МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
РОСТОВСКИЙ ГОСУДАРСТВЕННЫЙ ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ (РИНХ)

Факультет Компьютерных технологий и информационной безопасности

Кафедра Информационных технологий и защиты информации

ДОПУСТИТЬ К ЗАЩИТЕ
Зав. кафедрой ИТ и ЗИ
к.э.н., доцент
Ефимова Е. В.
«____» _____ 2020г.

ВЫПУСКНАЯ КВАЛИФИКАЦИОНАЯ РАБОТА
на тему:
«Методы анализа эффективности системы многофакторной аутентификации на примере РГЭУ(РИНХ)»

Выполнила
студентка группы ИБ-341 А.С. Гурикова
Направление 10.03.01 «Информационная безопасность»

Руководитель выпускной
квалификационной работы
д.э.н., профессор Е.Н. Тищенко

ФГБОУ ВО «РОСТОВСКИЙ ГОСУДАРСТВЕННЫЙ ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ (РИНХ)»

Факультет Компьютерных технологий и информационной безопасности
Кафедра Информационных технологий и защиты информации

«УТВЕРЖДАЮ»
Зав. кафедрой ИТ и ЗИ
к.э.н., доцент
Ефимова Е.В.
«___» _____ 2020 г.

ЗАДАНИЕ

на выполнение выпускной квалификационной работы

Обучающейся Гуриковой Анастасии Сергеевны группы ИБ-341

1. Тема ВКР: «Методы анализа эффективности системы многофакторной аутентификации на примере РГЭУ(РИНХ)» Утверждена приказом по РГЭУ № _____ от _____
2. Срок сдачи студентом законченной ВКР на кафедру «___» _____2020 года
3. Исходные данные для ВКР: РГЭУ(РИНХ), г. Ростов-на-Дону, ул. Большая Садовая 69.
4. Содержание выпускной квалификационной работы по разделам:
   4.1. Анализ организации доступа в РГЭУ(РИНХ)
   4.2. Методы биометрической аутентификации
   4.3. Эффективность многофакторной аутентификации

Дата выдачи задания
«___»_____2020г.

Руководитель ВКР _____ _____
подпись ФИО

Задание к исполнению принял _____
_____
подпись ФИО

Реферат

Выпускная квалификационная работа содержит 78 с., 15 рис., 25 табл., 34 источника.

СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, АУТЕНТИФИКАЦИЯ И ИДЕНТИФИКАЦИЯ, БИОМЕТРИЧЕСКАЯ АУТЕНТИФИКАЦИЯ, ЭФФЕКТИВНОСТЬ МЕТОДОВ МНОГОФАКТОРНОЙ АУТЕНТИФИКАЦИИ, СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

Объектом исследования является ФГБОУ ВО «РГЭУ (РИНХ)»

Целью данной работы является исследование эффективности использования методов многофакторной аутентификации для повышения эффективности существующей в РГЭУ (РИНХ) системы управления и контроля доступом.

Используемые методы и средства: метод расчета совокупной стоимости владения СЗИ, метод экспертных оценок, метод моделирования оценок эффективности мероприятий информационной безопасности при воздействии случайных факторов окружающей среды, система СИМ-UML, сканер отпечатков пальцев Fingkey Hamster, считыватель радужной оболочки BM-ET200.

Основные результаты: расчеты эффективности методов многофакторной аутентификации, которые включают в себя расчеты затрат от внедрения методов аутентификации по

отпечаткам пальцев и по радужной оболочке глаза, а также степень повышения защищенности системы контроля и управления доступом от их внедрения.

Результаты исследования приняты к сведению руководством управления компьютеризации учебной и административной деятельности РГЭУ (РИНХ).

СОДЕРЖАНИЕ

Список используемых сокращений

CASIA - Chinese Academy of Sciences Institute of Automation;

АРМ – автоматизированное рабочее место;

ЗИ – защита информации;

ЗК – закрытый ключ;

ИС – информационная система;

ИСПДн - информационная система персональных данных;

КЗ – контролируемая зона;

КПП – контрольно-пропускной пункт;

КСЗИ – комплексная система защиты информации;

НСД – несанкционированный допуск;

ОК – открытый ключ;

ОД – объект доступа;

ПДн – персональные данные;

СД – субъект доступа;

СЗИ – система защиты информации;

СКУД – система контроля и управления доступом;

ССВ – совокупная стоимость владения;

ФСТЭК – федеральная служба технического и экспортного контроля;

ЭВМ – электронно-вычислительная машина.

ВВЕДЕНИЕ

В период активного развития и использования информационных технологий практически во всех сферах деятельности человека, в том числе и в образовательную сферу (школы, средние учебные заведения, высшие учебные заведения); значительном увеличении объемов информации, обрабатываемой в информационных системах; сосредоточении информации различного уровня секретности и принадлежности в единых базах данных; расширении круга лиц, имеющих доступ к техническим средствам обработки информации; повышении возможности доступа ко всем видам информации и создании предпосылок к ведению компьютерной разведки важнейшей задачей является обеспечение информационной безопасности.

Современные образовательные учреждения имеют сложную организационную структуру, многоаспектность функционирования, высокую техническую оснащенность, высокую концентрацию в автоматизированных системах и ресурсах, территориальную разрозненность, накопление больших объемов информации на носителях, интеграцию в единые базы данных информации различного назначения и различной принадлежности, интенсивное взаимодействие между компонентами информационных систем, в том числе и удаленных друг от друга.

Таким образом, они представляют собой совокупность взаимосвязанных между собой различных элементов, то есть систему, в рамках которой обязательно должна осуществляться защита информации. Существует множество принципов. На основе которых строятся системы защиты информации. В данной ВКР большее внимание будет уделено двум принципам организации защиты информации:

- комплексность, то есть согласованное применение разнородных средств;
- принцип экономической эффективности, то есть получение максимума возможных благ от имеющихся ресурсов.

Одной из составляющих комплексной системы защиты информации (КСЗИ) является система контроля и управления доступом (СКУД), в задачу которой входит управление доступом, а именно контроль и ограничение доступа на заданную территорию и идентификация лица, имеющего доступ на заданную территорию.

Базовой частью любой СКУД является идентификация и аутентификация пользователей. Существуют различные методы аутентификации: по паролю, по электронным картам, по e-token, с помощью sms.

Одним из высокоперспективных направлений по идентификации и аутентификации является применение систем распознавания по биометрическим характеристикам человека. Такие системы позволяют повысить надежность защиты информации, автоматизировать процессы обеспечения доступа к защищаемым объектам на основе разработанных методов идентификации и аутентификации личности, соответствующих международным и отечественным стандартам.

В данной работе будет рассмотрена СКУД ФГБОУ ВО «РГЭУ (РИНХ)» с целью ее усовершенствования. Повысить ее эффективность возможно с помощью использования нескольких факторов аутентификации. Федеральная служба технического и экспортного контроля (ФСТЭК) рекомендует пользователям использовать вместо аутентификации на основе статических паролей многофакторную аутентификацию.

Многофакторная аутентификация основана на совместном использовании нескольких факторов аутентификации (знаний, средств или объектов хранения), что значительно повышает безопасность использования информации со стороны пользователей, подключающихся к информационным системам по защищенным и незащищенным каналам коммуникаций.

Одновременное использование нескольких факторов вместе уменьшает вероятность НСД и повышает вероятность защиты информации. В качестве одного из факторов можно использовать также биометрический показатель.

Таким образом, целью данной работы является исследование эффективности использования методов многофакторной аутентификации в РГЭУ (РИНХ).

Для достижения данной цели необходимо:

- изучить структуру РГЭУ (РИНХ);
- изучить возможные угрозы и способы защиты от них;
- изучить особенности СКУД РГЭУ (РИНХ);
- проанализировать существующие методы аутентификации, биометрические методы аутентификации;
- оценить эффективность системы защиты информации с точки зрения степени снижения потенциального ущерба от воздействия угроз безопасности применением СЗИ, биометрических систем и затраченных на систему защиты средств;
- выработать обоснованные рекомендации по обеспечению информационной безопасности и на практике оценить эффективность мероприятий по защите информации.

1 АНАЛИЗ ОРГАНИЗАЦИИ ДОСТУПА В РГЭУ (РИНХ)

1.1 Общие сведения о структуре РГЭУ (РИНХ)

Федеральное Государственное Бюджетное Образовательное Учреждение Высшего Образования «Ростовский Государственный Экономический Университет (РИНХ)» осуществляет свою деятельность с 28.02.1931 г. Его учебные корпуса расположены в самом центре г. Ростова-на-Дону по следующим адресам: главный учебный корпус – улица Большая Садовая, 69, учебный корпус факультета Менеджмента и предпринимательства (МиП) – ул. Островского, 62, учебный корпус Юридического факультета (ЮФ) – ул. М.Горького,166.

В состав РГЭУ (РИНХ) входят следующие структурные подразделения: институт магистратуры (ИМ), 7 факультетов, 40 кафедр, 9 филиалов, финансово-экономический колледж (ФЭК), бизнес-школа (БШ), научно-исследовательский институт (НИИ), малое инновационное предприятие, медиацентр (МЦ), издательско-полиграфический комплекс, 2 спортивно-оздоровительных лагеря.

В главном учебном корпусе имеется два входа:

- основной организован со стороны проспекта Ворошиловский,
- дополнительный - со стороны улицы Большая Садовая.

В ВУЗе также имеются 12 запасных выходов:

- на улице Большая Садовая - один,
- на проспекте Ворошиловский - два,
- на улице Суворова - три, во двор - шесть.

Для обеспечения безопасности персонала и студентов в ВУЗе реализуется следующий комплекс мер:

- поддерживается в эксплуатационном состоянии вся система жизнеобеспечения объектов, в том числе по водо-, тепло-, энергообеспечению;

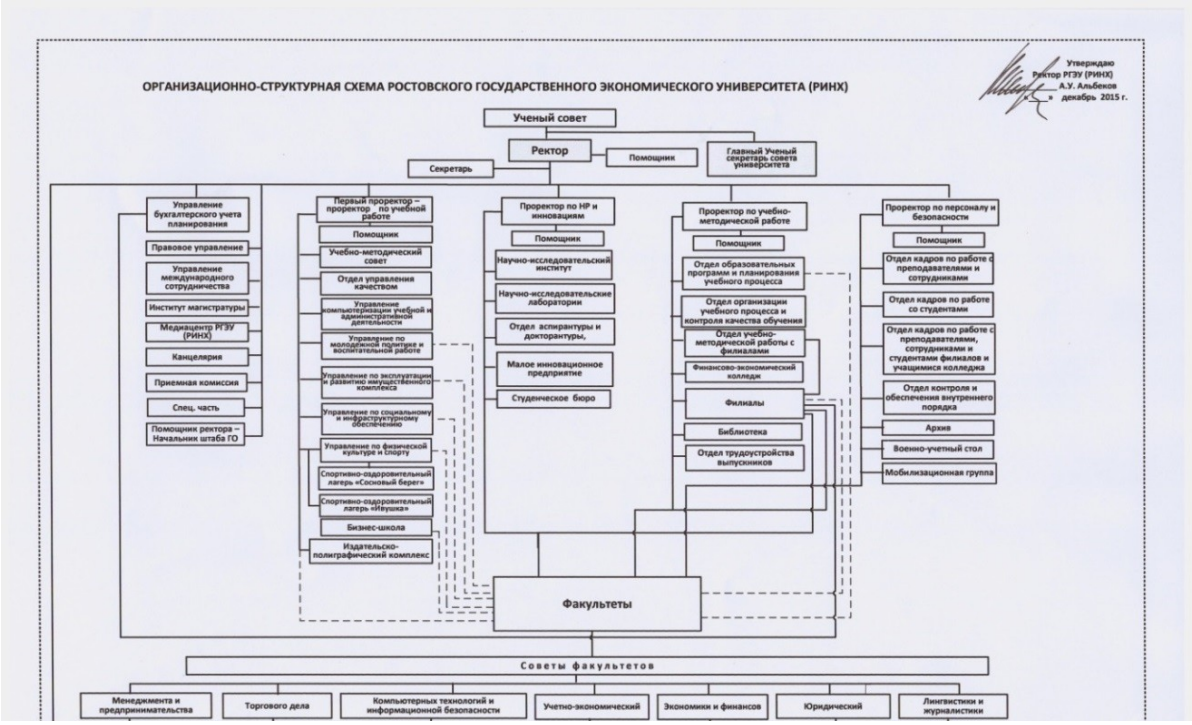
- обеспечивается контролируемый допуск работников, персонала, студентов и посетителей в корпуса ВУЗа и внос на его территорию различных материалов, оборудования и т. д.;
- ведется круглосуточный видеоконтроль территории объектов, периметра и внутренних помещений корпусов университета;
- установлены распашные решетки на окнах первого и второго этажей корпусов университета;
- корпуса университета оснащены системой пожарной сигнализации и средствами пожаротушения;
- все корпуса университета оборудованы системой речевого оповещения;
- работники, служебный персонал и студенты РГЭУ (РИНХ) проходят инструктаж по правилам пожарной безопасности, действиям при обнаружении задымления, возгорания, пожара;
- ежеквартально проводятся проверки подвалов, чердаков, кладовых, территории корпусов университета на предмет выявления горючих и взрывчатых веществ, оружия, боеприпасов, легко воспламеняющихся жидкостей;
- при каждодневных запланированных обходах территории объектов и всех зданий университета (поэтажно) контролируется соблюдение правил пожарной безопасности в структурных подразделениях ВУЗа и антитеррора.

Основные силы и средства, обеспечивающие безопасность персонала и студентов РГЭУ (РИНХ) [4]:

- отдел круглосуточного контроля и обеспечения внутреннего порядка университета;
- управление развития и эксплуатации имущественного комплекса университета:
- комиссия по ЧС и обеспечению пожарной безопасности;
- антитеррористический штаб;

- штаб гражданской обороны;
- добровольная пожарная дружина, присутствующая на каждом объекте ВУЗа;
- добровольные студенческие формирования гражданской обороны.

На рисунке 1.1 представлена организационная структура ФГБОУ ВО «РГЭУ (РИНХ)» [5].



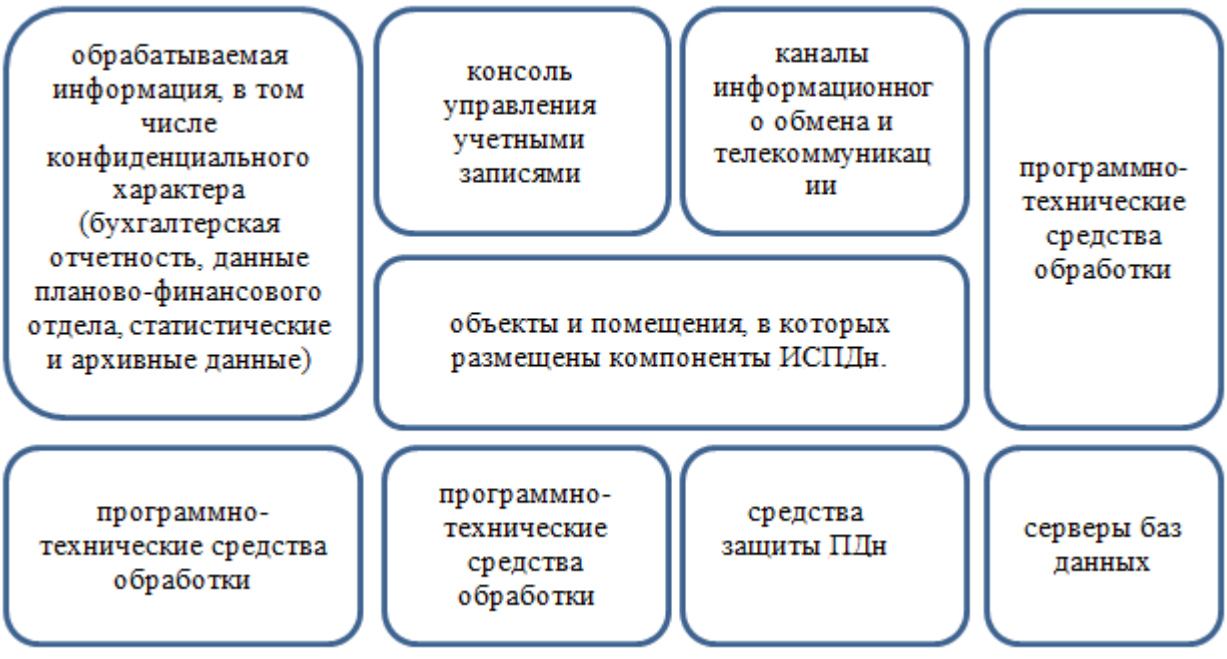


Рисунок 1.2 – Объекты защиты РГЭУ (РИНХ)

Таким образом, можно выделить следующие помещения, доступ к которым требуется ограничить: кабинет ректора, кабинеты проректоров, бухгалтерия, канцелярия, военно-учетный стол, спецчасть, правовое управление, управление компьютеризации учебной и административной деятельности, отдел кадров.

Основные категории пользователей ИС РГЭУ (РИНХ) представлены на рисунке 1.3.

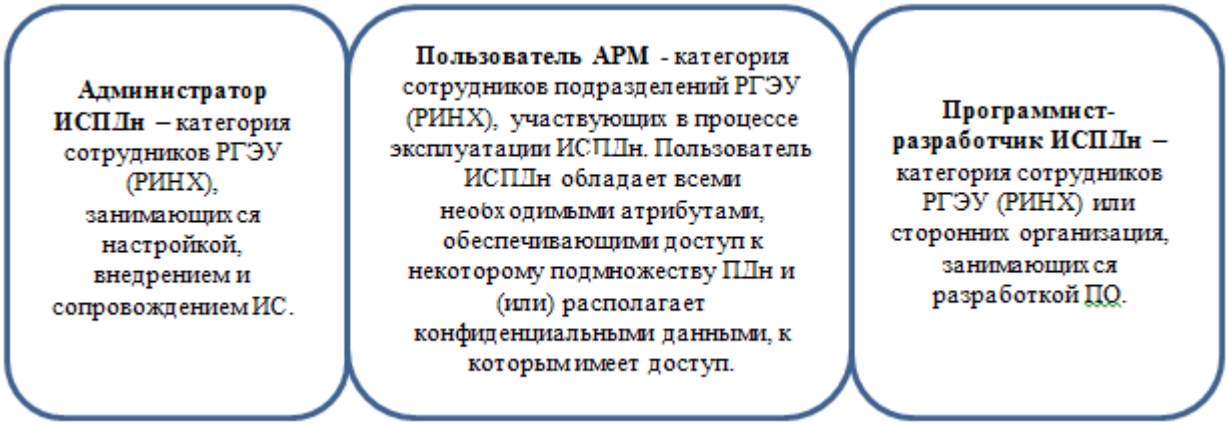


Рисунок 1.3 – Категории пользователей ИС РГЭУ (РИНХ)

Определим примерное количество пользователей университета, имеющих право допуска к помещениям: ректор, проректора, главный бухгалтер, сотрудники бухгалтерии, секретарь приемное ректора, начальник спецчасти, начальник правового управления, юрисконсульт, начальник управления компьютеризации учебной и административной деятельности, начальник отдела кадров, сотрудники отдела. Таким образом, примерно двадцать пять человек имеют допуск в упомянутые выше помещения.

1.2 Анализ угроз НСД к ИС РГЭУ (РИНХ)

Для анализа угроз безопасности к ИС РГЭУ (РИНХ) согласно Методическому документу «Меры ЗИ в ГИС» [6] необходимо оценить возможности (потенциал, оснащенность и мотивацию) внешних и внутренних нарушителей, провести анализ возможных уязвимостей ИС, возможных способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).

На рисунке 1.4 представлены источники угроз НСД в ИС в соответствии с действующей базовой моделью угроз [7]:

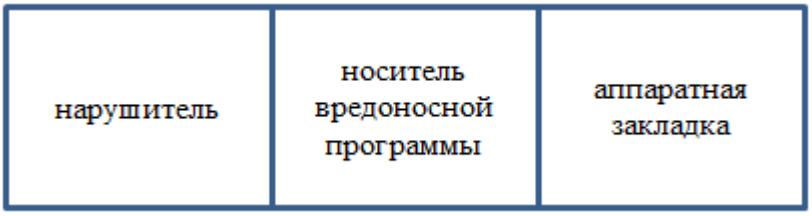


Рисунок 1.4 – Источники угроз НСД в ИС РГЭУ(РИНХ)

По наличию права постоянного или разового доступа в КЗ возможные злоумышленники подразделяются на два больших типа: внешние и внутренние нарушители.

Внешние нарушители - лица, не имеющие доступа к ИС, реализующие угрозы из внешних сетей связи общего пользования и/или сетей международного информационного обмена,

Внутренние нарушители - лица, имеющие доступ к ИС, включая пользователей ИС, реализующие угрозы непосредственно в самой ИС.

Внешними нарушителями могут быть: разведывательные службы иностранных государств; различные криминальные структуры; конкурирующие организации; недобросовестные партнеры; внешние субъекты (физические лица).

Внешний нарушитель имеет возможность осуществлять следующие действия:

- осуществлять НСД к каналам связи, выходящим за пределы служебных помещений, в которых обрабатывается информация конфиденциального характера;
- осуществлять НСД через АРМ, подключенные к сетям связи общего пользования и/или сетям международного информационного обмена;

- осуществлять НСД к информации с использованием специализированных программных воздействий (программные вирусы, вредоносные программы, алгоритмические или программные закладки);
- осуществлять НСД через элементы информационной инфраструктуры ИС, которые в процессе своего жизненного цикла (ЖЦ) (организация, модернизация, сопровождение, ремонт, утилизация) оказываются за пределами КЗ;

Лица, имеющие санкционированный доступ к ИС, но не имеющие доступа к информации. Это должностные лица, обеспечивающие нормальное функционирование ИС
Зарегистрированные пользователи ИС, осуществляющие ограниченный доступ к ресурсам ИС с АРМ. Доступ, аутентификация и права по доступу к некоторому подмножеству ПДн должны регламентироваться соответствующими правилами разграничения доступа.
Зарегистрированные пользователи ИС, осуществляющие удаленный доступ к ПДн по локальным и (или) распределенным ИС
Зарегистрированные пользователи ИС с полномочиями администратора безопасности сегмента (фрагмента) ИС
Зарегистрированные пользователи с полномочиями системного администратора ИС
Зарегистрированные пользователи с полномочиями администратора безопасности ИС
Программисты-разработчики (поставщики) прикладного ПО и лица, обеспечивающие его сопровождение на защищаемом объекте. Программисты-разработчики (поставщики) прикладного ПО и лица, обеспечивающие его сопровождение на защищаемом объекте
Разработчики и лица, обеспечивающие поставку, сопровождение и ремонт ТС на ИС.

Рисунок 1.5 – Восемь категорий внутренних нарушителей

При оценке возможностей реализации угроз безопасности необходимо учитывать указанные выше категории нарушителей.

Таким образом, можно сделать вывод об источниках возможных угроз безопасности информации в РГЭУ (РИНХ). Ими могут являться:

- оснащенные компьютерами учебные аудитории, в которых проходит непосредственно сам учебный процесс (лабораторные занятия, практики);
- Интернет – открытая сеть;
- автоматизированные рабочие станции в сфере ИБ работников ВУЗа, не обладающих достаточными компетенциями в области ИБ и умышленно или неумышленно нарушающие ИБ;
- внешние и внутренние нарушители.

1.3 Анализ способов защиты от НСД

Для обеспечения необходимого уровня защищенности информации в ИС РГЭУ (РИНХ) следует применять в комплексе

различные меры ЗИ, методы и средства безопасности: правовые, морально-этические, организационные, физические, технические (сочетают в себе аппаратные и программные меры ЗИ).

Правовые меры ЗИ – комплекс гражданско-правовых и уголовно-правовых норм, регулирующих общественные отношения в сфере использования компьютерной информации и устанавливающих ответственность за несанкционированное использование данных программных средств Правовые меры являются сдерживающим фактором для потенциальных злоумышленников.

Морально-этические мерам ЗИ – нормы поведения пользователей (пользователей ЭВМ, а также любых других сотрудников и персонала, не имеющих доступа к ЭВМ), складывающиеся на протяжении длительного времени, в процессе распространения ЭВМ в стране или мировом сообществе.

Организационные меры ЗИ – меры, носящие организационный характер, или методы, связанные с грамотной организацией режима допуска к секретам и контроля за секретоносителями на предприятии. Организационные методы делятся на режимные и специальные. Это меры, определяющие этапы и процессы функционирования ИСПДн, использование существующих ресурсов и возможностей ИСПДн, порядок деятельности работников и обслуживающего персонала, а также определяющие порядок взаимодействия пользователей с ИСПДн в таком виде, чтобы в наибольшей степени затруднить или полностью исключить возможность реализации угроз безопасности информации (УБИ) или значительно сократить величину потерь в случае их реализации.

Физические меры ЗИ основаны на применении механических, электро- или электронно-механических устройств, специально предназначенных для создания физических препятствий на пути движения потенциального нарушителя либо его доступа к компонентам системы и защищаемой информации, а также ТС визуального наблюдения, связи и охранной сигнализации. Это

могут быть системы ограждения и физической изоляции, системы контроля доступа, а также запирающие устройства и хранилища.

Физическая защиты корпусов, помещений, объектов и средств информатизации должна осуществляться установлением соответствующих постов охраны - рубежей защиты, с помощью ТС охраны либо иными способами, предотвращающими, существенно затрудняющими или полностью исключающими проникновение в помещения посторонних лиц, злоумышленников, хищение носителей информации, самих средств информатизации, исключающими нахождение внутри КЗ ТС разведки (видеокамер, подслушивающих устройств)

Технические меры ЗИ основаны на использовании различных электронных устройств и специальных программ, входящих в состав ИСПДн и выполняющих функции защиты.

Рисунок 1.6 – Состав системы защиты информации

Проанализировав СКУД РГЭУ (РИНХ) можно сделать следующие выводы: вход в университет осуществляется по бумажным или электронным пропускам (постоянным – для сотрудников и студентов; временным – для внешних субъектов) через контрольно-пропускной пункт (КПП), оборудованный турникетами. На КПП постоянно дежурят охранники.

Также в РГЭУ (РИНХ) установлены системы видеонаблюдения и пожарной сигнализации, системы речевого оповещения.

В Ростовском Государственном Экономическом Университете (РИНХ) имеются аттестованные помещения, имеющие аттестат соответствия. Данные помещения оборудованы шумогенераторами, датчиками против съема акустической информации в виде вибраций со стекол, имеют двойные двери с двойными стеклами.

Аудитории, оборудованные компьютерами и специальной дорогостоящей аппаратурой, а также помещения, в которых обрабатывается конфиденциальная информация (бухгалтерия, приемная ректора) по завершении в них работ закрываются на ключ и ставятся на сигнализацию охранниками КПП у главного входа под ответственность сотрудников, обладающими полномочиями ставить и снимать сигнализацию.

Таким образом, в РГЭУ (РИНХ) реализованы все необходимые меры ЗИ: технические, физические, организационные, морально-этические и правовые.

1.4 Анализ системы контроля и управления доступом в РГЭУ (РИНХ)

Система контроля и управления доступом (СКУД) в общем виде определяется как совокупность средств контроля и управления доступом, обладающих технической, информационной, программной и эксплуатационной совместимостью [8].

Основной задачей любой СКУД является управление доступом, а именно ограничение доступа на заданную территорию и идентификация лица, имеющего доступ на заданную территорию.

Дополнительными задачами СКУД являются:

- учёт рабочего времени;
- расчет заработной платы;
- ведение БД персонала, посетителей;
- интеграция с системой безопасности (системой видеонаблюдения, охранной сигнализации, пожарной сигнализации):

Основные элементы СКУД в общем виде представлены на рисунке 1.7.

Рисунок 1.7 – Элементы СКУД

В СКУД используются различные преграждающие устройства, устанавливаемые на дверях (электрозащелки, электромагнитные замки, электромеханические замки), на проходах/проездах (турникеты, шлюзовые кабины, ворота и шлагбаумы).

Базовым элементом СКУД являются идентификаторы. Они хранят код, необходимый при определения прав владельца: карточки, брелки, метки. В качестве идентификатора может выступать код, вводимый на клавиатуре, а также отдельные биометрические характеристики человека — отпечаток пальца, рисунок сетчатки или радужной оболочки глаза, трехмерное изображение лица.

Контроллер является основным элементом СКУД, содержит коды идентификаторов со списком прав доступа каждого владельца и определяет, пропустить его или нет. Когда человек предъявляет считывателю идентификатор, считанный из него код сравнивается с хранящимся кодом в БД, на основании чего принимается решение о допуске или не допуске пользователя.

Считыватель с увеличенной дальностью считывания - устройство, являющееся связующим звеном между контроллером и идентификатором. Он передает код идентификатора в контроллер. Вид считывателя зависит от самого идентификатора: для идентификатора в виде «таблетки» считывателем является два электрических контакта, для карты — электронная плата с антенной в корпусе, для считывания биометрической характеристики, на пример, рисунка сетчатки или радужки глаза считыватель должен включать телевизионную камеру.

При необходимости установить считыватель на улице (ворота, наружная дверь корпусов, проезд на территорию автостоянки) важно учитывать климатические условия — перепады температур, осадки — это наиболее важно для объектов в районах с суровыми климатическими условиями. Отдельно можно выделить считыватели для дальней идентификации объектов (с расстоянием идентификации до 50 м.). Такие системы удобны на автомобильных проездах, парковках, на въездах на платные дороги и т. п. Иде

нтификаторы (метки) для таких считывателей, как правило, а ктивные (содержат встроенную батарейку).

Конверторы среды служат для подключения аппаратных модулей СКУД друг к другу и к ПК. Некоторые контроллеры СКУД уже имеют встроенный интерфейс Ethernet, позволяющий без использования каких-либо дополнительных устройств подключа ться к ПК и связываться друг с другом.

Вспомогательное оборудование: блоки бесперебойного пита ния, дверные доводчики, датчики, кнопки, провода, видеонаблюде ние и т.д.

Программное обеспечение: не является обязательным элеме нтом СКУД, используется в случае, когда требуется обработка информации о проходах, построение отчетов либо когда для нача льного программирования, управления и сбора информации в процессе работы СКУД необходимо сетевое ПО, устанавливаемое на один или несколько ПК, соединенных в единую сеть.

Все СКУД можно отнести к двум большим классам: сетевые системы и автономные системы [9].

Сетевые системы

Подход, в котором все контроллеры соединены с главным компьютером, привносит множество преимуществ в сетевые систе мы, в особенности в деятельность крупных предприятий. Данные СКУД удобнее для больших объектов (офисы, производственные предприятия), так как осуществлять контроль доступа в а втономных СКУД с несколькими рубежами достаточно трудно. Се тевые системы применяются в следующих случаях:

- когда учреждению требуется вести архив произошедших ранее событий, либо когда необходим дополнительный контроль в ре жиме реального времени. Например, в сетевой СКУД имеется функция фотоверификации: на КПП при поднесении входящим человеком идентификатора к считывателю, служащий охра нного отдела может на экране монитора видеть фотографию че ловека, которому в БД присвоен данный идентификатор, и сра

внить с внешностью проходящего, что способствует предотвращению передачи карточек посторонним людям;

- когда требуется организовать учёт рабочего времени и контроль трудовой дисциплины;
- когда требуется обеспечить взаимодействие (интеграцию) с другими подсистемами безопасности, например, видеонаблюдением или пожарной сигнализацией).

Особенностью сетевых систем является возможность централизованного управления правами пользователей, ведения БД и контроля событий на всей охраняемой территории из одной точки. Сетевые системы также позволяют организовать несколько рабочих мест, разделив функции управления между разными сотрудниками и службами предприятия.

В случае, если нет возможности проложить проводные коммуникации между объектами, в сетевых СКУД могут применяться беспроводные технологии, Также беспроводные сети используются в случае сокращения финансовых затрат на монтаж точки прохода.

Автономные системы

Важным преимуществом автономных систем перед сетевыми является их дешевизна и простота в эксплуатации, они не требуют прокладки сотен метров кабеля, использования устройств сопряжения с компьютером, самого компьютера. К минусам таких систем относятся невозможность создавать отчеты, вести учёт рабочего времени, передавать и обобщать информацию о событиях, управлять СКУД дистанционно. При выборе автономной системы с высокими требованиями по безопасности рекомендуется обратить внимание на следующее:

Считыватель должен быть отделен от контроллера, чтобы провода, по которым возможно открывание замка, были не доступны снаружи.

Контроллер должен иметь резервный источник питания на случай отключения электропитания.

В составе автономной СКУД используются электронные замки, передающие информацию по беспроводным каналам связи: в двери устанавливается механический замок с электронным управлением и встроенным считывателем. Замок по радиоканалу связан с хабом, который уже по проводам обменивается информацией с рабочей станцией, на которой установлено специализированное ПО.

Для автономной СКУД возможно использовать «обратный метод», когда на контрольных точках устанавливаются идентификаторы, а работники и обслуживающий персонал отмечаются считывателем-контроллером, после чего полученные данные передаются при первой возможности — появление связи у считывателя.

Одним из основных направлений СКУД является идентификация и аутентификация субъектов доступа и объектов доступа.

К основным программно-техническим методам реализации идентификации и аутентификации (рисунок 1.8) относят [10]:

пароли	хеш-функции	шифрование с открытым ключом	сервер аутентификации Kerberos	биометрия	идентификационные карты и электронные ключи

Рисунок 1.8 – Программно-технические методы реализации идентификации и аутентификации

В таблице 1.1 приведены основные сведения о каждом методе идентификации и аутентификации, его слабые и сильные стороны.

Таблица 1.1 – Методы идентификации и аутентификации

Метод	Описание метода	Достоинства метода	Недостатки метода
1	**2**	**3**	**4**
Парольная идентификация	Введенный пользователем пароль сравнивается с паролем, имеющимся в	Простота и привычность.	Использование слабых паролей, редкая смена паролей; Злоумышленник
Протокол идентификации	Хеш-функция – легко вычислимая функция, преобразующая исходное сообще	Система не хранит пароле й, что повышает ее защище нность.	Злоумышленник может перехва тить хэш-образ при его передаче для хранения в

Продолжение таблицы 1.1

1	2	3	4
Протокол идентификация	Наиболее известными являются протокол на основе алгоритмов RSA,	Используют необратимые или односторонние функции, обла	Не все необратимые функции могут использоваться в реальных криптосистемах.
Сервер аутентификация	Доверенная третья сторона (доверяют все субъекты в	При любых взаимодействиях не передаются ни	Протокол не способен отражать атаки типа «отказ в
Идентификация/аутентификация	Биометрические характеристики пользователя снимаются, обра	Обеспечивают почти 100 % идентификацию, решая	БД шаблонов может быть изменена злоумышленником;
Идентификационные	Наиболее распространенные разновидности карт и ключей:	Удобство, простота применения.	Высокая стоимость развертывания системы аутентификации.

Таким образом, можно сделать вывод о том, что любой метод аутентификации имеет как преимущества, так и недостатки. Наиболее важными показателями при выборе метода аутентификации являются цена внедрения и устойчивость к атакам со стороны злоумышленников, а также качество идентификации, то есть на сколько точно система распознает легитимного пользователя и отказывает в доступе нелегитимному.

ФСТЭК рекомендует пользователям использовать вместо аутентификации на основе статических паролей многофакторную аутентификацию, о чем в том числе указано в методическом документе «Меры ЗИ в ГИС».

Многофакторная аутентификация основана на совместном использовании нескольких факторов аутентификации (знаний – пароль, средств – электронная карта или объектов хранения – биологические характеристики человека), что значительно повышает безопасность использования информации со стороны пользователей, подключающихся к ИС по защищенным и незащищенным каналам коммуникаций, и уменьшает вероятность НСД со стороны злоумышленников.

В качестве факторов можно использовать сочетания таких факторов как пароль и отпечаток пальца, пароль и изображение радужной оболочки глаза, пароль и изображение сетчатки глаза, отпечаток пальца и изображение радужной оболочки глаза и другие факторы, а также пароль, отпечаток пальца и изображение радужной оболочки глаза или даже сочетание четырех факторов: проход через турникеты по электронной карте, парольная аутентификация, аутентификация по отпечатку пальца и аутентификация по радужной оболочке глаза.

Таким образом, биометрические характеристики человека широко используются в СКУД. Далее будут более подробно проанализированы методы биометрической идентификации и аутентификации, их особенности, преимущества и недостатки, процесс биометрической идентификации и аутентификации, возможные атаки на биометрические системы, а также способы борьбы с ними.

2 МЕТОДЫ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ

2.1 Биометрическая аутентификация

Биометрия определена в ГОСТе как автоматизированное ра спознавание личности, основанное на определении его поведенче ских и биологических (анатомических и физиологических) характе ристик [11].

Биометрическая система – автоматизированная система, в основе которой лежит процесс получения биометрического обра зца от конечного пользователя, извлечения биометрических да нных из биометрического образца, сравнения биометрических да нных с данными, имеющимися в одном или более шаблонах, выявления степени их схожести, а также отображения результа тов идентификации или верификации (успешно или неуспешно).

Идентификация/идентифицировать – процесс сравнения биометрического образца со всеми биометрическими шаблонами в БД (схема «один ко многим») с целью определения его соотве тствия какому-либо шаблону и соответствующей шаблону личности; биометрическая система, использующая схему сравне ния «один ко многим», направлена преимущественно на поиск личности в БД, а не на подтверждение личности (схож с термином «верификация», но отличается от него).

Верификация/верифицировать – процесс сравнения получе нного биометрического образца с определенным по условию контрольным биометрическим шаблоном зарегистрированного конечного пользователя с целью определения схожести (схож с те рмином «идентификация», но отличается от него).

В нашем случае определение термина верификация совпадае т с определением термина аутентификация. Далее речь будет идти именно об аутентификации пользователей.

Идентификация и аутентификация по любой биометрической системе проходит четыре основных стадии (рисунок 2.1) [12]:

- запись — биологический или поведенческий образец пользова теля запоминается системой;

- выделение — уникальная информация выносится из биологического образца и составляется биометрический образец пользователя;
- сравнение — сохранённый биометрический образец сравнивается с представленным при регистрации в БД;
- совпадение/несовпадение — биометрическая система принимает и выносит решение о совпадении или несовпадении биометрических образцов.

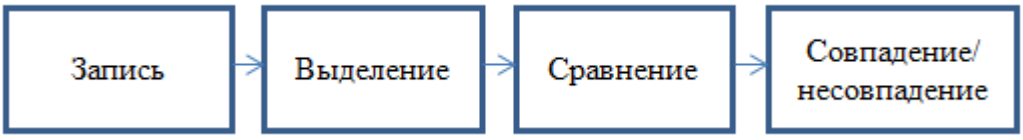


Рисунок 2.1 – Стадии биометрической идентификации

Обладая преимуществами перед обычными системами идентификации и аутентификации, биометрическая система все же является подверженной сбоям, связанным с естественными ограничениями и атаками злоумышленников.

Биометрическая система полагается на степень схожести двух биометрических образцов, а поскольку индивидуальные биометрические образцы, полученные в ходе регистрации и идентификации/аутентификации, редко идентичны, то биометрическая система может делать ошибки идентификации/аутентификации двух видов: ложное соответствие и ложное несоответствие.

Ложное несоответствие – два биометрических образца от одного и того же лица имеют малое сходство, и биометрическая система не может их сопоставить. Ложное несоответствие ведет к отказу в обслуживании легитимного пользователя.

Ложное соответствие – два биометрических образца от разных лиц имеют высокое сходство, и биометрическая система неверно объявляет их совпадающими. Ложное соответствие может привести к вторжению нарушителя.

Биометрическая система также может дать сбой в результате атакующих действий злоумышленников. Злоумышленник может обойти биометрическую систему, если принудит или вступит в

сговор с людьми, имеющими доступ к информации конфиденциа льного характера, либо воспользуется их халатностью (невыходом из системы после завершения транзакции или разглашение па роля), либо выполнит мошеннические манипуляции с процедурами регистрации и обработки исключений, которые изначально были разработаны для помощи авторизованным пользователям. Посре дством прямых атак на пользовательский интерфейс, на модули экстракции черт, на соединения между ними, на БД шаблонов вне шние злоумышленники также могут вызвать сбой в биометриче ской системе.

Примерами атак, направленных на системные модули, являются: трояны, атаки типа «человек посередине» и атаки воспроизведения. В связи с тем, что большинство видов прямых а так применимы и к системам идентификации/аутентификации по паролю, существует специальные контрмеры: криптографические преобразования, отметки времени и взаимной аутентификации. Эти меры способствуют предотвращению или значительной минимизации эффекта вторжений.

Наиболее серьезными уязвимостями являются атаки подде лки на пользовательский интерфейс и утечка из БД шаблонов. Упомянутые атаки оказывают негативное влияние на уровень за щищенности всей биометрической системы.

Атака подделки на пользовательский интерфейс заключается в предъявлении муляжа биометрической черты человека: слепок пальца из пластилина, снимок или маска лица или даже отреза нный палец легитимного пользователя. В случае успешной атаки нарушается базовое предположение о защищенности биометриче ской системы. Считается, что физическая привязанность биологической характеристики к живому пользователю позволяет системы иметь высокий уровень защищенности, несмотря на тот факт, что сами биометрические признаки не являются секретом (можно тайно получить фото лица легитимного пользователя или отпечаток его пальца с предмета или поверхности).

Утечка из базы шаблонов — это ситуация, когда информация о шаблоне легитимного пользователя становится доступной злоумышленнику.

2.2 Методы биометрической аутентификации

В настоящее время широко используется большое количество разнообразных методов биометрической аутентификации, которые можно в общем виде разделить на два класса [13]

1) Статические методы биометрической аутентификации основаны на физиологических характеристиках человека, присутствующих от его рождения и до самой смерти, находящиеся при нём в течение всей его жизни, и которые не могут быть поте ряны, украдены или скопированы (рисунок 2.2).

2) Динамические методы биометрической аутентификации основываются на поведенческих характеристиках человека, то е сть на характерных для него подсознательных движений в проце ссе воспроизведения или повторения какого-либо обыденного де йствия (рисунок 2.3).

Статические методы	По отпечатку пальца	По радужной оболочке глаза	По сетчатке глаза
	По геометрии руки	По геометрии лица	По термограмме лица

Рисунок 2.2 – Статические методы биометрической ауте нтификации

Аутентификация по отпечаткам пальцев является изве стным и широко распространенным методом биометрической ауте нтификации пользователей. Метод основан на использовании уникальности рисунка папиллярных узоров пальца человека. Для получения рисунка отпечатка пальца используется специальный сканер. Далее отпечаток преобразовывается в цифровой код, а за тем сравнивается с уже имеющимися наборами в БД эталонов. К преимуществам метода относятся легкость в использовании,

удобство и надежность, а также универсальность. Метод приме ним в совершенно любых сферах деятельности и для решения ра знообразных задач, начиная от получения доступа в помещение, заканчивая разблокировкой экрана смартфона.

Аутентификация по радужной оболочке глаза основана на испольщовании уникальности признаков и особенностей радужной оболочки человеческого глаза. Радужная оболочка – это передняя часть сосудистой оболочки, имеющая кругообразную форму и отве рстие внутри (зрачок). Радужная оболочка образовывается ещё до рождения человека и является неизменной в течение всей его жизни.

Аутентификация по сетчатке глаза основана на использова нии уникальности рисунка кровеносных сосудов глазного дна. Для сканирования сетчатки используется инфракрасное излучение низкой интенсивности, проходящее через зрачок к кровеносным сосудам на задней стенке глаза. Далее из полученного сигнала выделяется несколько сотен особых точек, информация о которых сохраняется в шаблоне. Метод требует достаточно чёткого изобра жения и чувствителен к неправильной ориентации сетчатки, что является его недостатком, так как пользователю необходимо смотреть очень аккуратно. Также метод чувствителен к таким за болеваниям как катаракта. Тем не менее метод обеспечивает одну из самых низких вероятностей ошибки первого рода (отказ в доступе для зарегистрированного пользователя) и почти нулевой процент ошибок второго рода, отчего получил большое распростра нение при доступе к сверхсекретным объектам [14].

Аутентификация по геометрии руки основана на использова нии в совокупности нескольких параметров формы кисти руки (изгибы пальцев, длина и толщина пальцев, ширина и толщина тыльной стороны руки, расстояние между суставами и структура кости, а также мелкие детали, как морщины на коже), так как не все параметры руки являются уникальными. К недостаткам ме тода можно отнести его чувствительность к возможному распуха нию тканей или ушибам руки, что может исказить исходную

структуру. Для создания 3D-образа кисти руки используется скане р, состоящий из камеры и подсвечивающих диодов (при сканирова нии, диоды включаются по очереди, это позволяет получить ра зличные проекции руки). Надежность аутентификации по геоме трии руки можно сравнить с аутентификацией по отпечатку па льца [14].

Аутентификация по геометрии лица. Широкое использова ние мультимедийных технологий, с помощью которых можно увиде ть достаточное количество видеокамер на вокзалах, аэропортах, площадях, улицах, дорогах и других местах скопления людей, ста ло решающим в развитии этого направлении. С технической стороны метод представляет собой сложную математическую зада чу. При построении трехмерной модели человеческого лица выде ляются контуры различных элементов лица (бровей, губ, глаз, носа), затем вычисляется расстояние между ними, и создается 3D-модель. Для определения уникального шаблона, соответствующе го определенному человеку, необходимо от 12 до 40 характерных элементов. Шаблон должен учитывать множество вариаций изображения на случаи поворота лица, изменения освещённости, изменения выражения, наклона. Диапазон таких вариантов ва рьируется в зависимости от целей применения данного метода (для идентификации, аутентификации, удаленного поиска на достаточно обширных территориях и т. д.). Некоторые алгоритмы даже позволяют компенсировать наличие у человека очков, шляпы, усов и бороды [14].

Аутентификация по термограмме лица основана на использовании уникальности термограмм лица каждого человека. Для получения термограмм используются камеры инфракрасного диапазона. Преимуществом данного метода является возможность различать близнецов, а также высокая точность термограммы да же при использовании специальных масок, проведении пластиче ских операций, старении организма, повышении или понижении температуры тела. Но данный метод не имеет широкого ра спространения из-за невысокого качества аутентификации [14]

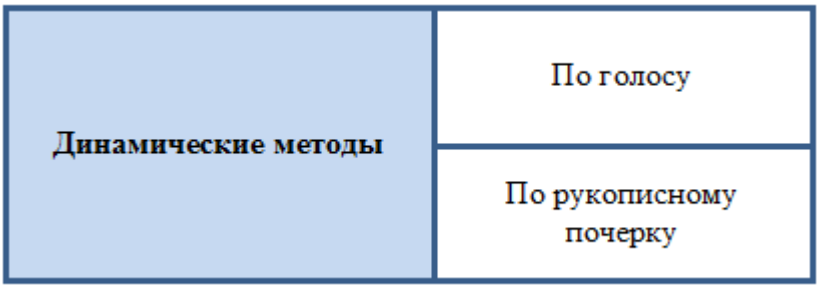


Рисунок 2.3 – Динамические методы биометрической аутентификации

Аутентификация по голосу. Данный метод активно развивается и находит применение в современных бизнес-центрах. К его преимуществам относятся простота в использовании, отсутствие необходимости дорогостоящей аппаратуры, достаточно микрофона и звуковой платы. Из всего множества способов построения шаблонов по голосу наиболее часто используются разные комбинации частотных и статистических характеристик голоса. Рассматриваются такие параметры, как модуляция, интонация, высота тона. Недостатком метода является его довольно низкая точность, связанная с возможными изменениями голоса (в зависимости от различных факторов: возраст, состояние здоровья, настроение) и шумовой составляющей. Также к недостаткам метода относится большая вероятность ошибок второго рода (порядка одного процента), поэтому метод применяется для управления доступом в помещениях со средним уровнем безопасности (компьютерные классы, лаборатории производственных компаний) [14].

Аутентификация по рукописному почерку основана на уникальности движений человеческой руки при письме. Для сохранения шаблона подписи применяются специальные ручки или сенсорные экраны, восприимчивые к давлению поверхности. Шаблон создается в зависимости от требуемого уровня защиты. Обработка данных о подписи осуществляется путем анализа росписи (анализируется степень совпадения двух картинок) или динамических характеристик написания, при этом для аутентификации строится

свертка, в которую входит информация по подписи, временными и статистическими характеристиками написания подписи.

Таким образом, существует большое количество разнообразных методов идентификации и аутентификации, каждый обладает как преимуществами, так и недостатками и внедряется в системы в зависимости от уровня секретности обрабатываемой информации и с учетом финансовых возможностей предприятий и учреждений, а также их конкретными потребностями. Два упомянутых выше статических методов идентификации и аутентификации: по отпечаткам пальцев и по радужной оболочке глаза далее рассмотрены более подробно, особенности их функционирования, преимущества и недостатки, а также возможные действия злоумышленников и способы борьбы с ними.

2.3 Методы аутентификации по радужной оболочке глаза и отпечаткам пальцев

2.3.1 Аутентификация по радужной оболочке глаза

На рисунках 2.4, 2.5 [15] представлена структура глазного яблока. Для изучения данного метода аутентификации рассмотрим радужную оболочку глаза, которая составляет переднюю часть сосудистой оболочки капсулы глазного яблока. При осмотре передней поверхности радужной оболочки она выглядит тонкой почти округлой пластинкой, лишь слегка эллиптической формы. У края зрачка на всем его протяжении отмечается чёрная зубчатая оторочка, окаймляющая его на всем протяжении и пре

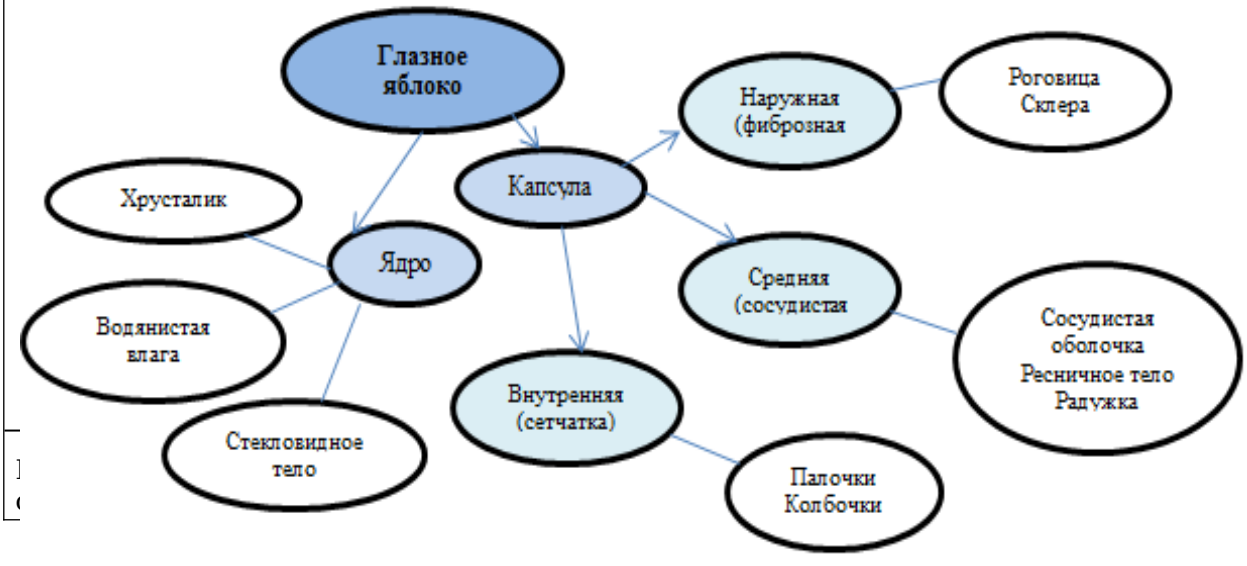


Рисунок 2.4 – Структура глазного яблока

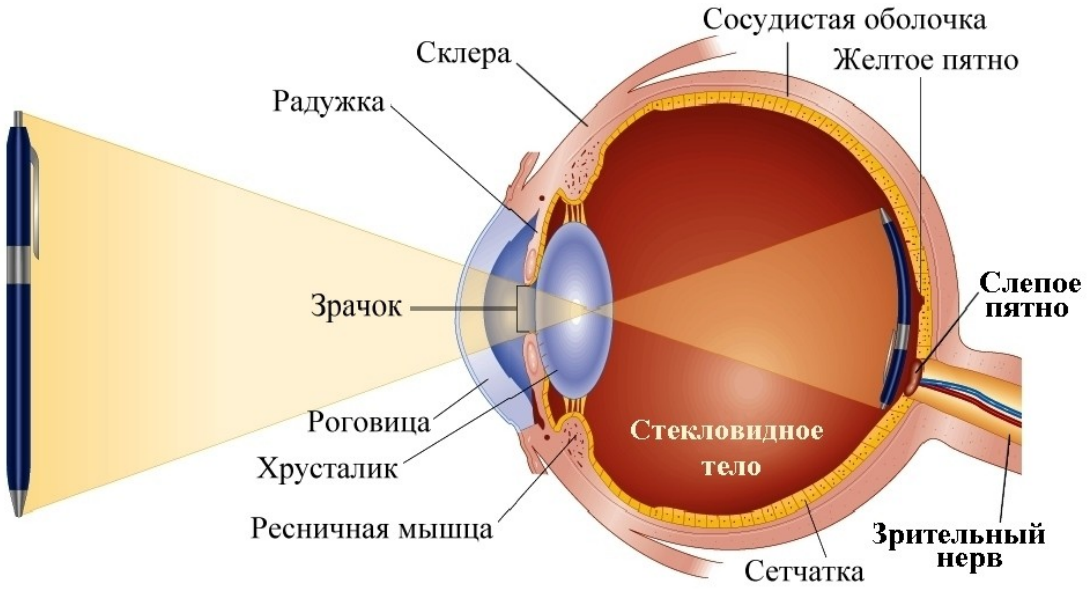


Рисунок 2.5 - Структура глазного яблока

В радужной оболочке различают два листка: передний и за дний.

Передний (мезодермальный, увеальный) – продолжение сосудистого тракта. Состоит из густого скопления клеток, ра

сположенных блихко друг к другу, параллельно поверхности ра дужной оболочки. Передний пограничный слой у края крипт пре рывается.

Задний (эктодермальный, ретинальный) – продолжение эмбриональной сетчатки, в стадии вторичного глазного пузыря, или глазного бокала. Из наружного слоя заднего пигментного листка в период эмбрионального развития формируются две мышцы радужной оболочки: сфинктер, сужающий зрачок, и дила татор, расширяющий зрачок.

Взаимодействие этих двух антагонистов позволяет радужной оболочке путём рефлекторного сужения и расширения зрачка ре гулировать поток проникающих внутрь глаза световых лучей, причём диаметр зрачка может изменяться от 2 мм до 8 мм [16].

Процесс идентификации и аутентификации по радужной оболочке глаза

Для получения изображения используются сканеры радужной оболочки. Также многие исследования ведутся на основе изобра жений, взятых из баз CASIA (Chinese Academy of Sciences Institute of Automation) [17], содержащих несколько разделов: CASIA-Iris-Interval, CASIA-Iris-Lamp, CASIA-Iris-Twins, CASIA-Iris-Distance, CA SIA-Iris-Thousand, CASIA-Iris-Syn. В таблице 2.1 представлено описание каждой из баз CASIA.

Таблица 2.1 – Краткое описание баз CASIA

Вид базы	Описание
CASIA-Iris-Interval.	Изображения получены в ближнем инфракрасном диапазоне с разрешением 320x280 пикселей. Спектр ближнего инфракрасного излучения выделяет особенности структуры радужки, облегча я последующие измерения в процессе идентификации.
CASIA-Iris-Lamp	Данные используется для изучения изме нения структуры радужной оболочки при изменении размеров зрачка. Изображе ния из этой БД содержат снимки с включённой и выключенной лампой с ра зрешением 640x480 пикселей.
CASIA-Iris-Twins	Используется для исследований индивидуальных особенностей строения радужки. БД содержит изображения ра

	дужных оболочек более 100 пар однояйцовых близнецов различного пола и возраста
CASIA-Iris-Distance	Используется для разработки методов идентификации, работающих на значительных расстояниях, и для разработки многопараметрических методов биоидентификации. Изображения получены с помощью камеры высокого разрешения (2352*1728) с расстояния 3 м.
CASIA-Iris-Thousand	Используется для изучения уникальных особенностей структуры радужки, проверки методов определения радужной оболочки и идентификации, а также для усовершенствования этих методов при условии наличия бликов, ношения очков и контактных линз. БД содержит изображения радужных оболочек более 1000 человек.
CASIA-Iris-Syn.	БД содержит синтезированные изображения радужной оболочки

Для получения качественного эталона важны условия регистрации изображения. Совокупность этих условий достаточно сложна и включает в себя следующие компоненты: освещённость (которая может быть недостаточной), наличие посторонних засветок (порождающих неравномерную освещённость области радужки), наличие спроецированных на радужку посторонних бликов (закрывающих и искажающих её рисунок), фокусировку, выдержку. Несоблюдение условий регистрации порождает дефекты изображений, часть из которых можно детектировать, численно оценить и затем отбраковать изображения со значительными дефектами

Выделение уникальной информации из образца происходит по следующей схеме [18]:

- Вначале осуществляется выделение зрачка, а именно его внешних границ. Для этого могут быть применены различные алгоритмы (например, алгоритм Канни).
- Очистка изображения – необходима для получения изображения, на котором ярко выделена область зрачка. Возможно использование различных фильтров: фильтр для

заливки круга, внутри границ зрачка; фильтр, отделяющий область соединённых пикселей сравнения областей светлых пикселей с областью ниже порога.

- После определения информации о зрачке происходит опре деление параметров радужки (радиус и границы радужки). Современные алгоритмы используют произвольные окружности для определения параметров радужки. Начина я от зрачка, эти алгоритмы перебирают потенциальные зна чения центра и радиуса радужки. Для определения границ радужки осуществляется пошаговое изменение яркости ра дужки в интересующей области. Эта область должна соотве тствовать компоненту с наивысшим значением на выходе фильтра выделения границ.
- Далее, имея оценки радиуса и центра радужки, производится развёртка изображения: переход от полярных координат в декартовы с нормировкой по радиусу для компе нсации линейного сжатия и растяжения радужки всле дствие изменений размеров зрачка.
- Далее находятся ключевые точки. Отличительные простра нственные характеристики радужки человека проявляются различно в различных масштабах. Например, отличите льный диапазон структур из общей формы радужной оболочки к распределению мелких крипт и детали те кстуры. Для захвата этого диапазона пространственных де талей предпочтительно использовать разложение предста вления на несколько масштабов.

К неправомерным действиям со стороны злоумышленника, позволяющим обойти систему идентификации и аутентификации, можно отнести следующие: предъявление фотографии (фотогра фий) глаза, предъявление модели, муляжа глаза, предъявление видеозаписи глаза, предъявление вырезанного глаза.

Предложены следующие способы борьбы, называемые также методами определения живости глаза:

- Изучение спектра отражения глаза. Спектр отражения живой влажной роговицы отличается от мертвой пересохше й, стекла или пластика модели. Однако, такой метод за щиты можно обойти, смачивая мёртвый глаз или покрыв модель слоем влажной белковой эмульсии (раствором жела тина).
- Исследование гиппуса/нистагма. Непроизвольные движе ния зрачка и глаза – хорошее доказательство его живости, но есть люди, у которых эти движения выражены очень сла бо или происходят редко (раз в несколько минут).
- Мигание случайно выбранных светодиодов осветителя в случайно выбранные моменты времени и проверка отраже ния осветителя на соответствующих кадрах видеопоследова тельности.
- Изучение реакции зрачка на световой стимул (поданный в случайный момент времени).

Для идентификации и аутентификации по радужной оболочке глаза используются сканеры радужной оболочки.

В РГЭУ (РИНХ) имеется считыватель радужной оболочки компании **Panasonic BM-ET200.** В таблице 2.2 представлены основные технические характеристики устройства [19].

Камера **BM-ET200** обеспечивает точный, быстрый бесконта ктный контроль доступа с использованием биометрической те хнологии идентификации личности по радужной оболочке глаза. Система может использоваться для идентификации пассажиров в аэропортах и для контроля доступа в различных отраслях промышленности.

Используются световой индикатор расстояния и голосовые команды для сообщения пользователю о правильном расстоянии для захвата изображения радужной оболочки глаз. Голосовое устройство на передней крышке также предоставляет голосовые команды для помощи при использовании и получении результатов идентификации. Имеется три режима работы голосовой подска

зки. Устройство позволяет просмотреть журнал доступа определе нного пользователя в определенное время.

Таблица 2.2 - Технические характеристики Panasonic BM-ET200

Показатель	Характеристика
1	2
Время идентификации	Приблизительно 0,3 секунды (после получе ния изображения радужной оболочки и до вывода результата идентификации) Приблизительно 5 секунд (Сертификация се рвера. После получения изображения ра дужной оболочки и до вывода результата идентификации)
Надёжность	коэффициент ошибочной идентификации 1 из 1,2 миллионов.
Расстояние для получе ния изображения глаза	30 - 40 см. между глазами и зеркалом
Макс. количество пользователей BM-E T200	Автономный режим: 50 пользователей ма ксимально Сетевой режим: 5025 пользователей ма ксимально 10025 пользователей максимально с доп. лицензией
Голосовые команды	14 поддерживаемых языков (английский, французский, немецкий,испанский, ита льянский, турецкий, арабский, китайский, корейский, русский, португальский, да тский, шведский и японский) Выбираемые режимы: Без оповещения, Простой (результат идентификации) и Полный (голосовая команда и результат идентификации)
Индикатор расстояния	Свет индикатора указывает необходимое расстояние между пользователем и основным блоком
Индикатор состояния	Мигающий, Вкл и Выкл на выбор
Угол поля зрения (каме	Горизонтальный: 115°

ра видеонаблюдения:BM-ETC202)	Вертикальный: 85° (фиксированный)
Функция безопасности	Выключатель обнаружения попыток несанкционированного вскрытия, шифрование данных системы идентификации
Источник питания	12В постоянного тока / 24В постоянного тока
Мощность	Максимально 24Вт
Интерфейс	Wiegand, RS-485
Сеть	10Base-T / 100 Base-TX
Сетевой протокол	TCP/IP
Устройство чтения карт	RWK400 (Изготовлено HID Corporation)

2.3.2 Аутентификация по отпечаткам пальцев

Данный метод отличает надежность, высокая практичность. Отпечатки пальцев у всех людей уникальны и не меняются в течение жизни, их невозможно потерять, забыть или украсть. Метод относят к статическим методам распознавания [20].

При распознавании происходит сравнение отпечатка пальца с ранее зарегистрированными шаблонами в БД. Функцию идентификации может выполнять установленный на входе считыватель отпечатков пальцев, подключенный к компьютеру датчик или встроенный сканер смартфона.

Наиболее часто система идентификации и аутентификации по отпечаткам пальцев является частью какой-либо другой системы контроля, например, системы запирания. В результате работы системы устанавливается личность человека, после чего система может выполнить нужные мероприятия (открыть замок, разрешить доступ пользователю к программе или разрешить загрузку компьютера).

Для получения сведений об отпечатках пальцев применяются специализированные сканеры. Известны три основных типа сканеров отпечатков пальцев: оптические, полупроводниковые, ультразвуковые.

В таблице 2.3 [21] данные три типа рассмотрены более подробно.

Таблица 2.3 – Типы сканеров отпечатков пальцев

Тип сканера	Особенности	Преимущества	Недостатки
Оптические (FTIR-сканеры, оптоволоконные, электрооптические, оптические протяжные, роликовые, бесконтактные)	Основаны на использовании оптических методов получения изображения	Высокое качество изображения, долговечность, экономичность, удобство и простота в использовании	Высокая стоимость
Полупроводниковые (емкостные, чувствительные к давлению, термо-сканеры, радиочастотные, протяжные термо-сканеры, емкостные протяжные, радиочастотные протяжные)	Основаны на использовании свойств полупроводников, изменяющихся в местах контакта гребней папиллярного узора с поверхностью сканера	Низкая стоимость	Неэффективная защита от муляжей Не устойчивая работа при плохом контакте пальца
Ультразвуковые	Сканирование ультразвуком и волнами и измерение расстояния между источником волн и впадинами и выступами на поверхности пальца по отраженному от них эху.	Высокое качество Высокая защита от муляжей	Высокая стоимость

Идентификация и аутентификации по отпечаткам пальцев основана на распознавании образа, когда папиллярные узоры сравниваются с зарегистрированными данными. Процесс идентификации и аутентификации выполняется в три этапа (рисунок 2.6).

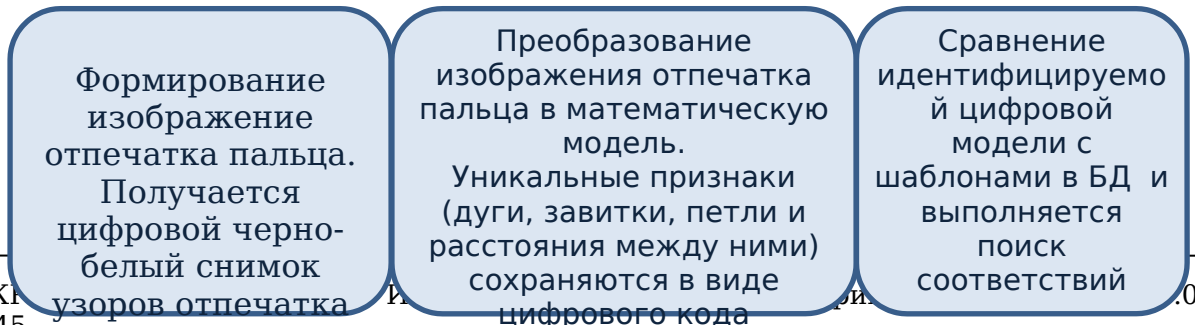


Рисунок 2.6 – Этапы идентификации и аутентификации по отпечаткам пальцев

К неправомерным действиям со стороны злоумышленника, позволяющим обойти систему идентификации и аутентификации, можно отнести следующие:

1. Конденсация (для оптических сканеров). При направлении на сканер струи тёплого воздуха, рисунок отпечатка пальца пре дыдущего пользователя восстанавливается.

2. Снятие отпечатка пальца скотчем имеет схожий с конденса цией принцип, наиболее вероятна для оптических сканеров.

3. Изготовление муляжа из жвачки, пластилина или другого вещества.

4. Метод «отрезанного пальца» имеет малую вероятность сра батывания, так как мертвые ткани быстро теряют свои свойства (меняется рисунок). Контрмерами против этого метода является использование сканеров, реагирующих на дополнительные призна ки "живого пальца" (температура, пульс и т.п.).

5. Использование клея, желатина и предмета, на котором оста лся отпечаток пальца.

Для снижения вероятности ложного допуска необходимо доба вление дополнительной проверки наличия температуры в прикла дываемом пальце, пульса.

В РГЭУ (РИНХ) имеются сканеры отпечатков пальцев Fingkey Hamster производителя NITGEN – оптический USB-сканер для отпечатков пальцев [22].

В таблице 2.4 [22, 23] приведены основные технические хара ктеристики данного сканера.

Таблица 2.4 – Технические характеристики сканера отпечатков па льцев Fingkey Hamster

Показатель	Характеристика

Тип интерфейса	USB
Внешний интерфейс соединения	USB1.1
Сенсор для распознавания отпечатка	оптический, OPP01
Разрешение	500 ppi
Размер устройства	25 x 41 x 68 mm (1.0" x 1.6" x 2.7")
Захват изображения	17 x 20 mm (0.7" x 0.8")
Мировые стандарты	SDK поддержка ISO BioAPI v2.0

Таким образом, в данной главе были проанализированы статистические и динамические методы биометрической аутентификации. Такие методы как аутентификация по отпечаткам пальцев и по радужной оболочке глаза были проанализированы более подробно. Был изучен процесс биометрической идентификации и аутентификации, а также возможные попытки злоумышленника осуществить НСД к системе. Было рассмотрено и изучено специализированное оборудование, необходимое для аутентификации по отпечаткам пальцев и по радужной оболочке глаза, а именно сканер отпечатков пальцев Fingkey Hamster и считыватель радужной оболочки Panasonic BM-ET200.

3 ЭФФЕКТИВНОСТЬ МНОГОФАКТОРНОЙ АУТЕНТИФИКАЦИИ

3.1 Методы оценки эффективности

Для проведения расчетов эффективности СЗИ от внедрения двух дополнительных факторов аутентификации в существующую СКУД РГЭУ (РИНХ) вначале определим, что будем подразумевать под эффективностью ЗИ.

Под эффективность ЗИ будем понимать степень соответствия результатов ЗИ цели ЗИ [24].

Требование по ЗИ – установленное правило или норма, которая должна быть выполнена при организации и осуществлении ЗИ, или допустимое значение показателя эффективности ЗИ.

Показатель эффективности ЗИ – мера или характеристика, необходимая для оценки эффективности ЗИ.

Норма эффективности ЗИ – значение показателя эффективности ЗИ, установленное нормативными и правовыми документами.

Эффективность СЗИ можно охарактеризовать, как способность системы противостоять несанкционированным действиям злоумышленника в рамках угрозы. Таким образом, эффективность СЗИ характеризует уровень защищенности объекта защиты.

Согласно ГОСТу эффективность СЗИ определяется сопоставлением результатов от функционирования СЗИ и затрат всех видов ресурсов, необходимых для ее создания, эксплуатации и модернизации [25].

Критерий эффективности определяют на множестве показателей, каждый из которых описывает одну из сторон рассматриваемой системы. Вид критерия (целевая функция или порядковая мера, устанавливающая упорядоченную последовательность сочетаний показателей) определяется от вида математического аппарата. Используемые показатели должны быть развернуты применительно к характеристикам конкретной СЗИ.

Для анализа эффективности СЗИ используются качественные и количественные методы. Качественные оценки не всегда могут дать полный ответ на вопрос об уровне надежности объекта, его защищенности. В таком случае эту проблему позволяют решить количественные методы. Для измерения уровня эффективности, для ее оценки необходимо иметь обоснованный критерий - показатель эффективности системы.

Можно выделить следующие виды критериев эффективности:

1. Критерии экономической эффективности. Позволяют оценивать достижение целей функционирования СЗИ при заданных затратах.

2. Критерии качества. Позволяют оценить качество СЗИ по заданным показателям и исключить те варианты, которые не удовлетворяют заданным ограничениям. При этом используются методы многокритериальной оптимизации, восстановления функций и функционалов, методы дискретного программирования.

3. Искусственно сконструированные критерии, позволяющие оценивать интегральный эффект (например, «линейная свертка» частных показателей, методы теории нечетких множеств).

Эффективность функционирования СЗИ зависит от множества действующих взаимосвязанных между собой элементов и, как правило, оценивается совокупностью критериев, находящихся в сложных, а порою даже конфликтных взаимоотношениях.

В настоящее время нет единого подхода к решению данной проблемы, отчего существует такое многообразие различных не взаимосвязанных между собой методов оценки качества СЗИ.

Процесс определения эффективности СЗИ начинают с выбора и обоснования показателей (критериев) оценки эффективности СЗИ, а затем переходят к подбору или разработке методик расчета этих показателей.

В таблице 3.1 приведены условные названия используемого подхода к выбору критериев и оценке параметров, показатели эффективности СЗИ и методики их расчета [26].

Таблица 3.1 – Подходы для оценки эффективности систем защиты

№	Подход	Показатели оценки эффективности	Способ расчета показателей
1	**2**	**3**	**4**
1	Статистический (statistical)	Угроза i-го типа возникает в среднем за период времени Ti.	Статистическая обработка потенциальных угроз и их последствий.
2	Вероятностный (probabilistic)	Суммарные средние потери $R=\sum_{i=1}^{2n}\sum_{j=1}^{2n} P(\mu/s)P(s)\Pi(\mu/s)+m$ P(μ/s) – вероятность устранения, P(s) – априорная вероятность состояния объекта контроля, П(μ/s) – потери принятия решения s при состоянии объекта s, m – количество распознаваемых угроз.	Определяется вероятность отказа системы от обработки данных в результате реализации угроз.

Продолжение таблицы 3.1

1	**2**	**3**	**4**
3	Частотный (frequency)	Ожидаемый ущерб от i-ой угрозы: $R_i = F(S,V)$ S – показатель частоты возникновения угрозы V – условный показатель ущерба	На основании анализа статистического материала задается значение S, величина V выбирается равной от 1 до max возможной суммы ущерба, рассчитывается значение показателя Ri как функции параметров V и S
4	Экспертное оценивание (e	Степень обеспечения безопасности SR системы S	Определяется количество и перечень параметров (i), характе

	xpert eva luation)	$SR = \frac{1}{n}WiGi$	ризующих СЗИ. Зада ются значения субъе ктивных коэффицие нтов важности (Wi) каждой из характе ристик Gi, назначе нные экспертным путем. Рассчитывае тся значение параме тра SR
5	Информа ционно-энтропийн ый (informa tional and entropic)	Величина информа ционной энтропии Ше ннона	Проводится ана литическое вычисле ние информационной энтропии системы, использую понятие свертки функции. При линейной за висимости эффе ктивность интегра ции подсистем в информационном пла не считают удовле творительной. В противном случае – неэффективной.
6	Нейросете вой подход (многокри териа льный) (ne ural ne twork)	Нечеткие показатели за щиты информационной системы в виде лингвистических переме нных, таких как «а бсолютно незащищенна я», «недостаточно за щищенная», «защищенна я», «достаточно защище нная», «абсолютно за щищенная»	Принадлежность определенного уровня безопасности определяется на промежутке [0,1], показатели наде жности являются функцией принадле жности, где – есть элемент множества X – требований бе зопасности, A – множество значений, определяющих выполнение требова ний безопасности. Оценка эффе ктивности производится по че тко определенным критериям.

Продолжение таблицы 3.1

1	2	3	4
7	Метод	Показатель экономиче	Произвести фикса

	минимизации рисков (risk minimization method)	ского эффекта от управления рисками рассчитывается по формуле, учитывающей М0 – суммарные вероятные потери без обработки идентифицированных рисков; суммарные вероятные потери после обработки рисков М; суммарные фактические потери от проявления рисков Iф; суммарные фактические расходы на обработку идентифицированных рисков (Н = Нф); суммарные фактические потери от проявления рисков Iфн; суммарные фактические расходы на обработку рисков Нфн)	цию рисков Определить индекс риска (м.б. выражен относительным или абсолютным уровнем затрат и измеряется вероятностью возникновения риска и степенью влияния риска при его возникновении) Классификация рисков по степени воздействия и уровня влияния Определение способов обработки риска Расчет показателей, характеризующих риски Расчет показателя экономического эффекта от управления рисками
8	Матричный (формальные модели защиты) (dot matrix)	Состояние системы защиты описывается тройкой параметров (S, O, M) - множества S – субъектов, O – объектов, M – прав доступа; Или (O, H, M): O – основы и составные части системы (нормативно-правовая, организационная, информационная и т.п.), H – направления защиты M – этапы создания СЗИ	Определение параметров. Составление трехмерной матрицы отношений. Преобразование матрицы отношений в двумерную таблицу. Определение качественных и количественных показателей.
9	Многоуровневый подход (multilevel)	Состояние системы защиты описывается совокупностью уровней конфиденциальности и набора категорий конфиденциальности	Модель конечных состояний Белла Ла-Падулы. Решетчатая модель Д.Деннинга
10	Оптимизационный подход (комбинаторный) (optimizational)	Решается задача дискретного программирования вида: максимизировать при условиях	Методы Балаша для целочисленных переменных ветвей и границ, исключения группы неизвестных, элементы теории двойственности, инструментарий линейного,

			выпуклого и параметрического программирования

Для объективной оценки экономического эффекта ИБ нет универсальных методов. Но считается, что затраты на обеспечение ИБ являются эффективными, если они обеспечивают выполнение требований государственных нормативных документов и стандартов, а также концепции ИБ. Под экономическим эффектом можно понимать превышение стоимостных оценок конечных результатов соответствующих мероприятий по ИБ над совокупными затратами ресурсов на их проведение за расчетный период.

Сложность оценки эффективности мероприятий по ИБ обусловлена целым рядом обстоятельств. В соответствии с теорией оценки эффективности систем, качество любого объекта, в том числе и СЗИ, проявляется лишь в процессе его использования по назначению (целевое функционирование), поэтому объективной является оценка по эффективности применения.

Любая СЗИ содержит элементы неопределенности, так как не возможно определить заранее, что точно произойдет в будущем с данной системой. Наиболее выраженно эти неопределенности проявляются в результате функционирования системы. Значительная неопределенность сопутствует этапу проектирования СЗИ. По мере реализации проекта ее уровень снижается, но эффективность СЗИ тем не менее не может быть адекватно выражена и описана детерминированными показателями. Процедуры испытаний, сертификации или лицензирования не устраняют полностью неопределенность свойств СЗИ или ее отдельных элементов и не учитывают случайный характер атак. Объективной характеристикой качества СЗИ, степенью ее приспособленности к достижению требуемого уровня безопасности в условиях реального воздействия случайных факторов, может служить ве

роятность, характеризующая степень возможностей конкретной СЗИ при заданном комплексе условий, достижение цели операции или выполнение задачи системой. Данная вероятность может быть положена в основу комплекса показателей и критериев оценки эффективности СЗИ. При этом критериями оценки служат понятия пригодности и оптимальности. Под пригодностью можно понимать выполнение всех установленных к СЗИ требований, а под оптима льностью — достижение одной из характеристик максимального значения при соблюдении ограничений и условий на другие свойства системы. Выбор конкретного критерия должен сопровождаться его согласованием с основной целью СЗИ.

Обычно при синтезе системы возникает многокритериальная задача сравнения различных структур СЗИ. В число рассматривае мых в задаче показателей входят и показатели эффективности, имеющие вероятностно-временной характер функций распределе ния. К ним относятся вероятность преодоления СЗИ за некоторое время.

Таким образом, к оценке эффективности функционирования СЗИ наилучшим образом применимы вероятностные методы, в соответствии с которыми уровни гарантий безопасности СЗИ тра нсформируются в доверительные вероятности соответствующих оценок показателей. Оценка оптимального уровня гарантий бе зопасности в значительной степени зависит от предотвращенного ущерба. Для получения численных оценок риска необходимо знать распределения случайных величин ущерба. Во многих случаях та кие оценки можно получить, например, с помощью имитационного моделирования или по результатам активного аудита СЗИ.

Таким образом, эффективность мероприятий по ИБ в СЗИ вряд ли может быть определена в детерминированных оценках. Ве роятностные характеристики - функции распределения показате лей позволяют наиболее полно определить эффективность ме роприятий по ИБ в СЗИ.

В расчетах эффективности, как правило, фигурируют две основные составляющие: получаемый от внедрения мероприятий по ИБ результат и затраты, необходимые на его реализацию.

Конечным результатом проведения мероприятий по обеспечению защищенности информации обычно считают значение предотвращенных потерь. Значение предотвращенных потерь Pi может быть рассчитано, исходя из вероятности возникновения i–го инцидента ИБ (i = 1, 2, …n) и возможных экономических потерь от него до и после реализации мероприятий по обеспечению ИБ на объекте:

$$P_i = P'_i - P''_i \ ,$$

где P'_i и P''_i – потери от реализации угроз до и после внедрения мероприятий, повышающих уровень защищенности системы соответственно.

Значение предотвращенных потерь отражает ту часть прибыли, которая могла бы быть потеряна в случае не применения мероприятия, повышающие уровень защищенности системы.

Суммарное значение предотвращенных потерь P по всем инцидентам ИБ определяется как:

$$P = \sum_{i=1}^{n} (Pi + Ri) \ ,$$

где Ri - непосредственно возвращаемые средства учреждения, например, возмещение стороной, виновной в инциденте ИБ, средства, полученные в результате применения штрафных санкций к сотрудникам, виновным в инцидентах ИБ, страховое возмещение.

Pi – значение предотвращенных потерь.

Наличие сложности точного определения значения предотвращенных потерь не является неочевидным. Источниками данных для расчета потерь могут быть статистические данные или результаты оценки инцидентов ИБ, полученные путем экспертного оценивания. Не всегда имеются достаточные и доступные для принятия решения статистические данные, в случае экспертного оценивания превалирует субъективизм оценок, что не повышает достоверности расчетов. Выходом из создавшегося положения может быть совместное применение обоих методов в рамках имитационного моделирования значений предотвращенных потерь - процессно-статистический подход. Данный подход предполагает следующие действия по имитационному моделированию значений предотвращенных потерь:

- разбиение возможных потерь на группы (по инцидентам ИБ);
- по каждому инциденту производится оценка (путем экспертного голосования или на основании статистических данных) значения величины потерь: минимальное (min), наиболее вероятное (mid) и максимальное (max) значения (до и после проведения мероприятий по ИБ);
- моделирование значений величины потерь (до и после проведения мероприятий по повышению ИБ), на основе определенных выше характеристик (согласно треугольному закону распределения);
- расчет суммарного значения предотвращенных потерь на основании моделируемых значений;
- расчет статистических характеристик моделированных суммарных значений предотвращенных потерь;
- расчет показателей эффективности проведенных мероприятий по ИБ и формулировка выводов.

В результате расчета получаем гистограмму распределения или интегральный процент распределения суммарного значения предотвращенных потерь. Знание значений упомянутого закона

позволяет без особых усилий оценить вероятность конкретного значения предотвращенных потерь в любой выбранной точке или вероятность нахождения значений в заданном интервале. Данную вероятность, с конкретным значением суммы предотвращенных потерь, можно считать в обосновании эффективности мероприятий по повышению ИБ гарантийной вероятностью.

Вторая составляющая, используемая при оценке эффективности мероприятий ИБ учреждения, это затраты на их реализацию и эксплуатацию. Такого рода затраты для совокупности мероприятий по ИБ могут включать:

- затраты на содержание подразделения ИБ;
- затраты на закупку и содержание аппаратно-программных средств ЗИ (непосредственно для реализации мероприятий);
- затраты на закупку и содержание иных средств ЗИ, не посредственно для реализации мероприятий;
- затраты на обучение персонала.

Полученные в результате составляющие (результат и затраты) могут быть использованы для расчета эффективности мероприятий по повышению ИБ образовательного учреждения с гарантийной вероятностью в любом из известных методов.

Таким образом, было проанализировано большое количество разнообразных подходов к оценке эффективности СЗИ, наиболее подходящим для оценки эффективности от внедрения методов многофакторной аутентификации можно считать вероятностный подход. Далее приведена реализация расчета эффективности использования методов аутентификации по отпечаткам пальцев и по радужной оболочке глаза, в начале осуществлен расчет затрат на внедрение данных методов.

3.2 Реализация расчета эффективности

Определим возможные затраты на внедрение методов идентификации и аутентификации по отпечаткам пальцев и радужной оболочке глаза в существующую СКУД РГЭУ (РИНХ). Используем

для этого метод оценки совокупной стоимости владения (ССВ) корпоративными системами защиты информации (КоСЗИ) [27]

Совокупная стоимость владения для организации многофа кторной аутентификации в РГЭУ (РИНХ) в общем случае складыва ется из стоимости:

- проектных работ;
- закупки и настройки программно-технических средств за щиты;
- затрат на обеспечение физической безопасности;
- обучения персонала;
- управления и поддержки системы (администрирование бе зопасности);
- аудита ИБ;
- периодической модернизации системы ИБ.

Определим затраты РГЭУ (РИНХ) на владение СЗИ (в таблице 3.2 приведен перечень затрат).

1. Затраты на приобретение и внедрение:
   - затраты на закупку и настройку программно-технических средств защиты (сканер отпечатков пальцев, считыватель радужной оболочки);
   - затраты, связанные с обслуживанием и настройкой програ ммно-технических средств защиты;
   - затраты, связанные с организацией сетевого взаимоде йствия;
   - затраты на повышение квалификации сотрудников пре дприятия в вопросах использования имеющихся средств за щиты, выявления и предотвращения угроз безопасности;
2. Затраты на эксплуатацию:
   - затраты на осуществление технической поддержки производственного персонала при внедрении средств за щиты и процедур;
   - затраты на контроль изменений состояния информационной среды предприятия;
   - потери от сбоев в работе;

Таблица 3.2 - Перечень критерий затрат на владение СЗИ.

Обозначение категории затрат	Описание
1	2
Z1	Затраты на закупку и настройку сканеров отпечатков пальцев
Z2	Затраты на закупку и настройку считывателей радужной оболочки
Z3	Затраты, связанные с обслуживанием и настройкой сканеров отпечатков пальцев
Z4	Затраты, связанные с обслуживанием и настройкой считывателей радужной оболочки

Продолжение таблицы 3.2

1	2
Z5	Затраты, связанные с организацией сетевого взаимодействия
Z6	Затраты на повышение квалификации сотрудников предприятия в вопросах использования имеющихся средств защиты, выявления и предотвращения угроз безопасности
Z7	Затраты на контроль изменений состояния информационной среды предприятия
Z8	Потери от сбоев в работе

Для проведения экспертизы было выбрано пять экспертов.

В таблице 3.3 представлены результаты реализации трех шагов экспертизы с использованием способа упорядочения группы затрат по критерию значимости.

На каждом шаге экспертизы осуществлялось ознакомление экспертов с медианой и средним значением (по Кемени) и с объяснениями, представленными в защиту сильно отличающихся ответов. Одновременно на каждом очередном шаге экспертизы при желании, эксперты могли менять свои предыдущие ответы.

Таблица 3.3 - Результаты реализации четырех шагов экспертизы

Эксперт	УПОРЯДОЧЕНИЕ (РАНЖИРОВАНИЕ) ЭКСПЕРТА			
	На шаге 1	На шаге 2	На шаге 3	На шаге 4
A1	Z2 Z4 Z1 Z3 Z5 Z8 Z6 Z7	Z2 Z4 Z1 Z3 Z5 Z8 Z6 Z7	Z2 Z4 Z1 Z3 Z5 Z8 Z6 Z7	Z2 Z4 Z1 Z3 Z5 Z8 Z6 Z7
A2	Z2 Z1 Z4 Z3 Z5 Z8 Z6 Z7	Z2 Z4 Z1 Z3 Z5 Z8 Z6 Z7	Z2 Z4 Z1 Z3 Z5 Z8 Z6 Z7	Z2 Z4 Z1 Z3 Z5 Z8 Z6 Z7
A3	Z2 Z4 Z5 Z1	Z2 Z4 Z5 Z1 Z3	Z2 Z4 Z5 Z1 Z3	Z2 Z4 Z5 Z1

	Z3 Z6 Z8 Z7	Z8 Z6 Z7	Z8 Z6 Z7	Z3 Z8 Z6 Z7
A4	Z2 Z1 Z8 Z4 Z3 Z6 Z7 Z5	Z2 Z4 Z8 Z1 Z3 Z6 Z5 Z7	Z2 Z4 Z1 Z8 Z3 Z6 Z5 Z7	Z2 Z4 Z1 Z3 Z8 Z6 Z5 Z7
A5	Z2 Z1 Z8 Z4 Z3 Z5 Z6 Z7	Z2 Z4 Z8 Z3 Z1 Z5 Z6 Z7	Z2 Z4 Z8 Z3 Z1 Z5 Z6 Z7	Z2 Z4 Z8 Z3 Z1 Z5 Z6 Z7

В таблицах 3.4, 3.5, 3.6, 3.7 представлены результаты каждого шага экспертизы, определены суммарное расстояние, медиана и среднее.

Таблица 3.4 - Шаг 1

	1	2	3	4	5	Сумма
1	0	6	4	13	9	32 1
2	6	0	10	11	9	36 1.3
3	4	10	0	17	13	44 1
4	13	11	17	0	4	45 1
5	9	9	13	4	0	35 0.7
Суммарное расстояние R1=192						
Медиана $A^{(1)}_1$: Z2 Z4 Z1 Z3 Z5 Z8 Z6 Z7						
Среднее $A^{(5)}_1$: Z2 Z1 Z8 Z4 Z3 Z5 Z6 Z7						

Таблица 3.5 - Шаг 2

	1	2	3	4	5	Сумма
1	0	0	6	10	10	26
2	0	0	6	10	10	26
3	6	6	0	12	12	44
4	10	10	12	0	4	36
5	10	10	12	4	0	36
Суммарное расстояние R1=168						
Медиана $A^{(1)}_1$: Z2 Z4 Z1 Z3 Z5 Z8 Z6 Z7						
Среднее $A^{(5)}_1$: Z2 Z1 Z8 Z4 Z3 Z5 Z6 Z7						

Таблица 3.6 - Шаг 3

	1	2	3	4	5	Сумма
1	0	0	6	8	10	24
2	0	0	6	8	10	24
3	6	6	0	10	12	34
4	8	8	10	0	6	32
5	10	10	12	6	0	38
Суммарное расстояние R1=152						
Медиана $A^{(1)}_1$: Z2 Z4 Z1 Z3 Z5 Z8 Z6 Z7						
Среднее $A^{(5)}_1$: Z2 Z1 Z8 Z4 Z3 Z5 Z6 Z7						

Таблица 3.7 – Шаг 4

	1	2	3	4	5	Сумма
1	0	0	6	6	10	22
2	0	0	6	6	10	22
3	6	6	0	8	12	32
4	6	6	8	0	8	28
5	10	10	12	8	0	40
Суммарное расстояние R1=144						
Медиана $A^{(1)}_1$:						
Среднее $A^{(5)}_1$:						

Оценки степени изменения суммарного рассогласования на каждом шаге:

$\Delta R2 = 13\ \%$

$\Delta R3 = 10\ \%$

$\Delta R4 = 5\ \%$

Поскольку на четвертом шаге суммарное рассогласование мнений экспертов отличается не более, чем на 5 % ($\Delta R3 = 3\ \%$) от суммарного рассогласования, полученного на предыдущем шаге, то после шага 4 можно завершать экспертизу.

Итогом реализации экспертной процедуры пошагового ранжирования объектов явилось следующее упорядоченное множество статей затрат:

Z2 Z4 Z1 Z3 Z5 Z8 Z6 Z7

В таблице 3.8 представлены множества экспертных оценок по каждой статье затрат, составляющих ССВ ИС.

Таблица 3.8 – Результаты шагов экспертизы для получения оценки статей затрат, составляющих ССВ СЗИ

Эксперт	Шаг 1			Шаг 2		
	Минимальное значение (тыс.руб)	Вероятное значение (тыс.руб)	Максимальное значение	Минимальное значение (тыс.руб)	Вероятное значение (тыс.руб)	Максимальное значение (тыс.руб)
1	**2**	**3**	**4**	**5**	**6**	**7**
Z1						
Э1	9	12	15	9	12	15
Э2	14	16	19	14	15	19
Э3	13	15	20	13	15	19
Э4	10	12	18	10	12	18

Э5	9	12	17	9	12	17
Z2						
Э1	90	120	150	90	120	150
Э2	110	130	160	110	130	160
Э3	100	130	150	100	130	150
Э4	95	120	140	100	120	140
Э5	100	120	140	100	130	140
Z3						
Э1	0	36	65	0	36	65
Э2	5	36	55	5	36	55
Э3	6	40	66	6	40	66
Э4	2	36	65	2	36	65
Э5	5	40	67	5	40	65
Z4						
Э1	0	45	90	0	45	90
Э2	3	55	70	4	55	70
Э3	4	45	65	4	45	70
Э4	0	45	90	0	45	90
Э5	3	55	70	3	55	70
Z5						
Э1	10	16	30	10	17	30
Э2	13	16	30	14	16	30
Э3	14	18	35	14	18	35
Э4	10	18	35	10	18	35
Э5	10	17	37	10	17	35
Z6						
Э1	5	8	15	5	8	15
Э2	4	8	16	4	9	16
Э3	5	9	15	5	9	15

Продолжение таблицы 3.8

1	**2**	**3**	**4**	**5**	**6**	**7**
Э4	5	8	15	5	8	15
Э5	4	9	14	4	9	15
Z7						
Э1	3	7	10	5	7	10
Э2	5	8	10	5	7	10
Э3	4	7	10	4	7	10
Э4	5	7	9	5	7	10
Э5	5	7	10	5	7	11
Z8						
Э1	10	47	90	10	40	90
Э2	11	36	100	11	36	100
Э3	12	36	98	12	36	98
Э4	11	37	100	12	37	100
Э5	11	35	95	11	35	95

В целях повышения точности расчетов, оценки каждого эксперта включают *три значения* искомого показателя: минимальное, максимальное и наиболее вероятное (представленные в виде треугольного распределения).

В качестве инструментальных средств для реализации имита ционного моделирования была использована система СИМ-UML, позволяющая с минимальными трудозатратами построить имита ционную модель.

Полученная модель включает множество переменных – пере менных-аргументов, представляющих собой экспертные оценки, и переменных-функций – обобщенных коллективных мнений *n* экспе ртов (здесь *n*=5) об искомом значении анализируемого показателя Z_i (i=$1,8\overline{1,16}$), определяемых как среднее *n (n=5)* случайных ве личин, имеющих треугольное распределение (мнений *n* уча стников экспертной группы), путем реализации на каждом *k*-ом шаге имитационного моделирования функции

$$E_{ob}^{(k)} = \frac{\sum_{i=1}^{n} E_i^{(k)}}{n},$$

где $E_{ob}^{(k)}E_{ob}^{(k)}$ - обобщенное мнение экспертов на *k-ом* шаге экспертизы;

$E_i^{(k)}E_i^{(k)}$ – оценка i-ого эксперта на *k-ом* шаге экспертизы;

n – количество экспертов, участвующих в экспертизе *(n = 5).*

В результате имитационного моделирования на каждом *k*-ом шаге были получены следующие статистические характеристики: математическое ожидание, дисперсия, коэффициент вариации, эксцесс, асимметрия. Было также получено распределение (в виде гистограммы) значений искомого показателя – функции $E_{ob}^{(k)} = f\left(E_i^{(k)}\right)E_{ob}^{(k)} = f\left(E_i^{(k)}\right)$. После реализации каждого k-ого ша га оценивалось изменение значений коэффициента вариации $Koef_{var}^{(k)}Koef_{var}^{(k)}$ функции $E_{ob}^{(k)}E_{ob}^{(k)}$. При отклонении коэффициента ва

риации от предыдущего значения на 5 % и менее считалось, что оценки экспертов стабилизировались и целесообразно завершать экспертизу, т.е. если . 100 < 5

$$\frac{\left|Koef_{var}^{(k)} - Koef_{var}^{(k+1)}\right|}{Koef_{var}^{k}} \times 100\% < 5\%, \frac{\left|Koef_{var}^{(k)} - Koef_{var}^{(k+1)}\right|}{Koef_{var}^{k}} . 100 < 5,$$

то экспертиза завершалась.

На последнем шаге экспертизы по каждой статье затрат по результатам имитационного моделирования оценивались доверительные границы значений искомого показателя и вероятность того, что его значения окажутся больше или меньше определенного числа.

Результаты имитационного моделирования для оценки показателей после каждого из двух шагов экспертизы приведены в приложении А.

В таблицах 3.9 и 3.10 представлены значения обобщенных мнений экспертов на 1 и 2 шагах с числом итераций – 1000.

Таблица 3.9 - Обобщенное мнение экспертов на 1 шаге с числом итераций – 1000

	Z1	Z2	Z3	Z4	Z5	Z6	Z7	Z8
Среднее	14	124	35,2	42,77	20,53	9,37	7,151	48,546
Дисперсия	0,4	22,58	30,22	48,36	4,65	0,87	0,26	63,13
Среднеквадратическое отклонение	0,64	4,75	5,5	6,95	2,16	0,93	0,5	7,95
Коэффициент вариации	0,046	0,038	0,156	0,163	0,105	0,1	0,071	0,164
Асимметрия	0,063	-0,114	-0,028	-0,111	14,969	0,058	0,026	0,175
Эксцесс	-0,276	-0,142	-0,223	0,019	28,46	-0,286	-0,254	-0,119
Минимум	12,27	108,92	20,18	18,87	14,96	6,66	5,434	27,062
Максимум	16	138,99	52,57	62,74	28,46	12,14	8,577	72,627
Модальный интервал	13,98 ÷ 14,33	122,57 ÷ 125,32	34,9 ÷ 37,85	38,8 ÷ 42,8	18,64 ÷ 19,87	8,65 ÷ 9,15	6,86 ÷ 7,15	47,77 ÷ 51,92

Таблица 3.10 - Обобщенное мнение экспертов на 2 шаге с числом итераций – 1000

	Z1	Z2	Z3	Z4	Z5	Z6	Z7	Z8
Среднее	13,97	125,28	34,69	43	20,67	9,5	7,329	47,753
Дисперсия	0,398	20,49	29,36	49,12	4,29	0,926	0,26	64,89
Среднеквадратическое отклонение	0,631	4,526	5,42	7,01	2,07	0,962	0,51	8,056
Коэффициент вариации	0,045	0,036	0,156	0,163	0,1	0,101	0,07	0,169
Асимметрия	0,142	-0,067	-0,003	-0,018	0,281	0,109	0,054	0,166
Эксцесс	-0,195	-0,164	-0,051	-0,019	0,022	-0,176	0,213	-0,11
Минимум	12,21	110,223	15,59	18,87	15,19	6,9	5,636	23,413
Максимум	16,1	138,42	52,79	62,74	28,75	12,39	9,149	76,966
Модальный интервал	13,63 ÷ 13,98	125,6 ÷ 128,17	32,5 ÷ 35,88	38,8 ÷ 42,8	18,9 ÷ 20,12	9,39 ÷ 9,89	7,233 ÷ 7,552	42,89 ÷ 47,76

Оценим целесообразность завершения экспертизы, то есть, определим, насколько существенно изменился коэффициент вариации на очередном шаге. Для вычисления значения изменения коэффициента вариации (в процентах) используем следующую формулу:

$$\frac{\left|Koef_{var}^{(1)} - Koef_{var}^{(2)}\right|}{Koef_{var}^{(1)}} \times 100\% \frac{\left|Koef_{var}^{(1)} - Koef_{var}^{(2)}\right|}{Koef_{var}^{(1)}} .100$$

В таблице 3.11 приведены вычисления изменения коэффициента вариации после второго шага.

Таблица 3.11 – Изменение коэффициента вариации

	ШАГ 1	ШАГ 2	Изменение коэффициента вариации, %
Z1	0,046	0,045	2
Z2	0,038	0,036	5

Z3	0,156	0,156	0
Z4	0,163	0,163	0
Z5	0,105	0,1	5
Z6	0,1	0,101	1
Z7	0,071	0,07	1
Z8	0,164	0,169	3

Так как после второго шаг изменение коэффициента вариации по всем критериям (Z1-Z8) меньше или равно 5 % можно завершать экспертизу.

На основании результатов имитационного моделирования сформирована таблица 3.12, содержащая исходные данные для расчета совокупной стоимости владения СЗИ.

Таблица 3.12 - Исходные данные для расчета совокупной стоимости владения СЗИ

Наименование статьи затрат	Обозначение статьи затрат	Значение (тыс.руб.)
1	**2**	**3**
Затраты на закупку и настройку сканеров отпечатков пальцев	Z_1	13,97
Затраты на закупку и настройку считывателей радужной оболочки	Z_2	125,28
Затраты, связанные с обслуживанием и настройкой сканеров отпечатков пальцев	Z_3	34,69
Затраты, связанные с обслуживанием и настройкой считывателей радужной оболочки	Z_4	43
Затраты, связанные с организацией сетевого взаимодействия	Z_5	20,67
Затраты на повышение квалификации сотрудников предприятия в вопросах использования имеющихся средств защиты, выявления и предотвращения угроз безопасности	Z_6	9,5
Затраты на контроль изменений состояния информационной среды предприятия	Z_7	7,329
Потери от сбоев в работе	Z_8	47,753
ИТОГО:		**302,192**

Реализовав предложенную методику оценки ССВ СЗИ, было определено, что совокупная стоимость владения информационной системой равна **302,192** тыс. рублей.

Далее проведем расчет эффективности по предложенному ранее методу [25].

Из таблицы 3.13 можно определить затраты на мероприятия ИБ: аутентификация по радужной оболочке и аутентификация по отпечаткам пальцев (Z2+Z4) и (Z1+Z3) соответственно.

Таблица 3.13 – Затраты на мероприятия ИБ

Мероприятия ИБ	Затраты, тыс. руб	Поступления, тыс. руб			
		Обозн.	min	mid	max
E1-считыватель ра дужки	168	P1	60	80	100
E2-сканер отпечатков	49	P2	30	40	50
Сумма	201		90	120	150
r-процентная ставка	10 %				

Рассчитаем чистый приведенный доход (NPV), индекс рентабельности (PI), внутреннюю норму доходности (IRR), модифицированную внутреннюю норму доходности (MIRR), дисконтированный срок окупаемости проекта (DPB). Выполним сценарный расчет и сделаем выводы о целесообразности инвестиций.

Осуществим моделирование объемов возможных поступлений средств по приведенным мероприятиям (предотвращенный ущерб). Данные по поступлению, полученные в процессе их моделирования, обобщаются как сумма поступлений в итоговое распределение (рисунок 3.1). Описательная статистика итогового распределения суммы предотвращенного ущерба приведена в таблице 3.14.

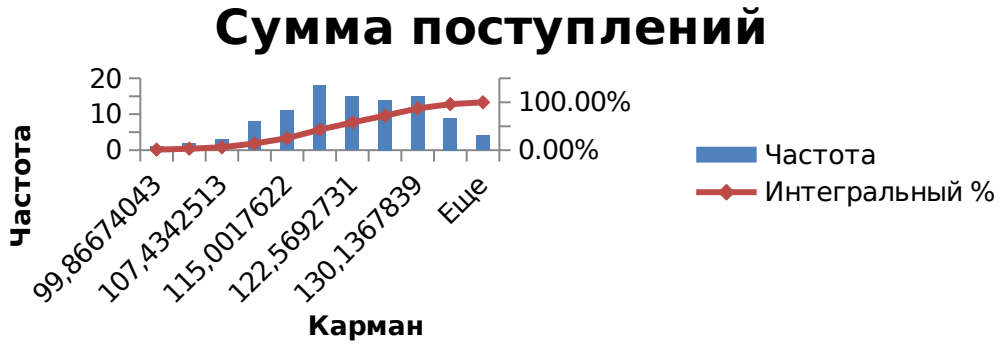


Рисунок 3.1 - Гистограмма суммы поступлений

Таблица 3.14 – Описательная статистика

Показатель	Значение

Среднее	116,89
Стандартная ошибка	3,62
Стандартное отклонение	11,46
Дисперсия выборки	131,24
Минимум	99,87
Максимум	133,92
Сумма	1168,94

Результаты моделирования и описательная статистика итогового распределения использованы для построения сценариев оценки эффективности (таблица 3.15).

Таблица 3.15 - Сценарии оценки эффективности

Сценарии	Обозначение	Объемы поступления платежей
Пессимистический (Pessimistic)	Sp	99,9
Наиболее вероятный (The most probable)	Sv	118,7
Оптимистический (Optimistic)	So	133,9

Для каждого из сценариев были выполнены расчеты показателей эффективности, приведенные в таблице 3.16.

Таблица 3.16 – Расчеты показателей эффективности

Показатели эффективности	Обозначение	Сценарии		
		Sp	Sv	So
Индекс рентабельности	PI	1,38	1,09	1,23
Дисконтированный срок окупаемости	DPB	1,83	0,51	0,69
Чистый приведенный доход	NPV	273,28	226,61	255,63
Затраты приведенные к моменту врем. 0	PVO	217,00	217,00	217,00
Модифицированная внутренняя норма доходности	MIIR	21%	26,41%	34,26%

Внутренняя норма доходности	IIR	4,91%	33,21%	45,02%
Поступления, приведенные к моменту окончания проекта	FVI	351,65	274,20	309,31

Для сценариев выполняются все условия одобрения:

NPV > 0;

PI > 1;

MIRR > R.

Таким образом, были реализованы методики расчета совокупной стоимости владения СЗИ и сценариев оценки эффективности СЗИ. Проведенные расчеты показывают, что даже в наиболее пессимистическом сценарии (Объемы поступления платежей - 99,9) внедрение предполагаемой СЗИ является эффективным. Внедрение СЗИ окупится в худшем случае на 3 год, наиболее вероятно через 2 года.

Далее необходимо оценить уровень защищенности СКУД, на сколько он изменится от внедрения методов многофакторной аутентификации.

3.3 Оценка основных показателей эффективности

Для оценки эффективности биометрических систем аутентификации следует опираться на действующие стандарты в области оценки эффективности аутентификации [29-33]. После подготовки базы проводятся необходимые эксперименты и рассчитываются основные численные показатели аутентификации биометрической системы:

- вероятность отказа регистрации (the probability of failure of registration);

- вероятность отказа сбора данных (the probability of failure of data collection);
- вероятность ложного несовпадения (the probability of false mismatch);
- вероятность ложного совпадения (the probability of false ma tch).

Далее рассмотрим более подробно данные параметры.

Вероятность отказа регистрации

ВОР (FTE) – это доля выборки, для которой система иде нтификации и аутентификации не может в виду различных причин закончить процесс регистрации. ВОР включает в себя пользовате лей, которые:

- не могут предоставить образец с достаточным каче ством;
- не могут получить результат оценки совпадения со своим заново созданным шаблоном при процессе ре гистрации.

При технологическом испытании анализ основан на предва рительно подготовленной тестовой БД. Но даже в этом случае может произойти сбой в регистрации, например, в ситуации, когда качество записи биометрического образца имеет столь низкое зна чение, что извлечь из него необходимые признаки становится не возможным. ВОР (в процентах) для целевой выборки следует опре делять как долю (или весовую долю) людей в испытуемой группе, которые не смогли успешно пройти процесс регистрации.

$$\text{ВОР}\ (\tau) = \frac{Nfail(\tau)}{Ntotal}.100\ ,$$

где $Ntotal$ - общее количество попыток регистрации,

$Nfail(\tau)$ - количество не успешных попыток регистрации, в зависимости от порога.

ВОР зависит от политики регистрации, которая определяет уровень качества образца для регистрации, порог принятия реше

ния для подтверждения применимости регистрации, а также число попыток или время, отведенное на регистрацию при транза кции регистрации. Политика регистрации должна быть описана на ряду с наблюдаемой ВОР. Более строгие требования к качеству ре гистрации увеличивают ВОР, но улучшают эксплуатационные хара ктеристики сравнений в биометрической системе.

Вероятность отказа сбора данных

ВОСД (FTA) – это доля попыток идентификации или ауте нтификации, для которых биометрическая система не может получить или отобрать образец достаточного качества. ВОСД может включать в себя:

- попытки, при которых биометрическая характеристика не может быть получена (например, из-за физического состояния);
- попытки, при которых не удается произвести сегмента цию или извлечение необходимых признаков;
- попытки, при которых извлеченные признаки не проходят порог проверки качества.

ВОСД можно определить для каждой транзакции, например, путем определения числа транзакций, в процессе которых ни при одной из попыток регистрации не был получен биометрический образец достаточного качества для сравнения. При технологиче ском испытании анализ основан на предварительно собранной БД. ВОСД (в процентах) следует определять как долю (или весовую долю) записанных попыток легитимного пользователя (и, по возможности, любых пассивных попыток злоумышленника в ре жиме реального времени), которые не могут быть закончены из-за отказов в представлении (изображение не получено), сегмента ции, извлечении признаков или контроля качества.

$$\text{ВОСД}\,(\tau) = \frac{Nfail(\tau)}{Ntotal}.100 \ ,$$

где $Ntotal$ - общее количество попыток верификации или идентификации,

$Nfail(\tau)$ - количество не успешных попыток идентификации или верификации, в зависимости от порога.

ВОСД зависит от порога качества образца, а также от времени, установленного на получение биометрического образца, или допускаемого числа представлений. Данные параметры настройки должны быть указаны в протоколе испытаний вместе со значением ВОСД.

Более строгий уровень качества для получения биометрического образцов увеличивает ВОСД, но улучшает эксплуатационные характеристики сравнений в биометрической системе. Попытки, при которых исходный образец не был получен или не имеет достаточного качества, не обрабатываются алгоритмом сравнения, а степень схожести не определяется. Такие отказы сбора данных должны быть исключены при вычислении ВЛС и ВЛНС, но должны быть включены в вычисление ВЛД и ВЛНД. ВОСД, ВЛС и ВЛНС должны быть вычислены при одних и тех же значениях порога принятия решения.

Вероятность ложного несовпадения

ВЛНС (FNMR) – это доля образцов, полученных в результате попыток легитимного пользователя, которые ошибочно признаны несовпадающими с шаблоном зарегистрированного в системе пользователя. ВЛНС (в процентах) следует определять как долю (или весовую долю) зафиксированных попыток легитимного пользователя, которые были переданы подсистеме сравнения, и для которых степень схожести была ниже соответствующего порога принятия решения о схожести.

$$\text{ВЛНС}\ (\theta) = \frac{Nimposter(error)(\theta)}{Ntarget}.100\ ,$$

где $Ntarget$ - количество сравнений вида "свой-свой",

$Nimposter(error)(\theta)$ - количество сравнений вида "свой-свой", идентифицированных как "свой-чужой", в зависимости от порога.

ВЛНС зависит от порога принятия решения о схожести и должна быть указана вместе с наблюдаемой ВЛС при том же пороге принятия решения.

Вероятность ложного совпадения

ВЛС (FMR) – это доля образцов, полученных в результате пассивных попыток злоумышленника, которые ошибочно признаны совпадающими с шаблоном зарегистрированного пользователя. При пассивных попытках злоумышленника пользователи предоставляют свою собственную биометрическую характеристику, как будто они совершают попытку успешной аутентификации с собственным шаблоном. Например, в случае динамической верификации подписи злоумышленник при пассивной попытке поставил бы свою собственную подпись. ВЛС (в процентах) следует определять как долю (или весовую долю) зафиксированных пассивных попыток злоумышленника, которые были переданы подсистеме сравнения и для которых степень схожести не ниже соответствующего порога принятия решения о схожести.

$$\text{ВЛС}\ (\theta) = \frac{Ntarget(error)(\theta)}{Nimposter}.100\ ,$$

где $Nimposter$ - количество сравнений вида "свой-чужой";

$Ntarget(error)(\theta)$ - количество сравнений вида "свой-чужой", идентифицированных как "свой-свой", в зависимости от порога.

ВЛС зависит от порога принятия решения о схожести и должна быть указана наряду с наблюдаемой ВЛНС при том же пороге принятия решения.

3.5 Моделирование расчета повышения эффективности СКУД

Для Моделирования расчета повышения эффективности СКУД от внедрения методов многофакторной аутентификации рассчитае м основные показатели эффективности СЗИ, для чего проведем испытания на существующих в РГЭУ (РИНХ) приборах (сканер отпечатков пальцев, считыватель радужной оболочки). Осуще ствим регистрацию пользователей, будем проводить их ауте нтификацию с неизменными параметрами, а также с параметра ми, отличными от параметров при регистрации. Определим ве роятности отказа регистрации, отказа сбора данных, ложного соответствия и ложного несоответствия для каждого метода ауте нтификации.

Метод аутентификации по отпечаткам пальцев

Используемое оборудование:

- Сканер отпечатков пальцев Fingkey Hamster;
- Компьютер с установленным ПО - Free Fingerprint Verifica tion.

В системе было зарегистрировано 20 пользователей. Система работает по 9-ти бальной шкале, при значениях меньше или равно 5, система отказывает в доступе.

При нормальных параметрах при регистрации система не выдавала ошибок в отказе регистрации. Если параметры были изменены (расположение пальца чуть боком, под углом вверх, под наклоном, палец сдвинут – неполное изображение, мокрый палец), то система отказывала в регистрации.

Таким образом, вероятность отказа регистрации при ра зличных параметрах равна:

$$\text{ВОР}\ (\tau) = \frac{Nfail(\tau)}{Ntotal}.100 = \frac{8}{20}.100 = 40.$$

При попытке идентификации пользователей система отказыва ла в сборе данных при следующих параметрах: мокрый палец, под углом, неполное изображение пальца, под наклоном.

Вероятность отказа сбора данных равна:

$$\text{ВОСД}\ (\tau) = \frac{Nfail(\tau)}{Ntotal}.100\ = \frac{5}{20}.100 = 25.$$

При различных параметрах (без каких-либо изменений, ра сположение пальца чуть боком, сильное надавливание на сканер, слабое надавливание, под углом вверх, под наклоном, палец те плый и немного влажный, мокрый палец, легкий слой крема на па льце, палец сдвинут – неполное изображение) можно рассчитать следующие параметры:

Вероятность ложного несовпадения:

$$\text{ВЛНС}\ (\theta) = \frac{Nimposter(error)(\theta)}{Ntarget}.100 = \frac{43}{110}\ .\ 100 = 39$$

Вероятность ложного совпадения:

$$\text{ВЛС}\ \theta = \frac{Ntarget(error)(\theta)}{Nimposter}.100 = 46\ /\ 110\ \ .\ 100 = 42$$

В приложении В приведены полученные при проведении эксперимента значения. В таблице 3.17 приведены усредненные значения по каждому параметру.

Таблица 3.17 – Усредненные значения по параметрам ауте нтификации по отпечаткам пальцев

Параметр	Среднее значение
Без каких-либо изменений	9
Расположение пальца чуть боком	4,27
Сильное надавливание на сканер	8,9
Слабое надавливание	8,9
Под углом вверх	1,55
Под наклоном	2,82

Палец теплый и немного влажный	8,55
Мокрый палец	7
Тонкий слой крема на пальце	5,09
Палец сдвинут – неполное изображение	2,36

Как видно из таблицы, лишь какие-либо серьезные изменения в параметрах (под углом, неполное изображение, чуть боком) увеличивают вероятность ложного несовпадения и вероятность отказа в сборе данных.

Метод аутентификации по радужной оболочке

Используемое оборудование:

- считыватель радужной оболочки BM-ET200 фирмы Panasonic
- компьютер с установленной ОС Windows XP, имеющий COM-порт и сетевую карту Ethernet;
- ПО администратора BM-ET200;

В системе было зарегистрировано 20 пользователей. Результат аутентификации: допустить пользователя – 1, не допустить пользователя – 0.

При нормальных параметрах при регистрации система не выдавала ошибок в отказе регистрации. Но если параметры были изменены (очки, попадание солнечного света; без очков, попадание солнечного света; линзы, попадание солнечного света), то система отказывала в регистрации.

Таким образом, вероятность отказа регистрации при различных параметрах равна:

$$\text{BOP}(\tau) = \frac{Nfail(\tau)}{Ntotal} .100 = 6/20 \,.\, 100 = 30\%.$$

При попытке идентификации пользователей система отказыва ла в сборе данных при следующих параметрах: очки, попадание солнечного света; без очков, попадание солнечного света; линзы, попадание солнечного света.

Вероятность отказа сбора данных равна:

$$\text{ВОСД}\ (\tau) = \frac{Nfail(\tau)}{Ntotal}.100\ = 6/20\ .\ 100\ \frac{5}{20} * 100\% = 30.$$

При различных параметрах (очки, искусственное освещение; очки, дневной свет; очки, попадание солнечного света; без очков, искусственное освещение; без очков, дневной свет; без очков, попадание солнечного света; линзы, искусственное освещение; линзы, дневной свет; линзы, попадание солнечного света) можно рассчитать следующие параметры:

Вероятность ложного несовпадения:

$$\text{ВЛНС}\ (\theta) = \frac{Nimposter(error)(\theta)}{Ntarget}.100 = 7\ /\ 62\ \frac{43}{110}.100 = 11{,}3$$

Вероятность ложного совпадения:

$$\text{ВЛС}\ \theta = \frac{Ntarget(error)(\theta)}{Nimposter}.100 = 0\ /\ 62\ .\ 100 = 0.$$

В приложении В приведены полученные при проведении эксперимента значения. В таблице 3.18 приведены усредненные значения по каждому параметру.

Таблица 3.18 – Усредненные значения по параметрам ауте нтификации по радужной оболочке

Параметр	Среднее значение
Очки, искусственное освещение	0,73
Очки, дневной свет	0,82
Очки, попадание солнечного све та	0
Без очков, искусственное освеще	0,9

ние	
Без очков, дневной свет	1
Без очков, попадание солнечного света	0
Линзы, искусственное освещение	0,83
Линзы, дневной свет	1
Линзы, попадание солнечного света	0

Как видно из таблицы, попадание солнечного света не позволяет осуществить регистрацию и сбор данных. Очки и линзы не оказывают сильного влияния на аутентификацию пользователя, но очки и линзы темного цвета увеличивают вероятность ложного несовпадения. При дневном свете и неизменных параметрах допуск осуществляется со стопроцентной вероятностью.

Сумма вероятностей НСД и защищенности равна единице [34].

$$\mathbf{P_{нсд} + P_{защ} = 1, \quad то\ P_{нсд} = 1 - P_{защ}}$$

Отсюда следует, что вероятность НСД при применении па роля, ключа или биометрии соответственно равна:

$$\mathbf{P_{нсд}^{п,к,б} = 1 - P_{защ}^{п,к,б} = 1 - (1- P_1^{п,к,б}) (1-P_2^{п,к,б})...(1-P_j^{п,к,б}) = 1 - \prod_{i=1}^{j} ¿¿_i^{п,к,б})\ ,}$$

где $P_i^{\,п,к,б}$ – вероятность правильной работы механизма паролирования, личного ключа или механизма биометрического признака.

Так как события получения НСД по всем трем факторам независимы, то общая вероятность НСД определяется в виде

$$\mathbf{P_{нсд} = (1-\prod_{i=1}^{j} P_i^{п})(1-\prod_{i=1}^{\varepsilon} P_i^{к})(1-\prod_{i=1}^{\mu} P_i^{б}).}$$

А вероятность защищенности равна

$$\mathbf{P_{защ} = \prod_{i=1}^{j} P_i^{п} \prod_{i=1}^{\varepsilon} P_i^{к} \prod_{i=1}^{\mu} P_i^{б}}$$

В таблице 3.19 рассчитаны вероятности НСД и вероятности защищенности для методов биометрической аутентификации, основанные на проведенных измерениях.

Таблица 3.19 – Вероятности для методов аутентификации (по радужной оболочке и отпечаткам пальцев)

Метод аутентификации (The method of authentication)	Вероятность отказа регистра	Вероятность отказа сбора да	Вероятность ложного не	Вероятность ложного совпа	**Вероятность НСД**	**Вероятность защищенности**
Отпечатки пальцев (Fingerprint)	0,40	0,25	0,39	0,42	**0,02**	**0,98**
Радужная оболочка глаза (Iris)	0,30	0,30	0,113	0,0	**0,01**	**0,99**

В нашем случае, СКУД РГЭУ (РИНХ) может быть представлена в виде следующих рубежей защиты: турникеты, парольная аутентификация, аутентификация по отпечаткам пальцев и аутентификация по радужной оболочке глаза. Тогда, вероятность защищенности СКУД РГЭУ (РИНХ) может быть рассчитана следующим образом:

$$\mathbf{P_{защ}} = P_i^m ¿ P_j^n * P_g^{po} * P_f^{on} \quad ,$$

где P_i^m – вероятность правильного функционирования турникетов,

$-$*вероятность правильного функционирвоания турникетов*

P_j^n – вероятность правильной работы механизма паролирования,

$P_g^{po} -$¿ вероятность правильного применения механизмов аутентификации по радужной оболочке глаза,

P_f^{on} - вероятность правильного применения механизмов аутентификации по отпечаткам пальцев.

Рассчитаем, как будет изменяться степень защищенности СКУД РГЭУ (РИНХ) в зависимости от применения или не применения каких-либо рубежей СКУД. В таблице 3.20 приведены степени защищенности СКУД РГЭУ (РИНХ).

Таблица 3.20 – Вероятность защищенности СКУД в зависимости от рубежа защиты

Степень защищенности рубежей защиты:				
Аутентификация по радужной оболочке глаза (Authentication by Iris)	P_g^{po}	-	-	0,99
Аутентификация по отпечаткам пальцев (Authentication by Fingerprint)	P_f^{on}	-	0,98	0,98
Аутентификация по паролю (Authentication by Password)	P_j^n	0,78	0,78	0,78
Проход через турникеты (The passage through the turnstiles)	P_i^m	0,65	0,65	0,65
Вероятность защищенности СКУД (The probability of security of the SCAM)		**0,923**	**0,998**	**0,999**

Таким образом, применение механизмов аутентификации по отпечаткам пальцев в дополнении к первоначальной СКУД (проход через турникеты, аутентификация по паролю) повышает ее защищенность на 0,075.

А совместное применение механизмов аутентификации по отпечаткам пальцев и аутентификации по радужной оболочке гла

за вместе с первоначальной СКУД повышает ее защищенность на 0,076.

Таким образом, в данной главе были проведены расчеты эффективности внедрения методов многофакторной аутентификации в СКУД РГЭУ (РИНХ), а именно расчет совокупной стоимости владения, расчет сценариев оценки эффективности (пессимистический, оптимистический, наиболее вероятный), расчет повышения защищенности СКУД.

Проведенные вычисления позволили сделать вывод о том, что внедрение методов многофакторной аутентификации позволит повысить эффективность системы контроля и управления доступом РГЭУ (РИНХ).

ЗАКЛЮЧЕНИЕ

В выпускной квалификационной работе были проанализирова ны вопросы и задачи обеспечения безопасности информации в системе контроля и управления доступом РГЭУ (РИНХ). Были та кже проанализированы организационная структура РГЭУ (РИНХ), реализуемый комплекс мер для обеспечения безопасности пе рсонала и студентов в университете, а также основные силы и сре дства, обеспечивающие безопасность персонала и студентов. Был сформирован перечень объектов защиты РГЭУ (РИНХ) и выделены основные категории пользователей ИС РГЭУ (РИНХ). Проана лизированы причины несанкционированного доступа к информа ции и способы защиты от них, проанализирована существующая в РГЭУ (РИНХ) система контроля и управления доступом, проана лизированы методы аутентификации и идентификации, более подробно проанализированы методы биометрической ауте нтификации по отпечаткам пальцев и по радужной оболочке гла за.

Были проанализированы методы биометрической ауте нтификации, стадии идентификация и аутентификация по биоме трической системе. Были изучены статические и динамические методы биометрической аутентификации. Более детально иссле дованы методы аутентификации по радужной оболочке глаза и по отпечаткам пальцев, рассмотрены возможные атаки злоумышле нников. Был также проанализирован процесс идентификации и а утентификации по радужной оболочке глаза и по отпечаткам па льцев. Были исследованы технические устройства, необходимые для аутентификации по радужной оболочке глаза и по отпечаткам пальцев.

Проанализированы действующие ГОСТы, существующие ме тоды оценки эффективности. Использован метод оценки совокупной стоимости владения системами защиты информации для определения возможных затрат от внедрения методов

многофакторной аутентификации в СКУД РГЭУ (РИНХ), проведено экспертное оценивание.

Проведен расчет эффективности СЗИ с использованием мате матического моделирования для построения сценариев оценки эффективности. Были выполнены расчеты показателей эффе ктивности для каждого из сценариев.

Проведена оценка основных показателей эффективности (ве роятность отказа регистрации, вероятность отказа сбора данных, вероятность ложного несовпадения, вероятность ложного совпа дения). Были осуществлены математические расчеты и моде лирование расчета повышения эффективности СКУД.

Все вышеперечисленное позволило сделать математические расчеты, подтверждающие эффективность и целесообразность вне дрения методов многофакторной аутентификации в СКУД РГЭУ (РИНХ).

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Гурикова А.С. Применение технологии двухэтапной аутентификации для защиты пользовательского аккаунта // Фундаментальные и прикладные научные исследования: сборник статей Международной научно-практической конференции (05 ноября 2015 г., г. Екатеринбург). / в 3 ч. Ч.2 – Уфа: Аэтерна 2015. – 270 с., ISBN 978-5-906836-14-4 ч.2, ISBN 978-5-906836-16-8
2. Гурикова А.С. Новый подход к решению проблем аутентификации в информационных системах // Перспективы развития научных исследований в 21 веке: материалы IX Международной научно-практической конференции (31.10.2015 г., г. Махачкала)
3. Гурикова А.С. Двухэтапная аутентификация как мера защиты информации пользователя информационных систем // Труды Северо-Кавказского филиала Московского технического университета связи и информатики, часть I. – Ростов-на-Дону.: ПЦ «Университет» СКФ МТУСИ, 2015, 552 с., С 493 – 496. – 0,465 п.л., ISSN 221-7975
4. Паспорт безопасности «РГЭУ (РИНХ)». [Электронный ресурс]. URL: http://www.rsue.ru/doc/bezopasnost/pasp_bezop.pdf (дата обращения: 10.03.2016).
5. Структура и органы управления «РГЭУ (РИНХ)» [Электронный ресурс]. URL: http://rsue.ru/Podrazdelenie.aspx?id=5930 (дата обращения: 10.03.2016).
6. Методический документ ФСТЭК Меры ЗИ в ГИС, 2014. [Электронный ресурс]. URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/805-metodicheskij-dokument (дата обращения: 23.03.2016).
7. Базовая модель угроз безопасности ПД при их обработке в ИСПД. 15.02. 2008 г [Электронный ресурс]. URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsia

lnye-normativnye-dokumenty/379-bazovaya-model-ugroz-bezopa snosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informa tsionnykh-sistemakh-personalnykh-dannykh-vypiska-fstek-rossii-2008-god (дата обращения: 23.03.2016).

8. ГОСТ Р 54831-2011. СКУД. Устройства преграждающие упра вляемые. Общие технические требования. Методы испытаний. [Электронный ресурс]. URL: http://vsegost.com/Cata log/51/51742.shtml (дата обращения: 23.03.2016).
9. ГОСТ Р 51241 – 2008. СКУД. Классификация. Общие техниче ские требования. Методы испытаний. [Эле ктронный ресурс]. URL: http://expert-01.com/assets/image s/uslugi/kontrol_dostupa/GOST%20R%2051241-2008.pdf (дата обращения: 23.03.2016).
10. Анисимов В.В. Протоколы аутентификации (идентификации). [Электронный ресурс]. URL:https://sites.google.com/site/a nisimovkhv/learning/kripto/lecture/tema11 (дата обращения: 29.03.2016).
11. ГОСТ Р ИСО/МЭК 19794-2—2005 Автоматическая идентифика ция. Идентификация биометрическая. Форматы обмена биоме трическими данными. Часть 2. Данные изображения отпечатка пальца - контрольные точки [Электронный ресурс]. URL: http:// vsegost.com/Catalog/21/2128.shtml (дата обращения: 29.03.2016).
12. Биометрия. Международный фонд автоматической иде нтификации. [Электронный ресурс]. URL: http://www.fond-ai.ru/a rt1/art228.html (дата обращения: 29.03.2016).
13. Обзор биометрических методов аутентификации. [Эле ктронный ресурс]. URL: http://dic.acade mic.ru/dic.nsf/ruwiki/1748182 (дата обращения: 10.04.2016).
14. Шаров В. Биометрические методы компьютерной безопа сности // PC Magazine/Russian Edition №4 (80), апрель 2005. [Электронный ресурс]. URL: http://www.bytema g.ru/articles/detail.php?ID=6719 (дата обращения: 10.04.2016).

15. Биологический энциклопедический словарь. - М.: ДиректМедия Паблишинг, 2006. - 9000 с. [Электронный ресурс]. URL: http://biblioclub.ru/?page=dict&dict_id=93 (дата обращения: 10.04.2016).
16. Радужная оболочка глаза (радужка), строение. [Электронный ресурс]. URL: http://zrenue.com/anatomija-glaza/40-raduzhka/345-raduzhnaja-obolochka-glaza-raduzhka-stroenie.html (дата обращения: 11.04.2016).
17. Официальный сайт Biometric Ideal Test. Базы данных по биометрическим параметрам. [Электронный ресурс]. URL: http://biometrics.idealtest.org/ (дата обращения: 16.04.2016).
18. Iris Recognition Technology. [Электронный ресурс]. URL: http://www.irisid.com/productssolutions/technology-2/irisrecognitiontechnology/ (дата обращения: 16.04.2016).
19. Считыватель радужной оболочки глаза Panasonic BM-ET200. [Электронный ресурс]. URL: http://www.hansab.ru/%D0%A2%D0%BEv%D0%B0ry/Panasonic-BM-ET200-Iris-Reade (дата обращения: 16.04.2016).
20. Симанков В.С., Луценко Е.В. Адаптивное управление сложными системами на основе теории распознавания образов. [Электронный ресурс]. URL: http://victor-safronov.ru/systems-analysis/books/simankov-lucenko/14.html (дата обращения: 16.04.2016).
21. Сканеры отпечатков пальцев. Классификация и способы реализации [Эл. ресурс]. URL: https://geektimes.ru/post/116458/ , Сканеры отпечатков пальцев [Эл. ресурс]. URL: http://www.idexpert.ru/equipment/7/ (дата обращения: 21.04.2016).
22. NITGEN Fingkey Hamster. [Электронный ресурс]. URL: http://www.neurotechnology.com/fingerprint-scanner-nitgen-fingkey-hamster.html (дата обращения: 21.04.2016).
23. Fingkey Hamster. [Электронный ресурс]. URL: http://www.nitgen.com/eng/product/finkey.html#a1 (дата обращения: 21.04.2016).

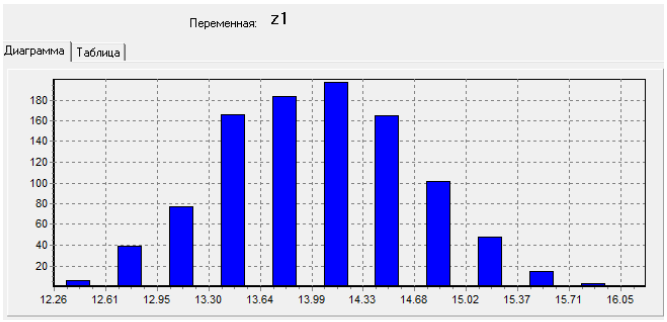
24. ГОСТ Р 50922-2006 ЗИ. Основные термины и определения. [Электронный ресурс]. URL: http://www.altell.ru/legislation/standards/50922-2006.pdf (дата обращения: 29.05.2016).
25. ГОСТ 24.702-85. Единая система стандартов автоматизированных систем управления. Эффективность автоматизированных систем управления. Основные положения. [Электронный ресурс]. URL: http://vsegost.com/Catalog/20/20041.shtml (дата обращения: 27.04.2016).
26. Маслова Н.А. Методы оценки эффективности систем защиты информационных систем: журнал «Искусственный интеллект». 2008, №4. [Электронный ресурс]. URL: http://www.nbuv.gov.ua/old_jrn/natural/II/2008_4/JournalAI_2008_4/Razdel3/07_Maslova.pdf (дата обращения: 19.05.2016).
27. Научная школа Хубаева. Математическое и имитационное моделирование экономических и информационных процессов.
28. Ефимов Е.Н. Моделирование оценок эффективности мероприятий информационной безопасности компании при воздействии случайных факторов окружающей среды: Журнал Известия ЮФУ. Технические науки. 2015, №5 [Электронный ресурс]. URL: http://cyberleninka.ru/article/n/modelirovanie-otsenok-effektivnosti-meropriyatiy-informatsionnoy-bezopasnosti-kompanii-pri-vozdeystvii-sluchaynyh-faktorov (дата обращения: 19.05.2016).
29. ГОСТ Р ИСО/МЭК 19795-1-2007. Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 1. Принципы и структура. [Электронный ресурс]. URL: http://www.gosthelp.ru/gost/gost47675.html (дата обращения: 27.04.2016).
30. ГОСТ Р ИСО/МЭК 19795-2-2008. Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии. Ча

сть 2. Методы проведения технологического и сценарного испытаний. [Электронный ресурс]. URL: http://www.gosthelp.ru/gost/gost48963.html (дата обращения: 27.04.2016).

31. ГОСТ Р ИСО/МЭК ТО 19795-3-2009. Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 3. Особенности проведения испытаний при различных биометрических модальностях. [Электронный ресурс]. URL: http://vsegost.com/Catalog/48/48632.shtml (дата обращения: 27.04.2016).
32. ГОСТ Р ИСО/МЭК ТО 19795-4-2010. Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 4. Тестирование производительности биометрических систем. [Электронный ресурс]. URL: http://vsegost.com/Catalog/17/1757.shtml (дата обращения: 27.04.2016).
33. ГОСТ Р ИСО 9000-2011. Системы менеджмента качества. Основные положения и словарь. [Электронный ресурс]. URL: http://vsegost.com/Catalog/52/52164.shtml (дата обращения: 29.05.2016).
34. Иванов В.П. Математическая оценка защищенности информации от НСД. [Электронный ресурс]. URL: http://www.bnti.ru/dbtexts/ ipks/old/analmat/1/am/ivanov/ivanov.pdf (дата обращения: 31.05.2016).

Приложение А
(рекомендуемое)

Результаты имитационного моделирования



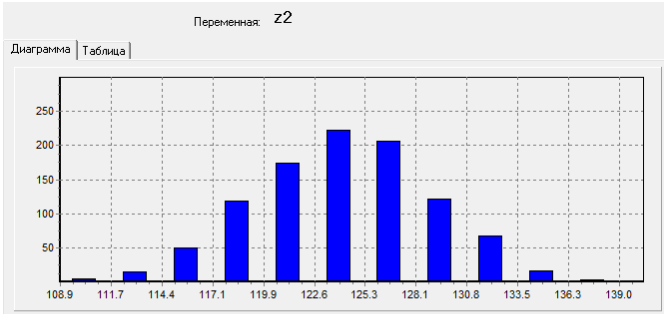
а)

Переменная: z1

Диаграмма | Таблица

Xmin	Xmax	Частота	Вероятность	Накопленная
12.26	12.61	6	0.006	0.006
12.61	12.95	39	0.039	0.045
12.95	13.30	77	0.077	0.122
13.30	13.64	166	0.166	0.288
13.64	13.99	183	0.183	0.471
13.99	14.33	197	0.197	0.668
14.33	14.68	165	0.165	0.833
14.68	15.02	101	0.101	0.934
15.02	15.37	48	0.048	0.982
15.37	15.71	15	0.015	0.997
15.71	16.05	3	0.003	1.000

б)



в)

Переменная: z2

Диаграмма | Таблица

Xmin	Xmax	Частота	Вероятность	Накопленная
108.9	111.7	5	0.005	0.005
111.7	114.4	15	0.015	0.020
114.4	117.1	50	0.050	0.070
117.1	119.9	119	0.119	0.189
119.9	122.6	174	0.174	0.363
122.6	125.3	223	0.223	0.586
125.3	128.1	206	0.206	0.792
128.1	130.8	121	0.121	0.913
130.8	133.5	68	0.068	0.981
133.5	136.3	16	0.016	0.997
136.3	139.0	3	0.003	1.000

г)

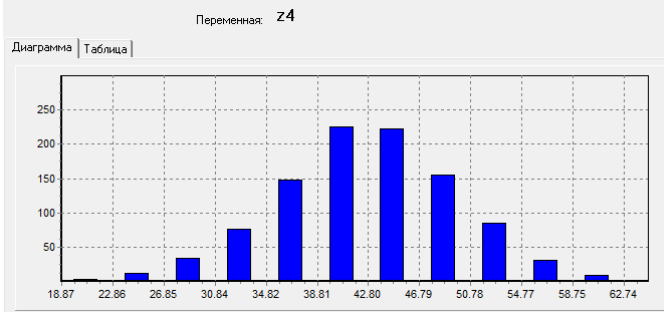
д)

Переменная: z3

Диаграмма | Таблица

Xmin	Xmax	Частота	Вероятность	Накопленная
20.18	23.13	14	0.014	0.014
23.13	26.07	41	0.041	0.055
26.07	29.02	78	0.078	0.133
29.02	31.96	150	0.150	0.283
31.96	34.90	186	0.186	0.469
34.90	37.85	215	0.215	0.684
37.85	40.79	166	0.166	0.850
40.79	43.74	83	0.083	0.933
43.74	46.68	54	0.054	0.987
46.68	49.63	10	0.010	0.997
49.63	52.57	3	0.003	1.000

е)



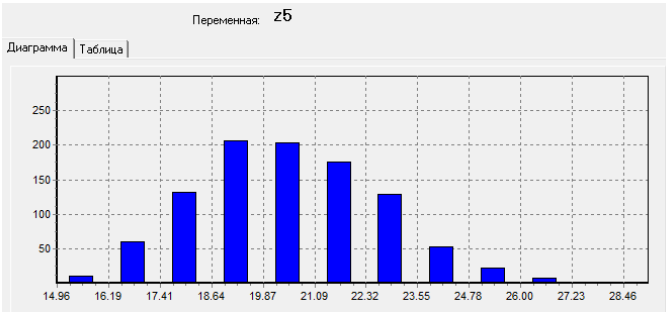
Переменная: z4

Диаграмма | Таблица

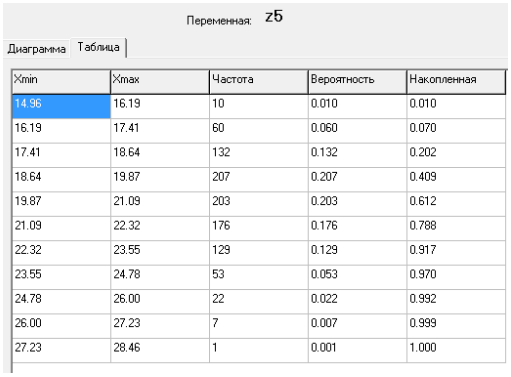
Xmin	Xmax	Частота	Вероятность	Накопленная
18.87	22.86	3	0.003	0.003
22.86	26.85	11	0.011	0.014
26.85	30.84	34	0.034	0.048
30.84	34.82	76	0.076	0.124
34.82	38.81	148	0.148	0.272
38.81	42.80	226	0.226	0.498
42.80	46.79	222	0.222	0.720
46.79	50.78	155	0.155	0.875
50.78	54.77	85	0.085	0.960
54.77	58.75	31	0.031	0.991
58.75	62.74	9	0.009	1.000

Таблица С - Результаты экспериментальных испытаний со считывателем радужной оболочки BM-ET200

Параметры	Пользователи											Ср. значение
	1	2	3	4	5	6	7	8	9	10	11	
Без каких-либо изменений	9	9	9	9	9	9	9	9	9	9	9	9
Расположение пальца чуть боком	0	3	0	0	0	9	9	8	9	0	9	4,27
Сильное надавливание на сканер	9	9	9	8	9	9	9	9	9	9	9	8,9
Слабое надавливание	9	9	9	9	9	9	9	9	8	9	9	8,9
Под углом вверх	0	4	0	3	0	2	2	2	2	0	2	1,55
Под наклоном	2	4	3	2	3	2	4	3	2	3	3	2,82
Палец теплый и немного влажный	9	8	9	9	8	8	8	9	8	9	9	8,55
Мокрый палец	7	7	7	8	8	7	6	8	7	5	7	7
Легкий слой крема на пальце	5	6	9	0	7	0	4	1	9	8	7	5,09
Палец сдвинут – не полное изображение	3	3	4	2	1	0	2	3	3	3	2	2,36

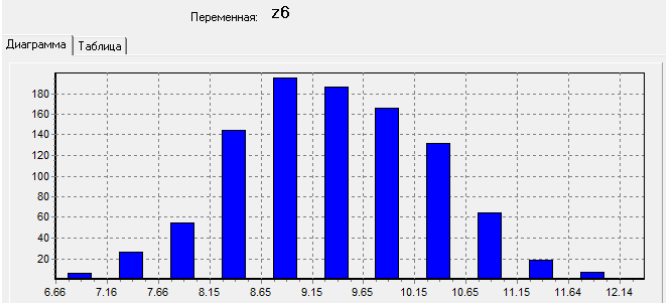


з)

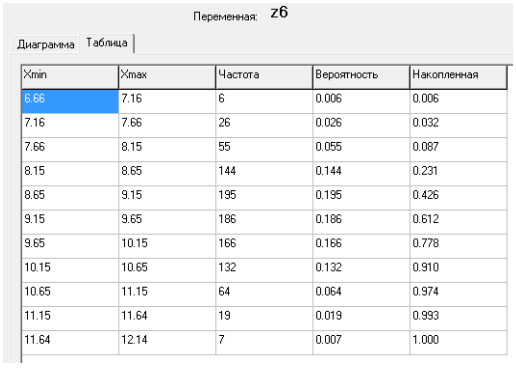


Xmin	Xmax	Частота	Вероятность	Накопленная
14.96	16.19	10	0.010	0.010
16.19	17.41	60	0.060	0.070
17.41	18.64	132	0.132	0.202
18.64	19.87	207	0.207	0.409
19.87	21.09	203	0.203	0.612
21.09	22.32	176	0.176	0.788
22.32	23.55	129	0.129	0.917
23.55	24.78	53	0.053	0.970
24.78	26.00	22	0.022	0.992
26.00	27.23	7	0.007	0.999
27.23	28.46	1	0.001	1.000

и)



й)



Xmin	Xmax	Частота	Вероятность	Накопленная
6.66	7.16	6	0.006	0.006
7.16	7.66	26	0.026	0.032
7.66	8.15	55	0.055	0.087
8.15	8.65	144	0.144	0.231
8.65	9.15	195	0.195	0.426
9.15	9.65	186	0.186	0.612
9.65	10.15	166	0.166	0.778
10.15	10.65	132	0.132	0.910
10.65	11.15	64	0.064	0.974
11.15	11.64	19	0.019	0.993
11.64	12.14	7	0.007	1.000

к)

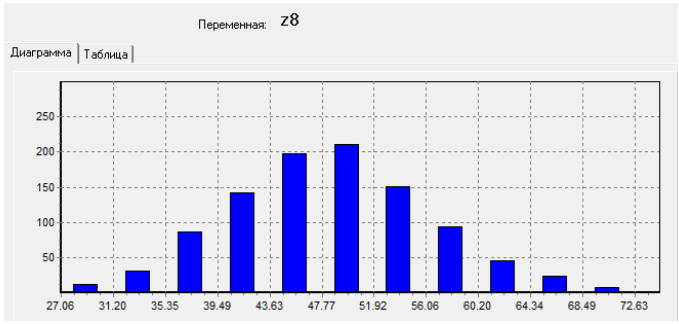
л)

Переменная: z7

Диаграмма | Таблица

Xmin	Xmax	Частота	Вероятность	Накопленная
5.434	5.719	1	0.001	0.001
5.719	6.005	8	0.008	0.009
6.005	6.291	38	0.038	0.047
6.291	6.577	87	0.087	0.134
6.577	6.862	151	0.151	0.285
6.862	7.148	220	0.220	0.505
7.148	7.434	196	0.196	0.701
7.434	7.719	164	0.164	0.865
7.719	8.005	95	0.095	0.960
8.005	8.291	27	0.027	0.987
8.291	8.577	13	0.013	1.000

м)



н)

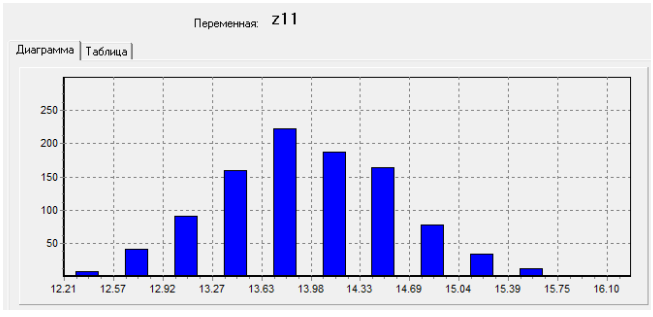
Переменная: z8

Диаграмма | Таблица

Xmin	Xmax	Частота	Вероятность	Накопленная
27.06	31.20	11	0.011	0.011
31.20	35.35	31	0.031	0.042
35.35	39.49	87	0.087	0.129
39.49	43.63	142	0.142	0.271
43.63	47.77	197	0.197	0.468
47.77	51.92	210	0.210	0.678
51.92	56.06	151	0.151	0.829
56.06	60.20	94	0.094	0.923
60.20	64.34	46	0.046	0.969
64.34	68.49	24	0.024	0.993
68.49	72.63	7	0.007	1.000

о)

Рисунок А1 – Результаты моделирования после шага 1



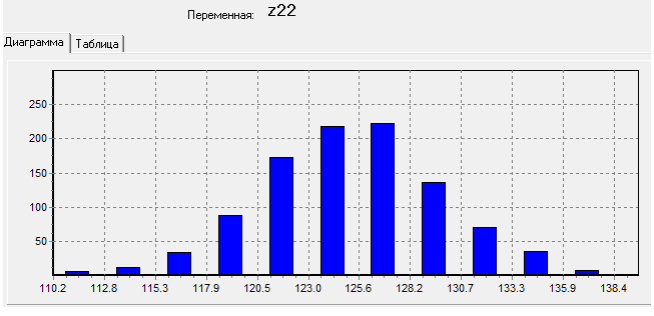
а)

Переменная: z11

Диаграмма | Таблица

Xmin	Xmax	Частота	Вероятность	Накопленная
12.21	12.57	7	0.007	0.007
12.57	12.92	41	0.041	0.048
12.92	13.27	91	0.091	0.139
13.27	13.63	160	0.160	0.299
13.63	13.98	223	0.223	0.522
13.98	14.33	188	0.188	0.710
14.33	14.69	164	0.164	0.874
14.69	15.04	78	0.078	0.952
15.04	15.39	34	0.034	0.986
15.39	15.75	12	0.012	0.998
15.75	16.10	2	0.002	1.000

б)

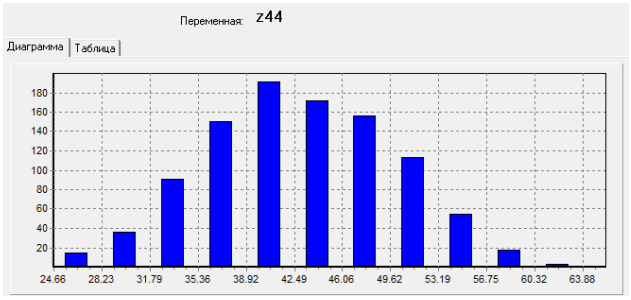


Переменная: z22

Диаграмма | Таблица

Xmin	Xmax	Частота	Вероятность	Накопленная
110.2	112.8	6	0.006	0.006
112.8	115.3	11	0.011	0.017
115.3	117.9	33	0.033	0.050
117.9	120.5	88	0.088	0.138
120.5	123.0	172	0.172	0.310
123.0	125.6	218	0.218	0.528
125.6	128.2	223	0.223	0.751
128.2	130.7	136	0.136	0.887
130.7	133.3	70	0.070	0.957
133.3	135.9	35	0.035	0.992
135.9	138.4	8	0.008	1.000

в)



г)

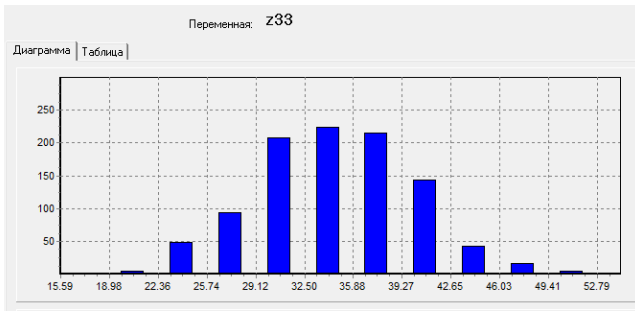
Переменная: z44

Диаграмма | Таблица

Xmin	Xmax	Частота	Вероятность	Накопленная
24.66	28.23	15	0.015	0.015
28.23	31.79	36	0.036	0.051
31.79	35.36	91	0.091	0.142
35.36	38.92	150	0.150	0.292
38.92	42.49	191	0.191	0.483
42.49	46.06	172	0.172	0.655
46.06	49.62	156	0.156	0.811
49.62	53.19	113	0.113	0.924
53.19	56.75	55	0.055	0.979
56.75	60.32	18	0.018	0.997
60.32	63.88	3	0.003	1.000

д)

е)



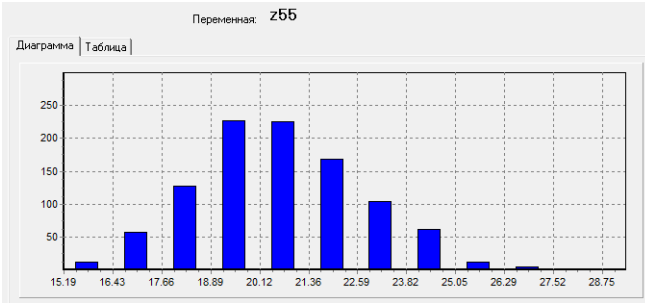
Переменная: z33

Диаграмма | Таблица

Xmin	Xmax	Частота	Вероятность	Накопленная
15.59	18.98	1	0.001	0.001
18.98	22.36	5	0.005	0.006
22.36	25.74	48	0.048	0.054
25.74	29.12	94	0.094	0.148
29.12	32.50	208	0.208	0.356
32.50	35.88	224	0.224	0.580
35.88	39.27	215	0.215	0.795
39.27	42.65	143	0.143	0.938
42.65	46.03	42	0.042	0.980
46.03	49.41	16	0.016	0.996
49.41	52.79	4	0.004	1.000

ё)

ж)



Переменная: z55

Диаграмма | Таблица

Xmin	Xmax	Частота	Вероятность	Накопленная
15.19	16.43	11	0.011	0.011
16.43	17.66	57	0.057	0.068
17.66	18.89	128	0.128	0.196
18.89	20.12	227	0.227	0.423
20.12	21.36	225	0.225	0.648
21.36	22.59	169	0.169	0.817
22.59	23.82	104	0.104	0.921
23.82	25.05	62	0.062	0.983
25.05	26.29	11	0.011	0.994
26.29	27.52	5	0.005	0.999
27.52	28.75	1	0.001	1.000

з)

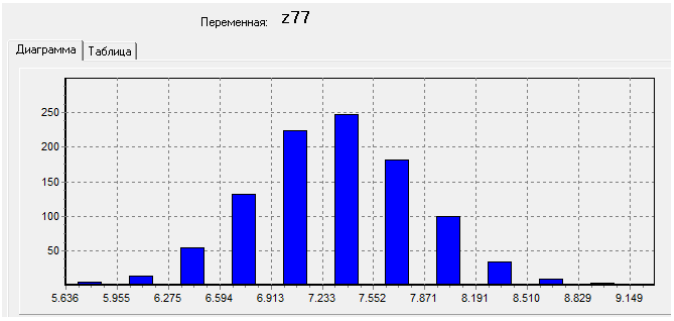
и)

Переменная: z66

Диаграмма | Таблица

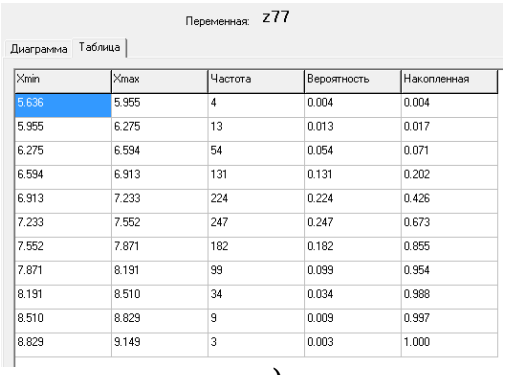
Xmin	Xmax	Частота	Вероятность	Накопленная
6.90	7.40	8	0.008	0.008
7.40	7.90	38	0.038	0.046
7.90	8.40	77	0.077	0.123
8.40	8.90	148	0.148	0.271
8.90	9.39	187	0.187	0.458
9.39	9.89	213	0.213	0.671
9.89	10.39	142	0.142	0.813
10.39	10.89	114	0.114	0.927
10.89	11.39	46	0.046	0.973
11.39	11.89	19	0.019	0.992
11.89	12.39	8	0.008	1.000

й)



л)

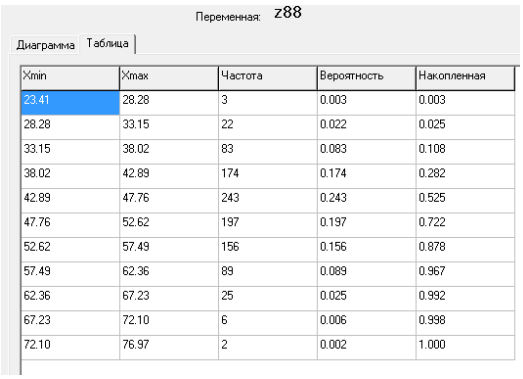
к)



Xmin	Xmax	Частота	Вероятность	Накопленная
5.636	5.955	4	0.004	0.004
5.955	6.275	13	0.013	0.017
6.275	6.594	54	0.054	0.071
6.594	6.913	131	0.131	0.202
6.913	7.233	224	0.224	0.426
7.233	7.552	247	0.247	0.673
7.552	7.871	182	0.182	0.855
7.871	8.191	99	0.099	0.954
8.191	8.510	34	0.034	0.988
8.510	8.829	9	0.009	0.997
8.829	9.149	3	0.003	1.000

м)

н)



Xmin	Xmax	Частота	Вероятность	Накопленная
23.41	28.28	3	0.003	0.003
28.28	33.15	22	0.022	0.025
33.15	38.02	83	0.083	0.108
38.02	42.89	174	0.174	0.282
42.89	47.76	243	0.243	0.525
47.76	52.62	197	0.197	0.722
52.62	57.49	156	0.156	0.878
57.49	62.36	89	0.089	0.967
62.36	67.23	25	0.025	0.992
67.23	72.10	6	0.006	0.998
72.10	76.97	2	0.002	1.000

о)

Рисунок А2 – Результаты моделирования после шага 2

Приложение Б
(обязательное)

Результаты экспериментальных испытаний со считывателем радужной оболочки

Таблица Б1 - Результаты экспериментальных испытаний со считывателем радужной оболочки ВМ-ЕТ200

Параметры	Пользователи											Ср. значение
	1	2	3	4	5	6	7	8	9	10	11	
Без каких-либо изменений	9	9	9	9	9	9	9	9	9	9	9	9
Расположение пальца чуть боком	0	3	0	0	0	9	9	8	9	0	9	4,27
Сильное надавливание на сканер	9	9	9	8	9	9	9	9	9	9	9	8,9
Слабое надавливание	9	9	9	9	9	9	9	9	8	9	9	8,9

Под углом вверх	0	4	0	3	0	2	2	2	2	0	2	1,55
Под наклоном	2	4	3	2	3	2	4	3	2	3	3	2,82
Палец теплый и не много влажный	9	8	9	9	8	8	8	9	8	9	9	8,55
Мокрый палец	7	7	7	8	8	7	6	8	7	5	7	7
Легкий слой крема на пальце	5	6	9	0	7	0	4	1	9	8	7	5,09
Палец сдвинут – не полное изображение	3	3	4	2	1	0	2	3	3	3	2	2,36

Приложение В
(обязательное)

Результаты экспериментальных испытаний со сканером отпечатков пальцев

Таблица В1 - Результаты экспериментальных испытаний со сканером отпечатков пальцев Fingkey Hamster

Параметры	Пользователи											Ср. значение
	1	2	3	4	5	6	7	8	9	10	11	
Очки, искусственное освещение	1	1	1	0	0	0	1	1	1	1	1	0,73
Очки, дневной свет	1	1	1	0	0	1	1	1	1	1	1	0,82
Очки, попадание солнечного света	0	0	0	0	0	0	0	0	0	0	0	0
Без очков, искусственное освещение	1	1	1	1	1	0	1	1	1	1	1	0,9
Без очков, дневной свет	1	1	1	1	1	1	1	1	1	1	1	1
Без очков, попадание солнечного света	0	0	0	0	0	0		0	0	0	0	0
Линзы, искусственное освещение	-	-	-	-	-	0	1	1	1	1	1	0,84
Линзы, дневной свет	-	-	-	-	-	1	1	1	1	1	1	1
Линзы, попадание солнечного света	-	-	-	-	-	0	0	0	0	0	0	0