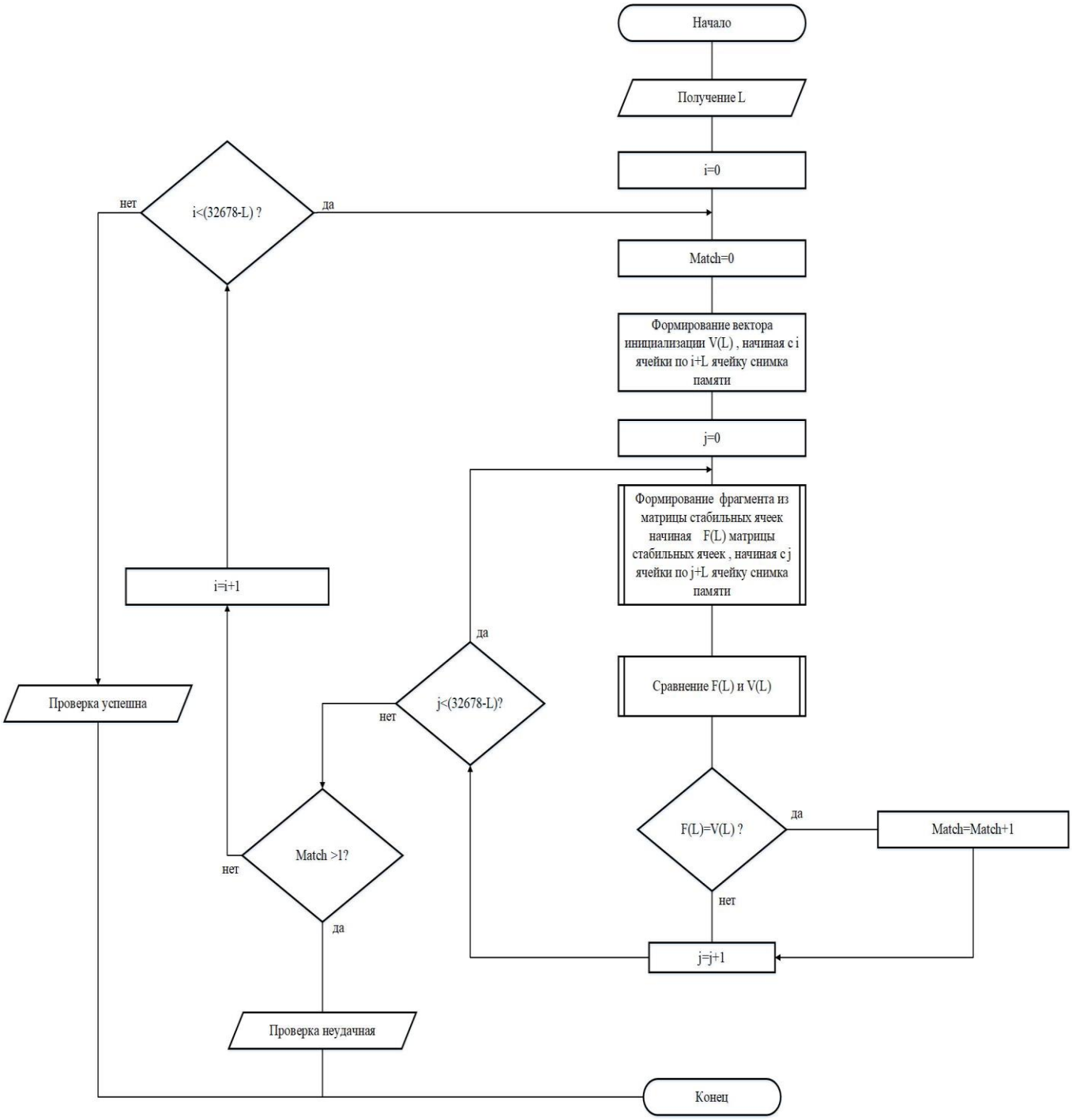

Рисунок 3.2 – Блок-схема алгоритма проверки длины вектора

На основе данных алгоритмов будет проводится начальный этап фазы инициализации карты доступа с статической ОЗУ для алгоритма взаимной аутентификации.

3.2. Разработка алгоритма взаимной аутентификации на основе свойств физически неклонируемых функций СОЗУ

Для организации взаимной аутентификации проводится фаза инициализации, в ходе которой выполняется исследование СОЗУ и на основе полученных данных определяется оптимальная длина вектора инициализации L. Так же делается матрица стабильных ячеек памяти СОЗУ M и определяется секретный ключ q и секретный идентификатор secret известный только контроллеру и карте. Блок-схема этапа инициализации алгоритма взаимной аутентификации представлена на рисунке 3.3.

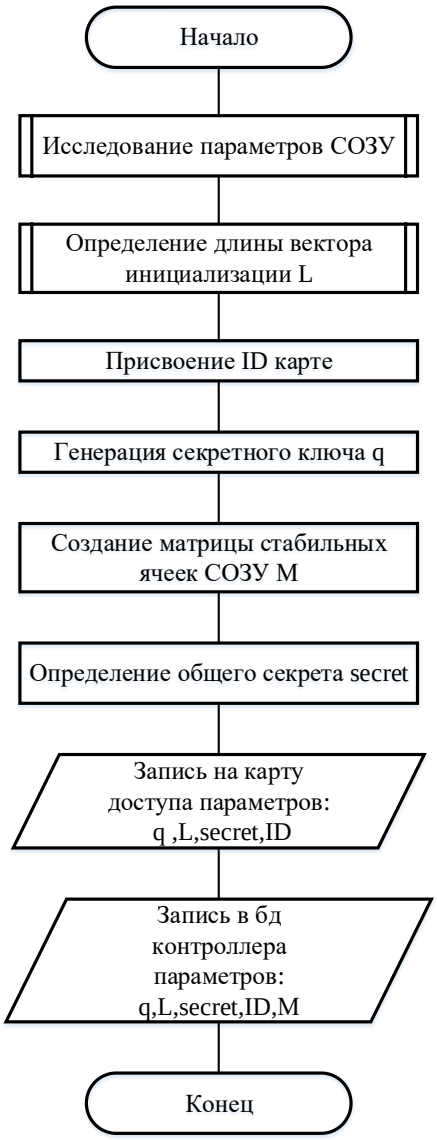

Рисунок 3.3 – Блок-схема этапа инициализации алгоритма взаимной аутентификации

После определения основных параметров в smart карту и базу данных контроллера записывается секретный ключ q, секретный идентификатор secret и длина вектора инициализации L, а в базу данных контроллера записывается также матрица стабильных ячеек памяти СОЗУ M.

Фаза аутентификации начинается после того как карта прикладывается к считывателю. Карта генерирует случайное число n и на основе образа памяти СОЗУ D, числа n и записанной на карту длины вектора инициализации, генерируется вектор инициализации V(n), где n номер ячейки образа памяти, с которой нужно считать L символов. После этого карта передаёт контроллеру ID и вектор инициализации V(n) и увеличивает счетчик безопасности с 0 до 1.

В случае если на карту с контроллера не придет ответ или ответ окажется не корректным, и будет заново инициирована процедура аутентификации счетчик будет увеличиваться на 1. Как только счетчик будет доходить до значения 3, на 4 попытку карта автоматически будет блокироваться, это позволит избежать успешной попытки сбора информации о образе памяти.

Как только контролер получит IDи V(n) он определит какая именно карта пытается авторизоваться и существует ли она. Если ID не соответствует легитимной карте, контролер отказывает в доступе и отправляет уведомление администратору. Если ID карты является действительным, контроллер на основе матрицы стабильных ячеек M осуществляет поиск однозначного совпадения между матрицей стабильных ячеек M и вектора инициализации, после чего определяет смещение offset. Смещение должно совпадать с случайным числом n, сгенерированным картой. После чего контролер вычисляет хэш-функцию Hash от смещения offset и секретного ключа q и передает хэш-функцию смарт карте.

Как только смарт карта получает хэш-функцию, кара вычисляет хэш-функцию Hash1 от случайного числа n и секретного ключа q. после чего осуществляет сравнение Hash и Hash1.Если хэш-функции совпадают счетчик безопасности обнуляется, и карта вычисляет хэш-функции Hash2 от случайного числа n, которое равно offset, и секретной информации secret, после чего отправляет полученный Hash2 контроллеру.

Блок-схема алгоритма взаимной аутентификации на стороне карты доступа представлена на рисунке 3.4.

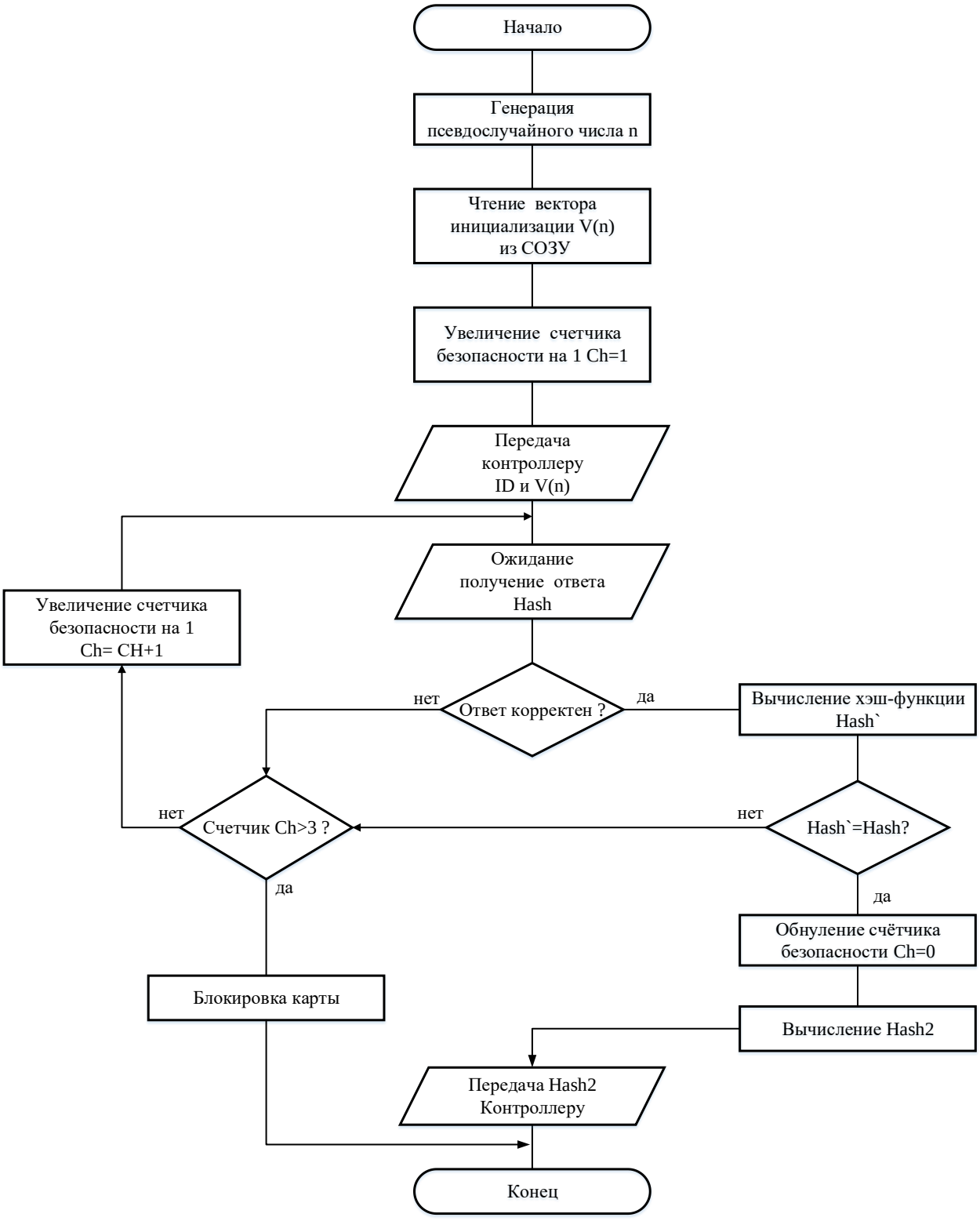

Рисунок 3.4 – Блок-схема работы алгоритма взаимной аутентификации на стороне карты доступа

Блок-схема алгоритма взаимной аутентификации на стороне контроллера представлена на рисунке 3.5.

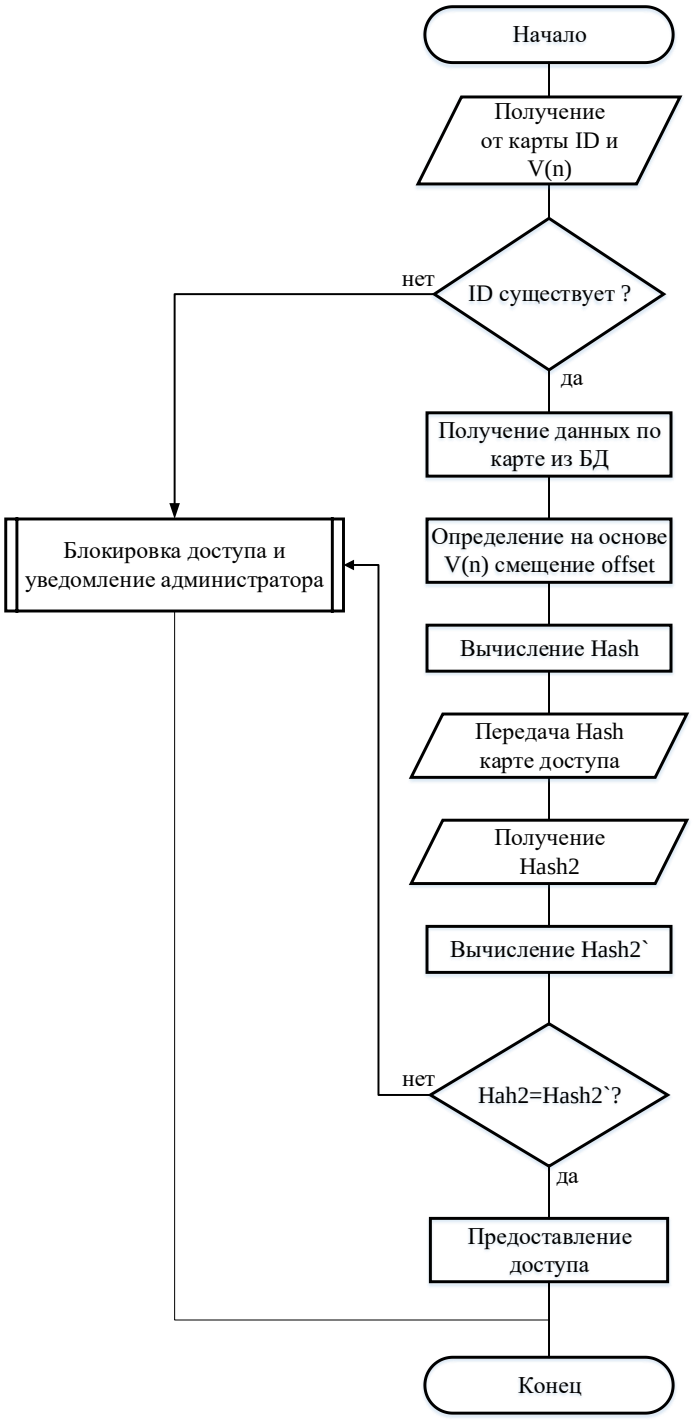

Рисунок 3.5 – Блок-схема работы алгоритма взаимной аутентификации на стороне контроллера

После принятия хэш-функции, контроллер на основе ID находит секретный идентификатор secret и вычисляет на основе secret и смещение offset хэш-

функцию Hash2' и выполняет сравнение Hash2 и Hash2'. Если хэш-функции совпадают доступ открыт, если хэш-функции не совпадают в доступе отказывается и отправляется уведомление администратору.

Защищенность данных будет гарантироваться двумя факторами, секретным ключом q и смещения вектора инициализации. Поскольку ключ передаваться в открытом виде не будет, а смещение можно вычислить на основе матрицы стабильных ячеек, хранимой только на контроллере, получить данные не представляется возможным. В случае если карта будет утеряна или украдена, карта доступа признается скомпрометированной и вносится в черный список, а при попытке злоумышленника воспользоваться данной картой, доступ будет закрыт и будет проинформирована служба безопасности.

К тому же каждая карта доступа обладает уникальным набором значений параметров СОЗУ, и вследствие чего компрометация одной карты не повлияют на другие карты доступа.

3.3. Тестирование и описание основных модулей программы алгоритма взаимной аутентификации на основе статической ОЗУ

В рамках разработки и тестирования программы алгоритма взаимной аутентификации на основе физически не клонируемой функции статической ОЗУ будет создано консольное приложение, которое будет содержать основные модули алгоритма, а также позволит проверить работу алгоритма.

На основе данных блок схем на объектно-ориентированном языке программирования C# будут созданы 2 класса: class smartcard , class controller.

Класс smartcard – это код отвечающий за работу алгоритма на стороне карты доступа. Он будет содержать 7 методов, которые выполняют следующие задачи: генерацию псевдослучайного числа, извлечение из СОЗУ данных, формирования из полученных данных вектор инициализации, передачу вектора контроллеру, получения и проверки хэш-функции котроллера, вычисление хэш-функции и передача её контроллеру, счетчик безопасности.

Методы smartcard:

Sec – метод обеспечение безопасности карты доступа, выполняет фиксирование неудачных попыток получение данных с карты доступа. В случае превышение 3 неудачных попыток, метод блокирует карту доступа.

Rand – метод генерирует псевдослучайное число начале сессии, необходимое для генерации вектора инициализации.

ReadMass – метод чтение снимка памяти.

GetVector – метод формирования вектора инициализации на основе результатов методов Rand, ReadMass.

Broadcast – метод передачи данных контроллеру.

CheckHash – метод получение и проверка хэш-функции от контроллера

Hash2 – метод формирования ответной хэш функции в случае легитимного контроллера.

Класс controller – это код отвечающий за работу алгоритма на стороне контроллера. Он будет содержать 5 методов, которые выполняют следующие задачи: получение данных от карты доступа, на основе полученного ID, получать из базы данных параметры карты доступа, вычисление смещение карты доступа, вычисление хэш-функции и передача карте доступа, получение и проверка хэш-функции карты доступа и на её основе отказ или предоставление доступа.

Методы controller:

ReadVector – метод получение данных из карты доступа.

GetData – метод запроса на основе ID карты, данных по карте доступа, снимка стабильных ячеек и секретный ключ и секретный ID.

GetOffset – метод вычисление смещение на основе предоставленных данных картой доступа и данных о карте доступа контроллера.

Hash – метод вычисление хэш функции на основе смещения и секретного ключа.

CheckHash2 – метод проверки хэш-функции от карты доступа и на основе проверки подтверждение или отказ карте в доступе.

В виду тестирования программы карты доступа будут эмитироваться и данные о картах представленные в таблице 3.1, будут внесены в код программы.

Таблица 3.1 – Таблица параметров тестовых карт доступа

Карты	Карта 1	Карта 2	Карта 3	Карта 4	Карта 5	Карта 6	Карта 7
ID	1	2	3	4	5	6	7
Стабильный вектор инициализации	28	58	90	60	412	186	1040

Одной из особенности алгоритма будет наличие псевдослучайного числа карты доступа и смещение контроллера. Для успешной сессии авторизации, 2 числа должны совпасть и на основе этих числе и секретных ключей должны совпасть вычисленные хэш-функции у обеих сторон.

Программа работает по следующему алгоритму, первыми запускается 5 метода класса smartcard. Первым и них запускается метод Broadcast который вызывает метод GetVector, а метод GetVector взывает ещё 2 метода Rand и ReadMass. В метод Broadcast передаются основные параметры такие как: путь к файлу из которого извлекаю данных о карте доступа, ID карты доступа, путь записи файла содержащий вектор инициализации.

Метод Rand формирует псевдослучайное число N и возвращает его методу GetVector.

Метод ReadMass получает параметр путь к txt файлу с данными о значениях ячеек 32-х Кбайтной СОЗУ. Далее метод извлекает и записывает эти данные в массив после чего возвращает массив методу GetVector.

После получения всех необходимых данных метод GetVector формирует

вектор инициализации. Для этого он определяет соответствующей ID карты длину вектора инициализации L, затем в полученном массиве от метода ReadMass он запрашивает N элемент массива и начиная с него извлекает L символов в новый массив и передает методу Broadcast.

Затем метод Broadcast формирует массив куда первым элементом вносит ID карты, далее вносится вектор инициализации, полученный массив записывается в файл Vector.txt.

Вовремя работы метода GetVector также запускает метод Sec увеличивающий счётчик безопасности с 0 на 1.

После этого запускается череда методов класс controller. Первым методом запускается Hash, далее он вызывает метод GetOffset, который в свою очередь вызывает ещё 2 метода: ReadVector,GetData.

Метод ReadVector извлекает из файла Vector.txt ID карты и вектор инициализации и передаёт методу GetOffset.

Метод GetData на основе ID извлекает соответствующий массив данных содержащий расположение стабильных ячеек памяти и возвращает методу GetOffset.

Далее из полученных данных метод GetOffset вычисляет смещение C, и передаёт его методу Hash.

Метод Hash вычисляет хэш-функцию на основе секретного ключа, соответствующего ID карты и смещения C. Полученные данные, записываются в файл Hash.txt.

Далее запускает 3 метода класса smartcard CheckHash, Sec, Hash2. Первым инициируется CheckHash который вызывает уже метод Sec и Hash2.

В начале метод CheckHash извлекает хэш-функцию из файла Hash.txt, далее он вычисляет собственную хэш-функцию на основе ID и случайно числа N. После метод сравнивает две хэш-функции, в случае совпадения он вызывает метод Sec, который обнулит счетчик безопасности, а далее запустится метод Hash2. В случае несовпадения хэш-функций метод CheckHash завершит сеанса, а счётчик безопасности останется с значением 1.

Данный счетчик будет фиксировать череду неудачных попыток, и когда число неудачных попыток подряд превысит 3, карта будет заблокирована.

После успешной проверки метода CheckHash метод Hash2 вычислит новую хэш-функцию на основе числа N и другого секретного идентификатора, полученный результат будет записан в файл Hash2.txt.

По завершению метода Hash2 запустится метод класса controller CheckHash2. Данный метод извлечет и файла Hash2.txt хэш-функцию и вычислит свою хэш-функцию на основе смещения C и секретного идентификатора карты. Данный идентификатор будет определён на основе ID карты. После вычисления метод сравнит 2 хэш-функции и в случае совпадения доступ будет открыт, а в случае провала доступ будет закрыт.

Для осуществления тестирования программы запустим консольное приложение и в открывшемся окне рисунок 3.6 откроется меню выбора карт доступа.

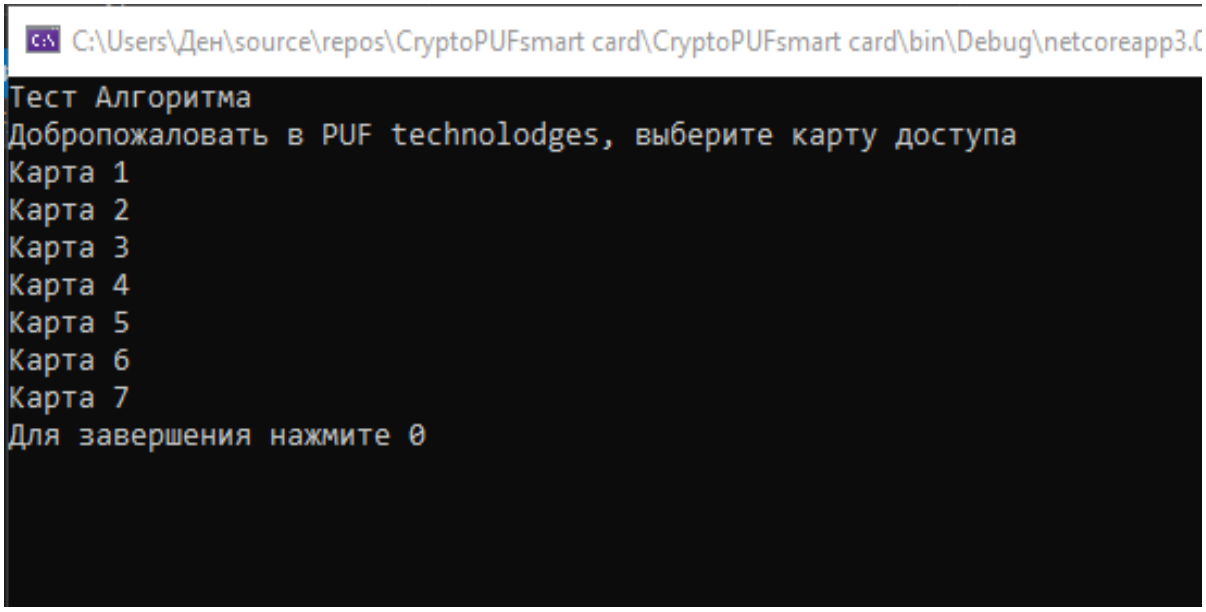

Рисунок 3.6 – Меню выбора карт доступа

В рамках тестирования программы карты с № 1,3-7 имеют совпадающие пары аутентификационных данных, то есть определенному снимку памяти карты доступа соответствует, построенная на основе данных о карте, матрица стабильных ячеек, записанная на стороне контроллера.

У карты № 2 было умышленно перепутаны данные снимка памяти карты доступа и снимка стабильных ячеек контроллера, для демонстрации неудачной попытки аутентификации и попытки атаки.

На рисунке 3.7 продемонстрированы успешно выполненная авторизация, поскольку случайное число и смещение совпали, следовательно, контролер вычислил верную хэш-функцию и является легитимным. Затем карта доступа предоставила верную хэш-функцию тем самым авторизовав себя.

В этом случае счетчик безопасности обнуляется и у карты доступа снова имеется 3 попытки на успешную авторизацию. Даже в случае если были осуществлены 2 неудачные попытки авторизации, к примеру карту доступа по ошибке применяли к чужому контроллеру, а затем карту применили к легитимному контроллеру, то счетчик безопасности обнулится.

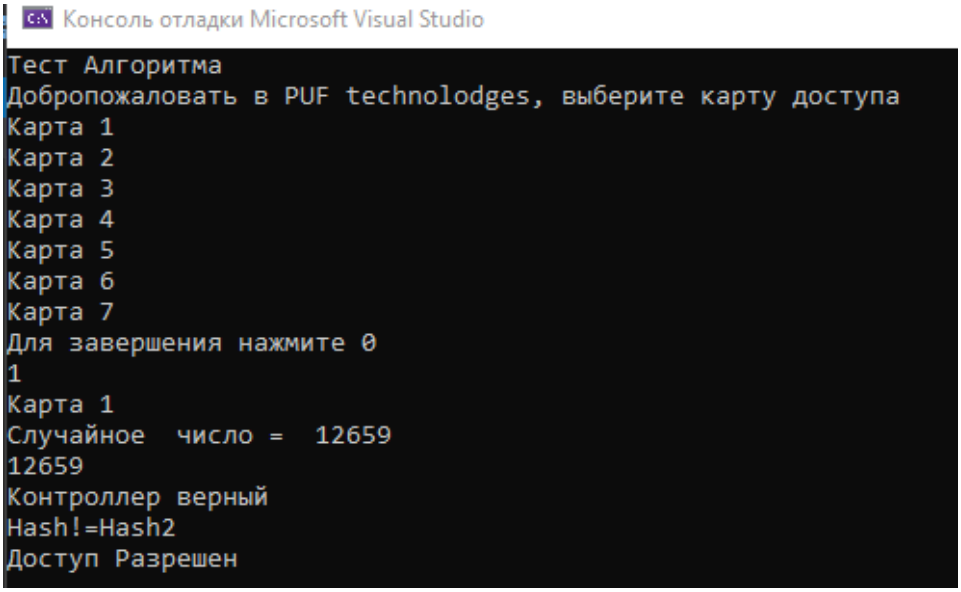

Рисунок 3.7 – Успешная авторизация

Продемонстрируем неудачную попытку авторизацию, показную на рисунок 3.8. Данная карта доступа и данные контроллера не соответствую друг другу, в результате чего хэш-функции не совпадут, и карта доступа завершает сеанс. При этому счетчик безопасности не обнулится и останется на значении 1 и при следующей неудачной попытке увеличится на единицу.

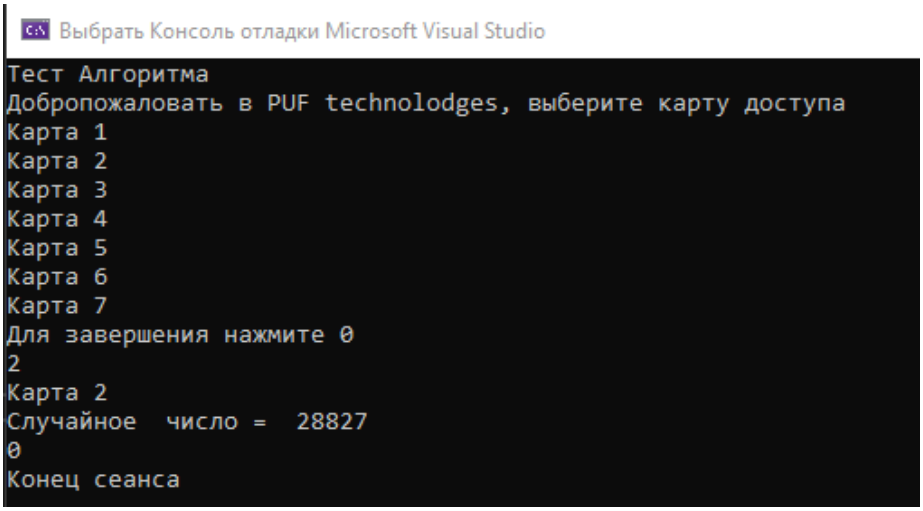

Рисунок 3.8 – Неудачная авторизация

После проведения 3-х подряд неудачных попыток авторизации, счетчик безопасности будет иметь уже значение 3 и на 4 неудачную попытку карта доступа заблокируется, что продемонстрировано на рисунке 3.9.

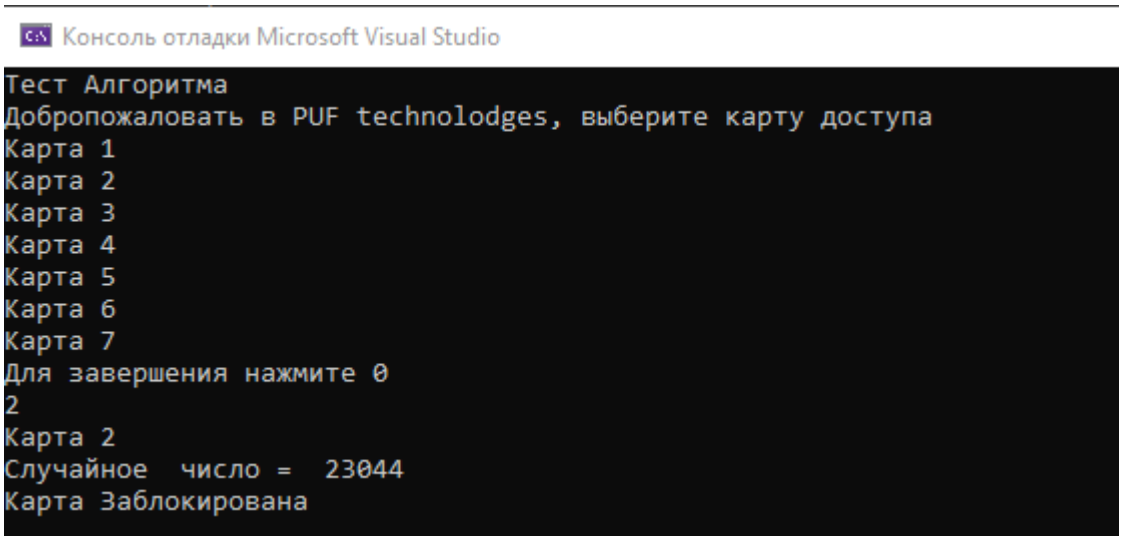

Рисунок 3.9 – Блокировка карты

Далее после блокировки карты доступа при попытке ещё раз инициировать авторизацию, методом Sec проверит значение счётчика безопасности и завершит сеанс авторизации, что показано на рисунке 3.10.

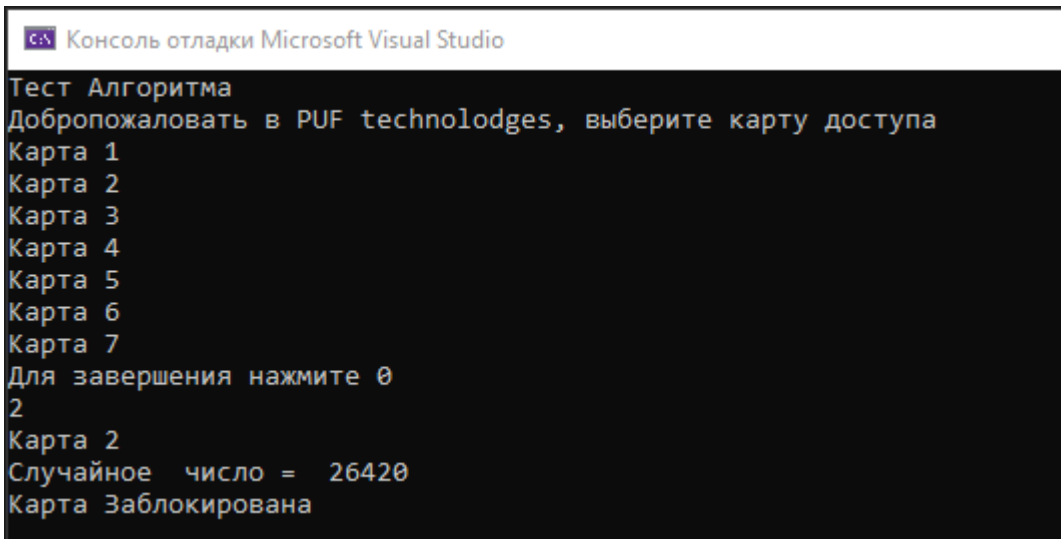

Рисунок 3.10 – Повторная блокировка карты

Таким образом программа выполняет основную функцию алгоритма взаимной аутентификации на основе физически неклонируемой функции статической СОЗУ. Это продемонстрировано тем, что на основе уникальной структуры СОЗУ карты доступа создаётся уникальный запрос контроллеру, а он в свою очередь на основе, полученных от карты доступа, открытых данных и уже имеющийся у него секретных данных о карте, вычисляет ответ. Далее после того, как карта доступа удостоверяется в действительности контроллера, она подтверждает свою действительность.

Также была продемонстрирована функция зашиты карты от многочисленных попыток доступа карте не действительным контроллером.

3.4. Выводы

В ходе разработки алгоритма взаимной аутентификации на основе физически неклонируемой функции СОЗУ замечено что для нормального функционирования системы потребуется база данных связанная с контроллером доступа. Данная база данных будет содержать информацию необходимую котроллеру доступа для осуществления взаимной аутентификации с картами доступа, а также для введения журнала безопасности о неудачных попытка авторизации и фиксирования успешных попыток авторизации. При успешной

авторизации в журнал будет записываться время получения доступа, имя и фамилия, а также должность сотрудника.

Карты доступа будут защищены от попыток изготовления дубликата, а также будут обособленны друг от друга, так как будут иметь уникальные параметры благодаря свойствам СОЗУ. Но стоит отметить, что необходимо строго контролировать кражу или утерю карт доступа сотрудниками, поскольку, имея в наличии карту доступа злоумышленник может беспрепятственно проникнуть в контрольную зону. Поэтому в случае утери необходимо внести карту доступа в черный список.

Ещё одним немаловажным элементом системы будет автоматизированное рабочее место (АРМ) администратора безопасности, поскольку за ним будет закреплено ряд важных задач:

- просмотр журнала безопасности и выявление инцидентов безопасности;
- инициализация карт доступа для новых сотрудников;
- заполнение и проверка базы данных карт;
- проверка СОЗУ на возможность использования в алгоритме;
- внесение в черный список утерянных карт доступа;
- разблокировка карт доступа.

От выполнения администратором этих задач будет, завесить стабильность работы алгоритма взаимной аутентификации на основе свойств физически неклонируемой функции статической ОЗУ.

4. Безопасность и экологичность проекта

4.1. Требования к производственным помещениям

Умственный труд один из важны видов деятельности человека, при этом он является интенсивным, напряженным, требующим значительных затрат умственной, эмоциональной и физической энергии. Это потребовало комплексного решения проблем эргономики, гигиены и организации труда, регламентации режимов труда и отдыха.

В настоящее время компьютерная техника широко применяется во всех областях деятельности человека. При работе с компьютером человек подвергается воздействию ряда опасных и вредных производственных факторов, например, электромагнитных полей (диапазон радиочастот: ВЧ, УВЧ и СВЧ), инфракрасного и ионизирующего излучений, шума и вибрации, статического электричества и др.

Работа с компьютером характеризуется значительным умственным напряжением и нервно-эмоциональной нагрузкой операторов, высокой напряженностью зрительной работы и достаточно большой нагрузкой на мышцы рук при работе с клавиатурой ЭВМ. В процессе работы с компьютером необходимо соблюдать правильный режим труда и отдыха. Большое значение имеет рациональная конструкция и расположение элементов рабочего места, что важно для поддержания оптимальной рабочей позы человека-оператора.

Правильно спроектированное и выполненное производственное освещение улучшает условия зрительной работы, снижает утомляемость, способствует повышению производительности труда, благотворно влияет на производственную среду, оказывая положительное психологическое воздействие на работающего, повышает безопасность труда и снижает травматизм.

Недостаточность освещения приводит к напряжению зрения, ослабляет внимание, приводит к наступлению преждевременной утомленности. Чрезмерно яркое освещение вызывает ослепление, раздражение и резь в глазах.

Неправильное направление света на рабочем месте может создавать резкие тени, блики, дезориентировать работающего. Все эти причины могут привести к несчастному случаю или заболеваниям глаз, поэтому столь важен правильный расчет освещенности.

Существует три вида освещения – естественное, искусственное и совмещенное (естественное и искусственное вместе).

Естественное освещение – освещение помещений дневным светом, проникающим через оконные проемы. Естественное освещение характеризуется тем, что меняется в широких пределах в зависимости от времени дня, времени года, характера области и ряда других факторов.

Искусственное освещение применяется при работе в темное время суток и днем, когда не удается обеспечить нормированные значения коэффициента естественного освещения (пасмурная погода, короткий световой день). Освещение, при котором недостаточное по нормам естественное освещение дополняется искусственным, называется совмещенным освещением. Искусственное освещение подразделяется на рабочее, аварийное, эвакуационное, охранное. Рабочее освещение, в свою очередь, может быть общим или комбинированным. Общее – освещение, при котором светильники размещаются в верхней зоне помещения равномерно или применительно к расположению оборудования. Комбинированное – освещение, при котором к общему добавляется местное освещение.

При выполнении работ категории высокой зрительной точности (наименьший размер объекта различения 0,3.0,5мм) величина коэффициента естественного освещения (КЕО) должна быть не ниже 1,5%, а при зрительной работе средней точности (наименьший размер объекта различения 0,5.1,0 мм) КЕО должен быть не ниже 1,0%. В качестве источников искусственного освещения обычно используются люминесцентные лампы типа ЛБ или ДРЛ, которые попарно объединяются в светильники, которые должны располагаться над рабочими поверхностями равномерно.

Требования к освещенности в помещениях, где установлены компьютеры,

следующие: при выполнении зрительных работ высокой точности общая освещенность должна составлять 300лк, а комбинированная – 750лк; аналогичные требования при выполнении работ средней точности – 200 и 300лк соответственно. Кроме того, степень освещения помещения и яркость экрана компьютера должны быть примерно одинаковыми, т.к. яркий свет в районе периферийного зрения значительно увеличивает напряженность глаз и, как следствие, приводит к их быстрой утомляемости.

Принцип нормирования микроклимата – создание оптимальных условий для теплообмена тела человека с окружающей средой. Вычислительная техника является источником существенных тепловыделений, что может привести к повышению температуры и снижению относительной влажности в помещении. В помещениях, где установлены компьютеры, должны соблюдаться определенные параметры микроклимата. В санитарных нормах СНиП 2.04.05-91 установлены величины параметров микроклимата, создающие комфортные условия. Эти нормы устанавливаются в зависимости от времени года, характера трудового процесса и характера производственного помещения.

Параметры микроклимата для помещений, где установлены компьютеры показаны в таблице 4.1.

Объем помещений, в которых размещены работники вычислительных центров, не должен быть меньше 19,5м^3/человека с учетом максимального числа одновременно работающих в смену.

Таблица 4.1 – Параметры микроклимата для помещений, где установлены компьютеры

Период года	Параметр микроклимата	Величина
Холодный	Температура воздуха в помещении, Относительная влажность, Скорость движения воздуха	22.24°C 40.60% до 0,1м/с
Теплый	Температура воздуха в помещении, Относительная влажность, Скорость движения воздуха	23.25°C 40.60% 0,1.0,2м/с

Для обеспечения комфортных условий используются как организационные

методы (рациональная организация проведения работ в зависимости от времени года и суток, чередование труда и отдыха), так и технические средства (вентиляция, кондиционирование воздуха, отопительная система).

Шум ухудшает условия труда, оказывая вредное действие на организм человека. Работающие в условиях длительного шумового воздействия испытывают раздражительность, головные боли, головокружение, снижение памяти, повышенную утомляемость, понижение аппетита, боли в ушах и т. д. Такие нарушения в работе ряда органов и систем организма человека могут вызвать негативные изменения в эмоциональном состоянии человека вплоть до стрессовых. Под воздействием шума снижается концентрация внимания, нарушаются физиологические функции, появляется усталость в связи с повышенными энергетическими затратами и нервно-психическим напряжением, ухудшается речевая коммутация. Все это снижает работоспособность человека и его производительность, качество и безопасность труда. Длительное воздействие интенсивного шума [выше 80 дБ(А)] на слух человека приводит к его частичной или полной потере. В таблице 4.2 указаны предельные уровни звука в зависимости от категории тяжести и напряженности труда, являющиеся безопасными в отношении сохранения здоровья и работоспособности.

Таблица 4.2 – Предельные уровни звука, дБ, на рабочих местах.

Категория напряженности труда	Категория тяжести труда			
	Легкая	Средняя	Тяжелая	Очень тяжелая
Мало напряженный	80	80	75	75
Умеренно напряженный	70	70	65	65
Напряженный	60	60	-	-
Очень напряженный	50	50	-	-

Уровень шума на рабочем месте сотрудников не должен превышать 50дБА, а в залах обработки информации на вычислительных машинах – 65дБА.

Для снижения уровня шума стены и потолок помещений, где установлены

компьютеры, могут быть облицованы звукопоглощающими материалами.

4.2. Электромагнитное и ионизирующее излучения

Большинство ученых считают, что как кратковременное, так и длительное воздействие всех видов излучения от экрана монитора не опасно для здоровья персонала, обслуживающего компьютеры. Однако исчерпывающих данных относительно опасности воздействия излучения от мониторов на работающих с компьютерами не существует и исследования в этом направлении продолжаются. Допустимые значения параметров неионизирующих электромагнитных излучений от монитора компьютера в соответствии с СанПиНом 2.2.2.542-2003 представлены в таблице 4.3.

Максимальный уровень рентгеновского излучения на рабочем месте оператора компьютера обычно не превышает 10мкбэр/ч, а интенсивность ультрафиолетового и инфракрасного излучений от экрана монитора лежит в пределах 10.100мВт/м^2.

Таблица 4.3 – Допустимые значения параметров неионизирующих электромагнитных излучений

Наименование параметра	Допустимые значения
Напряженность электрической составляющей электромагнитного поля на расстоянии 50см от поверхности видеомонитора	10В/м
Напряженность магнитной составляющей электромагнитного поля на расстоянии 50см от поверхности видеомонитора	0,3А/м
Напряженность электростатического поля для взрослых пользователей не должна превышать	20кВ/м

Для снижения воздействия этих видов излучения рекомендуется применять мониторы с пониженным уровнем излучения устанавливать защитные экраны, а также соблюдать регламентированные режимы труда и отдыха.

В таблице 4.4 представлены сведения о регламентированных перерывах, которые необходимо делать при работе на компьютере, в зависимости от продолжительности рабочей смены, видов и категорий трудовой деятельности с мониторов ПЭВМ в соответствии с СанПиНом 2.2.2 542-2003 «Гигиенические требования к видеодисплейным терминалам, персональным электронно-вычислительным машинам и организации работ».

Таблица 4.4 – Время регламентированных перерывов при работе на компьютере

Категория работы с ВДТ или ПЭВМ	Уровень нагрузки за рабочую смену при видах работы с ВДТ			Суммарное время регламентированных перерывов в минутах	
	Группа А, количество знаков	Группа Б, количество знаков	Группа В, часов	При 8-часовой смене	При 12-часовой смене
I	до 20000	до 15000	до 2,0	30	70
II	до 40000	до 30000	до 4,0	50	90
III	до 60000	до 40000	до 6,0	70	120

В противном случае у персонала отмечаются значительное напряжение зрительного аппарата с появлением жалоб на головные боли, раздражительность, нарушение сна, усталость и болезненные ощущения в глазах, в пояснице, в области шеи и руках.

При несоответствии фактических условий труда требованиям Санитарных правил и норм время регламентированных перерывов следует увеличить на 30%.

В соответствии со СанПиН 2.2.2 546-2003 все виды трудовой деятельности, связанные с использованием компьютера, разделяются на три группы:

– группа А: работа по считыванию информации с экрана ПЭВМ с предварительным запросом;

– группа Б: работа по вводу информации;

– группа В: творческая работа в режиме диалога с ЭВМ.

Эффективность перерывов повышается при сочетании с производственной гимнастикой или организации специального помещения для отдыха персонала с удобной мягкой мебелью, аквариумом, зеленой зоной и т.п.

4.3. Эргономические требования к рабочему месту

Проектирование рабочих мест, снабженных ПЭВМ, относится к числу важных проблем эргономического проектирования в области вычислительной техники.

Рабочее место и взаимное расположение всех его элементов должно соответствовать антропометрическим, физическим и психологическим требованиям. Большое значение имеет также характер работы. В частности, при организации рабочего места должны быть соблюдены следующие основные условия: оптимальное размещение оборудования, входящего в состав рабочего места и достаточное рабочее пространство, позволяющее осуществлять все необходимые движения и перемещения.

Эргономическими аспектами проектирования рабочих мест, в частности, являются: высота рабочей поверхности, размеры пространства для ног, требования к расположению документов на рабочем месте (наличие и размеры подставки для документов, возможность различного размещения документов, расстояние от глаз пользователя до экрана, документа, клавиатуры и т.д.), характеристики рабочего кресла, требования к поверхности рабочего стола, регулируемость элементов рабочего места.

Главными элементами рабочего места администратора являются стол и кресло. Основным рабочим положением является положение сидя. Рабочая поза сидя вызывает минимальное утомление. Рациональная планировка рабочего места предусматривает четкий порядок и постоянство размещения предметов, средств труда и документации.

То, что требуется для выполнения работ чаще, расположено в зоне легкой досягаемости рабочего пространства. Моторное поле – пространство рабочего места, в котором могут осуществляться двигательные действия человека.

Максимальная зона досягаемости рук – это часть моторного поля рабочего места, ограниченного дугами, описываемыми максимально вытянутыми руками при движении их в плечевом суставе. Оптимальная зона – часть моторного поля рабочего места, ограниченного дугами, описываемыми предплечьями при движении в локтевых суставах с опорой в точке локтя и с относительно неподвижным плечом.

Большое значение придается характеристикам рабочего кресла. Так, рекомендуемая высота сиденья над уровнем пола находится в пределах 420-550мм. Поверхность сиденья мягкая, передний край закругленный, а угол наклона спинки – регулируемый. Необходимо предусматривать при проектировании возможность различного размещения документов: сбоку от ПЭВМ, между монитором и клавиатурой и т.п. Кроме того, в случаях, когда монитор имеет низкое качество изображения, например, заметны мелькания, расстояние от глаз до экрана делают больше (около 700мм), чем расстояние от глаза до документа (300-450мм).

Большое значение также придается правильной рабочей позе пользователя. При неудобной рабочей позе могут появиться боли в мышцах, суставах и сухожилиях. Причина неправильной позы пользователей обусловлена следующими факторами: нет хорошей подставки для документов, клавиатура находится слишком высоко, а документы – низко, некуда положить руки и кисти, недостаточно пространство для ног.

В целях преодоления указанных недостатков даются общие рекомендации: лучше передвижная клавиатура; должны быть предусмотрены специальные приспособления для регулирования высоты стола, клавиатуры и
экрана, а также подставка для рук.

Существенное значение для производительной и качественной работы на компьютере имеют размеры знаков, плотность их размещения, контраст и соотношение яркостей символов и фона экрана. Если расстояние от глаз оператора до экрана дисплея составляет 60.80 см, то высота знака должна быть не менее 3мм, оптимальное соотношение ширины и высоты знака составляет 3:4, а

расстояние между знаками – 15.20% их высоты. Соотношение яркости фона экрана и символов – от 1:2 до 1:15.

Во время пользования компьютером медики советуют устанавливать монитор на расстоянии 50-60 см от глаз. Когда человек смотрит прямо перед собой, его глаза открываются шире чем, когда он смотрит вниз. За счет этого площадь обзора значительно увеличивается, вызывая обезвоживание глаз. К тому же если экран установлен высоко, а глаза широко открыты, нарушается функция моргания.

Это значит, что глаза не закрываются полностью, не омываются слезной жидкостью, не получают достаточного увлажнения, что приводит к их быстрой утомляемости.

Создание благоприятных условий труда и правильное эстетическое оформление рабочих мест на производстве имеет большое значение, как для облегчения труда, так и для повышения его привлекательности, положительно влияющей на производительность труда.

4.4. Выводы

В данной главе было произведено исследование ряда факторов, воздействующих на пользователя:

- электромагнитное и ионизирующее излучения;
- эргономические требования к рабочему месту;
- освещение;
- микроклимат.

Также были приведены общие мероприятия по безопасности жизнедеятельности на объекте. Приведенные меры необходимы для уменьшения воздействия неблагоприятных факторов на человека. Поскольку неправильное освещение, микроклимат, а также электромагнитное и ионизирующее излучения могут привести к зрительному и общему утомлению, снижает

производительности труда и его качество; вызывает различные заболевание у человека; может являться источником возникновения аварийных ситуаций и т.д.

Применение описанных в главе мер поможет значительно снизить влияние неблагоприятных факторов на рабочем месте на сотрудника.

5. Технико-экономическое обоснование дипломного проекта

5.1 Определение трудоемкости разработки

Технико-экономическое обоснование должно содержать:

- определение трудоемкости разработки;
- подсчет затрат на разработку проекта;
- вычисление ориентировочной цены проекта;
- обоснованный выбор программных и аппаратно-программных средств;
- оценку социально-экономических результатов функционирования дипломного проекта.

Для определения трудоемкости разработки дипломного проекта, сначала определяется список основных этапов работ, которые необходимо выполнить. В таблице 5.1 расписаны работы по этапам с оценкой трудоемкости их выполнения.

Выделено два этапа проведения: получение информации о предметной области и разработка программы. Первый этап требует значительного умственного труда.

Таблица 5.1 – Распределение работ по этапам и видам и оценка их трудоемкости

Этап проведения	Вид работы на данном этапе	Трудоемкость выполнения, чел.-ч.
Получение информации о предметной области	Сбор данных с микросхем.	48
	Обработка собранных данных	64
Разработка программы	Разработка алгоритма и определение ключевых параметров	64
	Написание и отладка программы	64
Итого трудоемкость выполнения дипломного проекта		240

5.2 Расчет затрат на разработку приложения

Для оценки расходов на реализацию составляется определенная смета, которая имеет следующие пункты:

1. Затраты на оплату труда.
2. Затраты на оборудование и комплектующие.
3. Прочие затраты.

В статью «Затраты на оплату труда» включаются расходы по оплате труда всех работников, занятых разработкой. Общее время работы программиста определяется из таблицы 5.1 и равно 240 часов. Федеральным агентством по образованию РФ установлены следующие нормы затрат рабочего времени на одну дипломную работу: руководитель работы 20 ч, консультант по БЖД – 2 ч, консультант по экономической части – 2 ч.

Общая сумма затрат на оплату труда (S_P) определяется по формуле:

$$S_P = \sum_{i=1}^{n} P_i \times T_i \quad , \tag{5.1}$$

где P_i – часовая ставка i-го работника, руб.,

T_i – время на разработку, час,

i – категория работника,

n – количество работников, занятых разработкой.

Среднечасовая заработная плата рассчитывается по формуле:

$$P_i = \frac{MP_i}{TW_i} \quad , \tag{5.2}$$

где MP_i – среднемесячная заработная плата разработчика, руб.;

TW_i – среднемесячный фонд рабочего времени (100 часов в месяц).

Стоимость одного часа работы студента равна:

$$P_i = \frac{3000}{100} = 30 \text{ руб.} \tag{5.3}$$

Стоимость одного часа работы доцента равна:

$$P_i = \frac{20000}{100} = 200 \text{ руб.} \tag{5.4}$$

Общая сумма затрат на оплату труда равна:

$$S_P = 240 \times 30 + 20 \times 200 + 2 \times 200 + 2 \times 200 = 12000_{\text{руб.}} \quad (5.5)$$

Общие затраты на оплату труда, приведены в таблице 5.2.

Таблица 5.2 – Затраты на оплату труда

Категория работника	Квалификация	Трудоемкость разработки, чел.-ч.	Часовая ставка, руб/ч	Сумма, руб
Разработчик программы	студент	240	30	7 200
Руководитель диплома	доцент	20	200	4 000
Консультант по БЖД	доцент	2	200	400
Консультант по экономической части	доцент	2	200	400
Итого				12 000

Затраты на оборудования и комплектующие вынесены в таблицу 5.3. В данном расчет не будут учитывать комплектующие собственного производства. Итоговая стоимость оборудования и комплектующих S_{Eq} рассчитывается по формуле.

$$S_{Eq} = \sum_{i=1}^{n} Eq_i \times N_i \quad , \quad (5.6).$$

где Eq_i – цена за шт. i-го оборудования и комплектующих, руб.,

N_i – количество i-го оборудования и комплектующих, шт.,

i – номер оборудования и комплектующих,

n – количество оборудования и комплектующих.

Таблица 5.3 – Расчет стоимости материалов

№	Наименование оборудования и комплектующих	Цена, руб/шт	Количество, шт	Стоимость, руб
1	Универсальный модуль Arduino Mega 2560	2 300	1	2300

Продолжение таблицы 5.3

2	Микросхема статического ОЗУ HM62256	100	7	700
3	Быстросъемная панель для микросхем памяти	400	1	400
			Итоговая стоимость	3400

Цены указаны в рублях по курсу на 2020-05-20.

В статью «Прочие затраты» включаются расходы на содержание административно-управленческого и учебно-вспомогательного персонала, на отопление, освещение и текущий ремонт помещений, канцелярские, командировочные и прочие хозяйственные расходы. Затраты по этой статье принимаются в размере 70 % от затрат на оплату труда

$$S_o = 0.7 \times 12000 = 8\,400 \text{ руб.}$$

Общая сумма затрат на электроэнергию (S_E) рассчитывается по формуле:

$$S_E = \sum_{i=1}^{n} Pw_i \times K_i \times T_i \times P, \quad (5.7)$$

где Pw_i – паспортная мощность i-го электрооборудования, кВт;

K_i – коэффициент использования мощности i-го электрооборудования (принимается $K_i = 0.7 \div 0.9$);

T_i – время работы i-го оборудования за весь период разработки, ч;

P – цена электроэнергии, руб/кВт·ч.

i – вид электрооборудования;

n – количество электрооборудования.

Таблица 5.4 – Смета затрат на разработку

Наименование оборудования	Паспортная мощность, кВт	Коэффициент использования мощности	Время работы оборудования для разработки, ч	Цена электроэнергии, $\frac{руб.}{кВт \cdot ч}$	Сумма, руб.
Компьютер №1	0.44	0.85	240	4,63	415.58

Продолжение таблицы 5.4

Arduino Mega 2560	$0{,}330*10^{-3}$	0.8	48	4,63	0,058
ИТОГО затраты на электроэнергию					415,63

Общая сумма затрат на электроэнергию составляет:

$$З_э = 0.44 \times 0.85 \times 240 \times 4.63 + 0.330 \times 10^{-3} \times 0.8 \times 48 \times 4.63 = 415{,}63 \text{руб.}$$

На основании полученных данных по отдельным статьям составляется общая смета затрат на разработку дипломного проекта по форме, приведенной в таблице 5.5.

Таблица 5.5 – Смета затрат на разработку

Статьи затрат	Сумма, руб.
1. Затраты на оплату труда	12 000
2. Затраты на оборудования и комплектующих	3400
4. Прочие затраты	8400
5.Затраты на электроэнергию	415,63
Итого	24 215,63

Затраты на разработку составят $S_T = 24\,215{,}63$руб.

Величина договорной цены устанавливается с учетом эффективности, качества и сроков ее выполнения на уровне, отвечающем экономическим интересам потребителя и исполнителя.

Договорная цена (P_D) рассчитывается по формуле:

$$P_D = S_T \times \left(1 + \frac{R}{100}\right), \quad (5.8)$$

где S_T – затраты на разработку, руб.;

R – средний уровень рентабельности, % (принимается в размере 25%).

Исходя из этого, договорная цена данной будет следующей:

$$P_D = 24\,215{,}63 \times \left(1 + \frac{25}{100}\right) = 30\,269{,}53 \text{ руб.} \quad (5.9)$$

Таким образом, учитывая стоимость вычислительной техники, общая стоимость данного проекта будет приблизительно составлять:

$$P = 30269{,}53 + 42000 = 72269{,}53 \quad (5.10)$$

5.3 Экономическое обоснование выбора комплекса технических и программных средств и социально-экономический эффект от разработки

Для быстрой и качественной разработки требуется мощный компьютер с GPU от компании NVIDIA для, быстрой обработки данных . Изучив рынок персональных компьютеров, выбран ACER Aspire V3-571G Характеристика:

- процессор: Intel Core i5 3210;
- процессор, частота: 2,5 ГГц;
- количество ядер процессора: двухядерный;
- оперативная память: DDR3 8192 Мб ;
- тип графического контроллера: дискретный;
- видеокарта: NVIDIA GeForce GT 730M— 2048 Мб;
- жесткий диск: 465 Гб, 7200 об/мин, SATA III;
- оптический привод: DVD-RW;
- кард-ридер: встроенный;
- поддержка карт памяти: SD;
- тип кабельной сети (разъем RJ-45) Gigabit Ethernet;
- блок питания: 220 Вт;

В качестве IDE выбрана Visual Studio 2019 Community с пакетом C#. Версия Community можно бесплатно использовать в научных разработках, но для коммерческого использования нужно подсчитать доход организации и количество компьютеров, чтобы учесть законность бесплатного использования версии Community.

Продукт Visual Studio от Microsoft представляет линейку продуктов, которые помимо самой IDE и имеют ряд инструментов для разработки. С помощью данного продукта разрабатываются консольные приложения,

приложения с графическим пользовательским интерфейсом, веб-сайты, веб-приложения, веб-службы как в родном, так и в управляемом кодах для всех платформ, поддерживаемых Windows, Windows Mobile, Windows CE, .NET Framework, Xbox, Windows Phone .NET Compact Framework и Silverlight.

Целью работы является достижение социального эффекта, но приходится считаться и с материальными затратами на реализацию и установку. Эти затраты необходимы:

– обновление мощностей в сети, где функционирует разработка;
– обучение персонала.

Социальный эффект от внедрения программы:

– облегчается работа системного администратора;
– своевременно идентифицируются сотрудники, распространяющие закрытую информацию организации.

Одно из перспективных направление применения алгоритма взаимной аутентификации на основе ФНФ – обеспечение безопасности контрольной зоны. Существует множество способов защиты идентификаторов в системах СКУД, которые требуют дополнительные затраты на оборудование и мощностные характеристики оборудования. В связи с этим возрастает интерес к альтернативным методам при организации безопасности систем СКУД, менее затратные и менее ресурсозатратные, при это имеющие туже или повышенную эффективность.

5.4 Выводы

В данной главе были проведены технико-экономические расчеты, которые устанавливают размеры затрат осуществления разработки и проектирования устройства, описанного в предыдущих главах. На данной основе были рассчитаны основные затраты на дельнейшее ведение производства, а именно приобретения оборудования и комплектующих, оплаты электроэнергии и иных расходов. Немаловажным является оплата труда квалифицированных специалистов,

инженеров, которая расценивается по различным категория. В результате расчетных работ был произведен полной подсчет себестоимости разработки способа взаимной аутентификации на основе физически неклорируемой функции статической ОЗУ.

Заключение

В дипломном проекте, посвящённом разработке способа взаимной аутентификации с использованием свойств физически неклонируемых функций на основе микросхем статической памяти, достигнута сформулированная во введении цель, решены поставленные задачи по анализу существующих технологий обеспечения идентификации и аутентификации в системах контроля и управления доступом, разработан способ определения оптимальной длины вектора, разработан алгоритм взаимной аутентификации на основе свойств физически неклонируемой функции статической ОЗУ.

В первой главе был проведен анализ достоинств и недостатков существующих технологий обеспечения аутентификации в системах контроля и управления доступом.

При рассмотрении существующих методов организации системы контроля и управления доступом было замечено что большинство систем уязвимы к атакам на копирование ключа (смарт-карты), но в свою очередь их можно защитить с помощью криптографических алгоритмов, которые могут обеспечить достаточный уровень безопасности, но будут требовать дополнительные денежные затраты, а также мощностные ресурсы.

Так же было рассмотрен метод двухфакторной аутентификации, который обеспечит надёжность системы контроля и управление доступом, но сложность монтажа и большие денежные затраты для организации дополнительного метода аутентификации, как ввод pin кода или биометрические методы аутентификации, является недостатком таких систем. Так же процесс идентификации станет более сложным и продолжительным по сравнению с обычной системой контроля и управление доступом с использование карт или ключей доступа

В главе построена модель угроз на основе методических документов ФСТЭК России для информационной системы контроля и управления доступом. Выявлено 14 актуальных угроз из Банка угроз ФСТЭК и определены

технологические мероприятий по нейтрализации актуальных угроз, которые включают организационные и технические меры.

Решено, что проблему защиты идентификаторов от несанкционированного дублирования можно решить, используя алгоритм взаимной аутентификации с использованием свойств физически неклонируемой функции статической ОЗУ, это поможет защитить идентификатор от передачи данных не опознанному устройству, а также защиты данных передающихся по открытому каналу между идентификатором и контроллером доступа.

Вторая глава посвящена анализу свойства физически неклонируемых функций (PUF) на основе статической ОЗУ, определению оптимальной длины вектора инициализации алгоритма.

В главе были проанализированы данные с 7 различных микросхем в результате чего было замечено, что при различных параметрах, как число стабильных ячеек, число уникальных значений ячеек, частоты встречаемости значений в ячейках, максимальной длины между стабильными ячейками оказывают влияние на длину вектора инициализации при этом больше всего оказывает влияния параметры, как максимальное расстояние между стабильными ячейками и частота встречаемости значений в стабильных ячейках. Это влияние обусловливается тем, что длина вектора не может быть меньше расстояния между стабильными ячейками, а также чем меньше длина максимального расстояния между стабильными ячейками, тем меньше среднее расстояние между стабильными ячейками, а значит более плотно расположены стабильных ячеей что вместе с неравномерным распределением значений ячеек, где может преобладать одно или несколько значений повышает вероятность встречи однотипных комбинаций стабильных ячеек. Из-за чего для однозначного совпадения значения необходимо увеличить длину вектора инициализации и злоумышленнику становится проще проводить анализ вектора инициализации. Это связано с тем, что чем больше длина вектора инициализации, тем больше количества информации, продевается по открытому каналу. В свою очередь это

приведет к увеличению вероятности компрометации карт доступа на основе СОЗУ.

На основе этого можно сделать вывод что не каждая микросхема может применятся в алгоритме взаимной аутентификации на основе статического ОЗУ, поскольку повлиять на параметры СОЗУ не представляется возможным ввиду конструкторских особенностей и определенных условий окружающей среды.

Так же ввиду уникальности структуры каждой микросхемы СОЗУ оптимальная длина вектора инициализации будет для каждой микросхемы своя, и для её определения необходимо проводить исследования СОЗУ.

В третьей главе разработан способ исследования СОЗУ для определения возможности применения её в алгоритме взаимной аутентификации на основе статической ОЗУ, оптимальной длины вектора инициализации, а также получения данных необходимых для работы алгоритма с данной СОЗУ.

Разработан алгоритм взаимной аутентификации на основе свойств физически неклонируемой функции статической ОЗУ, противодействующий попыткам считать с карты доступа секретного идентификатора и дальнейшего его копирования.

Также алгоритм противодействует попыткам сбора информации по открытому каналу связи между идентификатором и контроллером доступа, для дальнейшего анализа параметров СОЗУ. Полученные данные по открытому каналу связи не помогут злоумышленнику реализовать успешную аутентификацию поскольку, нарушитель не будет знать секретный ключ q и вычислить смещение offset, необходимых для вычисления хэш-функции.

В случае утери или кражи карты доступа ID карты и все параметры связанные сданным ID признается не действительным. Сама же потеря карты доступа, не компрометирует другие карты ввиду уникальности СОЗУ.

В четвертой главе было произведено исследование ряда факторов, возникающих в производственной деятельности. Данные факторы могут привести к общему утомлению, снижает производительности труда и его качества, а также вызывать различные заболевание у сотрудника. Для уменьшения воздействия

неблагоприятных факторов на сотрудника приведенные меры противодействия им.

В пятой главе были проведены технико-экономические расчеты, которые устанавливают размеры затрат осуществления разработки алгоритма взаимной аутентификации на основе свойств физически неклонируемой функции статической ОЗУ. На данной основе были рассчитаны основные затраты на дельнейшее ведение разработки, а именно приобретения оборудования и комплектующих, оплаты электроэнергии, оплата труда квалифицированных специалистов и иных расходов. В результате расчетных работ был произведен полной подсчет себестоимости разработки способа взаимной аутентификации на основе физически неклорируемой функции статической ОЗУ.

Таким образом, в данной дипломном проекте разработан защищенный способ взаимной аутентификации на основе физически неклонируемой функции статической ОЗУ. Направлением дальнейшего развития работы является разработка готового прототипа карты доступа со встроенной СОЗУ.

Список используемой литературы

1. Pappu R. Physical One-Way Functions // Science. – 2002. – Vol. 297. –P. 2026–2030.

2. Pappu, R. Physical One-Way Functions: PhD Thesis in Media Arts and Sciences / Pappu R. Massachusetts Institute of Technology (MIT). – Cambridge, 2001. – 154 P.

3. Gassend B.Controlled physical random functions // Proc. of 18th Annual Computer Security Applications Conf. (ACSAC), Las Vegas, Nevada , 2002. – P. 149–160.

4. Gassend, B. Physical Random Functions: MSc Thesis / B. Gassend // Massachusetts Institute of Technology (MIT). – Cambridge, 2003. – 89 P.

5. Ekert, A.K. Quantum cryptography based on Bell's theorem / A.K. Ekert // Physical Review Letters. – 1991. – Vol. 67, № 6. – P. 661–663.

6. Bennett, C.H. Quantum cryptography using any two nonorthogonal states / C.H. Bennett //Physical Review Letters. – 1992. – Vol. 68, № 21. – P. 3121–2124.

7. Kocarev, L. Chaos-based cryptography: a brief overview / L. Kocarev // Circuits and Systems Magazine. – 2001. –Vol. 1, № 3. – P. 6–21.

8. Shannon, C.E. Communication theory of secrecy systems / C.E. Shannon // Bell System Tech. J. – 1949. – P. 656–715.

9. Ozturk, E. Physical unclonable function with tristate buffers / E. Ozturk, G. Hammouri, B. Sunar // Proc. of IEEE International Symposium on Circuits and Systems (ISCAS 2008). – Seattle, WA, USA, 2008. – P. 3194–3197.

10. Holocomb, D. Power-up SRAM State as an Identifying Fingerprint and Source of TrueRandom Numbers / D. Holocomb, W. Burleson // IEEE Transactions on Computers. – 2008. – Vol. 57, № 11. – P. 1198–1210.

11. Guajardo J. FPGA Intrinsic PUFs and Their Use for IP Protection / Lecture Notes in Computer Science. – 2007. – Vol. 4727. – P. 63–80.

12. Maes, R. Intrinsic PUFs from Flip-flops on Reconfigurable Devices / R. Maes, P. Tuyls, I. Verbauwhede // Proc. of 3rd Benelux Workshop on Information and System Security (WISSec 2008). – Eindhoven, The Netherlands, 2008. – P. 3–20.

13. Bohm, C., Hofer, M. An alternative to error correction for SRAM-like PUFs. In Cryptographic Hardware and Embedded Systems (CHES). Berlin, Heidelberg (Germany), 2010, p. 335–350.

14. Блейхут Р. Теория и практика кодов, контролирующих ошибки = Theory and Practice of Error Control Codes. — М.: Мир, 1986. — 576 с.

15. Christoph Böhm, Maximilian Hofer, Physical Unclonable Functions in Theory and Practice - Springer, 2013

16. Ярмолик В. Н., Вашинко Ю. Г. Физически неклонируемые функции Информатика. 2011. № 2. С. 92–103.

17. Aliev G., Examination of distribution regularities in static RAM microcircuit cells in case of using them as a PUF in a mutual authentication module/ G. Aliev, O. Malsugenov, O. Mezentseva // Proc. of the Young Scientist's Third International Workshop on Trends in Information Processing (YSIP3 2019), Stavropol, Russian Federation, 2019 – paper 11

18. Материалы сайта techportal.ru [Электронный ресурс] Режим доступа – http://www.techportal.ru/glossary/karti-kontrolya-dostupa.html

19. Материалы сайта securityrussia.com [Электронный ресурс] Режим доступа – https://securityrussia.com/blog/mifare.html

20. Маниш Бхуптани, Шахрам Морадпур. RFID-технологии на службе вашего бизнеса, RFID Field Guide: Deploying Radio Frequency Identification Systems / Троицкий Н.. — Москва: «Альпина Паблишер», 2007.

21. ГОСТ Р ИСО/МЭК 14443-4-2014 Карты идентификационные. Карты на интегральных схемах бесконтактные. Карты близкого действия.