Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
(ФГБОУ ВО «АмГУ»)

Факультет Математики и информатики

Кафедра Информационных и управляющих систем

Направление подготовки 09.03.02 «Информационные системы и технологии»

Направленность (профиль) образовательной программы Безопасность информационных систем

ДОПУСТИТЬ К ЗАЩИТЕ

И.о.зав.кафедрой

_____ А.В. Бушманов

«07» 07 2020г.

БАКАЛАВРСКАЯ РАБОТА

на тему: Разработка ПО, обеспечивающего безопасность помещения с помощью «умных вещей»

Исполнитель
студент группы 655 _____ (подпись, дата) А.А. Филимонова

Руководитель
доцент, канд.техн.наук _____ (подпись, дата) С.Г. Самохвалова

Консультант по безопасности
и экологичности
доцент, канд.техн.наук 19.06.2020 _____ (подпись, дата) А.Б. Булгаков

Нормоконтроль
доцент, канд.техн.наук _____ (подпись, дата) О.В. Жилиндина

Благовещенск 2020

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
(ФГБОУ ВО «АмГУ»)

Факультет Математики и информатики

Кафедра Информационных и управляющих систем

УТВЕРЖДАЮ
И.о.зав.кафедрой
А.В. Бушманов
«10» 02 2020г.

ЗАДАНИЕ

К выпускной квалификационной работе студента Филимоновой Алины Андреевны

Тема выпускной квалификационной работы: Разработка ПО, обеспечивающего безопасность помещения с помощью «умных вещей».

(утверждена приказом от 30.04.2020 № № 810-уч)

1. Срок сдачи студентом законченной работы 26.06.2020
2. Содержание выпускной квалификационной работы: область применения; инструментарий для разработки; практическая реализация программного продукта; безопасность и экологичность.
3. Перечень материалов приложения: Схема общего алгоритма, схема жизненного цикла базовых компонентов, листинг программы, снимок результата, структурное описание используемых классов.
4. Дата выдачи задания 20.02.2020

Руководитель бакалаврской работы: Самохвалова Светлана Геннадьевна, доцент, канд. техн. наук.

Задание принял к исполнению А.А. Филимонова

РЕФЕРАТ

Бакалаврская работа содержит 66 с., 16 рисунков, 3 приложения, 20 источников.

БЕЗПАСНОСТЬ ИНФОРМАЦИИ, ЗАЩИТА ИНФОРМАЦИИ, ХРАНЕНИЕ ДАННЫХ, ЗАЩИТА НОСИТЕЛЯ ИНФОРМАЦИИ, ПРОРАММНОЕ ОБЕСПЕЧЕНИЕ, КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ, ИНТЕРФЕЙС, УГРОЗЫ, НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП К ИНФОРМАЦИИ

Целью бакалаврской работы является разработка программного обеспечения, обеспечивающего безопасность помещения с помощью «умных вещей», с возможность отображения данных о погоде, о системе, на которой запускается приложение, зашифровкой текстовых данных с помощью криптографического метода ГОСТ 28147-89, добавлением устройств и отображения изменений журала ОС.

Объектом исследования является деятельность Амурского филиала ПАО «Ростелеком» в г. Благовещенск.

В бакалаврской работе разработано программное приложение «IoT - security», обеспечивающее решение проблемы защищенности информации. В современном мире такое решение представляется актуальным, поскольку приводит к уменьшению рисков несанкционированных действий по отношению к конфиденциальной инфорамции, с последующими кражей, копированием или изменением. ПО «IoT - security» включает в себя модуль криптографической защиты, модуль хранилища и модули сбора данных. Каждый из модулей направлен на решение конретной поставленной задачи.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В современном обществе происходит постоянный обмен информации, как на виртуальном, так и на естественном, физиологическом уровне. При этом степень защищенности от несанкционированного нападения злоумышленника с последующим взломом и кражей данных, подслушиванием или съемом, не прогрессирует, подвергая опасности наши конфиденциальные данные и безопасность личной жизни. С ростом внедрения такой технологии, как интернет вещей во все сферы жизни, проблема незащищенности информации становится всё актуальнее.

В большинстве случаев, в корне проблемы лежат такие человеческие факторы, как бездействие и информационная безграмотность. Во всех приборах, которые можно отнести к классу «умных», лежит передача данных через сеть Интернет или по радиоканалам. Как правило, у большинства приборов есть базовая парольная защита, которую зачастую настраивают на заводе производителя. Халатность пользователей позволяет даже самому неопытному злоумышленнику найти стандартные данные парольной системы, используемые на заводах производителей. Соответственно, достаточно знать модель вашего «умного» чайника, чтобы взломать его систему управления и завладеть вашими данными.

Архитектура многих устройств зачастую уязвима. Не все «умные» устройства могут корректно взаимодействовать между собой. Для технологии интернета вещей определены три основные характеристики - комплексные знания, надежная передача и интеллектуальная обработка. Как правило, структура «умных вещей» соответственно может делиться на уровень восприятия, сетевой уровень и прикладной уровень.

Так же важным аспектом защищенности помещения является выявление возможных каналов утечки информации в помещении. К ним относятся такие технические канала как: акустические каналы, оптические каналы,

акустоэлектрические каналы, виброакустические (телефонные) каналы и ПЭМИН.

В бакалаврской работе разработано ПО «IoT-security», обеспечивающее решение проблемы защиты информации с помощью технологии интернета вещей. Для предприятий такое решение представляется актуальным, поскольку снижает риск взлома, кражи и замены данных. ПАО «Ростелеком» тесно сотрудничает с корпорациями и государственными организациями, а также владеет большим количеством персональных данных, что делает офис компании привлекательным для злоумышленников. К циркулирующим данным в организации относятся:

a) персональные данные пользователей;
b) данные представляющие коммерческих характер;
c) технические данные организации;
d) проектные данные и т.д.

Большое количество информации, в том числе и конфиденциальные данные, зачастую озвучиваются или визуально демонстрируются в кабинете директора компании. Это самое уязвимое место во всей организации с колоссальной циркуляцией данных. Подобные помещения представляют угрозу безопасности и должны быть спроектированы высококвалифицированными специалистами в области обеспечения информационной безопасности. Данное ПО позволит обеспечить в таком помещение безопасность информации.

1 АНАЛИЗ ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЯ

1.1 Общая характеристика

Предприятием для разработки ПО был выбран Амурский филиал ПАО «Ростелеком» в г. Благовещенск (далее «Ростелеком» или организация). Организация предоставляет все виды услуг связи на территории Амурской области:

a) Местная, внутризоновая телефонная и телеграфная связь, IP-телефония;
b) Предоставление в аренду каналов связи и физических линий;
c) Передача данных и услуги сети Интернет;
d) Интерактивное телевидение.

Фактический адрес организации: Амурска область, г. Благовещенск, ул. Пионерская, 40. Телефон: 391-277. На сайте организации www.amur.rt.ru можно ознакомиться с подключаемыми услугами и сервисами, отправить заявку на подключение, оплатить счет, оплатить госуслуги: штрафы и налоги, ознакомиться с новостями компании и даже пройти обучение. Организация является крупнейшим в России провайдером цифровых услуг и решений. Сотрудничает с частными лицами, корпорациями и госучреждениями.

1.2 Организационная структура предприятия

Главным управляющим органом организации является совет директоров. Во главе стоит генеральный директор компании, который осуществляет руководство всей производственной, хозяйственной и финансовой деятельностью компании, организует всю работу, несёт полную ответственность за его состояние и результаты деятельности. Генеральный директор руководит предприятием с помощью заместителей и помощников.

На рисунке А.1 представлена диаграмма организационной структуры предприятия.

1.3 Функциональная структура предприятия

Предприятия зачастую выбирают функциональный подход для формирования подразделений. Под функциями, в данном случае, понимаются главные направления деятельности.

На контекстной диаграмме, представленной на рисунке Б.1, отображаются объекты и информационные потоки, определяющие деятельность предприятия. Основными входящими потоками для компании являются:

a) Заявки клиентов на оказание услуг (телевидение, телефонная связь, Интернет и т. д.);
b) Государственные и корпоративные заявки на оказание услуг (монтаж ЛВС, инсталляция ИС и ПО и т.д.);
c) Персональные данные участников отношений (банковские реквизиты, фактические места проживания, ФИО, контактные номера и т.д.).

К основным выходящим потокам относятся:

a) Провайдерские услуги;
b) Информационные системы и программное обеспечение;
c) Линии связи;
d) Телефонная связь;
e) Интерактивное телевидение.

На контекстной диаграмме также отражены управления и механизмы. В роли управления выступают регламент и методы, устав и Законодательство РФ. В роли механизмов выступают персонал предприятия, аппаратное обеспечение и информационные технологии.

Для более детального функционального анализа предприятия следует декомпозировать контекстную диаграмму. Декомпозиция основного блока представлена на рисунке Б.2. Функционирование рассматриваемого предприятия можно разделить на функционирование следующих отделов, отвечающих за бизнес-процессы:

a) Технический отдел;
b) Отдел продаж и обслуживания клиентов;
c) Отдел монтажных работ и инсталляции;
d) Отдел по работе с государственными и коммерческими проектами;
e) Отдел рекламы;
f) Отдел разработки и управления продуктами.

Для полноты сведений о рассматриваемом предприятии также был произведен анализ внешнего и внутреннего документооборота. В результате анализа была составлена контекстная диаграмма, представленная в приложениях В.1 и В.2.

1.4 Границы предметной области

Создаваемое программное обеспечение предназначено для защиты информации внутри служебного помещения, а именно кабинета директора компании. Защиту необходимо предусмотреть как на физическом уровне, так и на техническом. Поэтому анализу подлежит та часть предметной области, которая непосредственно касается защищенности помещения и обнаружению возможных каналов утечки информации. Для оценки защищенности помещения, необходимо провести анализ риска возможных утечек информации через различные каналы связи, а также соответственно определить меры защиты и профилактики, в том числе криптографические. Необходимо также понимать модель возможных угроз на предприятии и модель потенциального нарушителя безопасности.

2 ИССЛЕДОВАНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1 Анализ комплекса информационных и технических средств

Компания ПАО «Ростелеком» оснащена современными средствами хранения, обработки и передачи информации. На предприятии интегрированы различные сетевые технологии. Имеется локальная вычислительная сеть, соединяющая компьютеры отделов и сервер печати и обеспечивающая доступ к Интернету. Основным программным продуктом, использующимся в работе всего предприятия, является программный комплекс «1С: Предприятие», предназначенный для организаций. Он обеспечивает учет клиентов, поставщиков, оборудования, производимых и продаваемых продуктов, формирование приемных квитанций, актов выполненных работ, отчетов об оказании услуг. Также на каждом пользовательском компьютере имеется антивирус «Касперского», а также разграничение по учетным записям прав доступа.

2.2 Анализ уровня безопасности

Для программного обеспечения безопасность проявляется как свойство функционировать без проявления негативных последствий для конкретной компьютерной системы. Уровнем безопасности же является вероятность получения функционально корректного результата при заданных условиях.

Система обеспечения безопасности всех компонентов ПО в первую очередь должна носить конфиденциальный характер. Предварительно обязана быть обеспечена постоянным, а главное, комплексным контролем деятельность как всех разработчиков, так и простых пользователей компонентов. Кроме общих принципов, также необходимо конкретизировать принципы обеспечения безопасности ПО на каждом этапе его жизненного цикла. Это обмуслено тем, что негативное воздействие с помощью различных способов возможно на любой стадии жизненного цикла, а значит необходимо взять под особый контроль обеспечение безопасности на всех стадиях.

Таблица 1 – Принципы обеспечения безопасности По на этапах жизненного цикла

Принцип обеспечения технологической безопасности при обосновании, планировании работ и проектном анализе ПО	Комплексность обеспечения безопасности ПО, рассматривающее проблемы безопасности информационных и вычислительных процессов, а также обнаружения, времени и условий возникновения возможных каналов утечки информации и несанкционированного доступа к ней.
	Планирование переноса акцента на совместное системное проектирование ПО и средств его безопасности, а также планирование их использования в условиях эксплуатации.
	Обоснование средств обеспечения безопасности ПО.
	Достаточность безопасности программ, отражающая необходимость поиска эффективных и надежных мер безопасности при параллельной минимизации их стоимости.
	Гибкое управление защитой программ.
	Заблаговременное обеспечение технологической безопасности работ.
	Документируемость технологии создания программ, подразумевающей разработку пакета нормативно-технических документов по контролю программных средств на наличие преднамеренных дефектов.
Принципы достижения технологической безопасности ПО в процессе его разработки.	Регламентация технологических этапов разработки ПО.
	Автоматизация средств контроля на наличие дефектов.

Продолжение таблицы 1

1	2
	Осуществление последовательной фильтрации по время создания программных модулей.
	Типизация алгоритмов, программ и средств информационной безопасности.
	Централизованное управление базами данных проектов ПО и администрирование технологии их разработки с жестким разграничением функций, ограничением доступа в соответствии со средствами диагностики, контроля и защиты;
	Ведение системных журналов процессов разработки ПО, а также статистический учет
	Использование сертифицированных и единых инструментальных средств разработки программ.
Принципы обеспечения технологической безопасности на этапах стендовых и приемосдаточных испытаний.	Тестирование ПО на основе разработки комплексов тестов.
	Проведение программных испытаний с имитацией воздействия активных дефектов.
	Фильтрация программных комплексов с целью выявления дефектов.
	Разработка средств верификации программных изделий и сертификация по требованиям безопасности.
	Проведение испытаний ПО для определения программных ошибок проектирования и разработки и выявление потенциально уязвимых мест.
	Отработка средств защиты от несанкционированного воздействия.

Продолжение таблицы 1

1	2
Принципы обеспечения безопасности при эксплуатации программного обеспечения.	Сохранение и ограничение доступа к эталонам программных средств, недопущение внесения изменений в них.
	Профилактическое тестирование программных средств на наличие преднамеренных дефектов.
	Идентификация ПО на момент ввода его в эксплуатацию в соответствии с предполагаемыми угрозами безопасности ПО и его контроль.
	Обеспечение модификации программных изделий во время их эксплуатации.
	Строгий учет и каталогизации всех сопровождаемых программных средств, а также собираемой, обрабатываемой и хранимой информации.
	Статистический анализ информации обо всех процессах и рабочих операциях ПО.
	Гибкое применение дополнительных средств защиты ПО в случае выявления новых, непрогнозируемых угроз информационной безопасности.

2.3 Определение источников угроз

Существует большое количество событий, которые могут быть причиной для неправильной работы программы. К подобного рода событиям относятся такие факторы как: сбои компьютерных систем, ошибки программистов и операторов, дефекты в ПО (преднамеренные и непреднамеренные). Преднамерен-

ные дефекты, как правило, появляются в результате злоумышленных действий, в то время как непреднамеренные - ошибочных действий человека.

Правильное определение угроз безопасности информации необходимо для установления существования возможности нарушения конфиденциальности, целостности или доступности информации и приведет ли нарушение хотя бы одного из свойств безопасности информации к наступлению негативных последствий для обладателя информации.

Для оценки угроз безопасности информации необходимо воспользоваться проведением экспертного метода. Рекомендации по формированию экспертной группы и проведению экспертной оценки приведены в методике определения угроз безопасности информации в информационных системах, утверждённой ФСТЭК России. Также необходимо уметь определять тип угроз на всех стадиях жизненного цикла ПО.

Таблица 2 – Угрозы на стадиях жизненного цикла ПО

Стадии ЖЦ		Угрозы
Проектирование	Проектные решения	Злоумышленный выбор нерациональных алгоритмов работы.
	Используемые информационные технологии	Внедрение информационных технологий или их элементов, содержащих программные закладки.
		Внедрение неоптимальных информационных технологий.
	Используемые аппаратно-технические средства	Поставка вычислительных средств, содержащих программные, аппаратные или программно-аппаратные закладки.
		Поставка вычислительных средств с низкими характеристиками или имеющих высокий уровень экологической опасности.

Продолжение таблицы 2

1	2	3
	Задачи коллективов разработчиков и их персональный состав	Внедрение злоумышленников в коллективы разработчиков программных и аппаратных средств.
		Вербовка сотрудников путем подкупа, шантажа.
Кодирование	Архитектура программной системы	Доступ к "чужим" подпрограммам и данным.
		Нерациональная организация вычислительного процесса.
		Организация переадресации команд, запись информации в используемые программной системой ячейки памяти.
	Функции кодируемой части программной системы.	Формирование программной закладки, воздействующей на другие части или изменяющей структуру программной системы.
		Организация замаскированного спускового механизма программной закладки.
	Технология записи программного обеспечения и исходных данных	Поставка программного обеспечения и технических средств со встроенными дефектами или закладками.
Отладка и испытания	Функционирование и архитектура программной системы	Встраивание программной закладки в программную систему.

Продолжение таблицы 2

1	2	3
		Формирование программной закладки с динамически формируемыми командами.
		Организация переадресации отдельных команд программной системы.
	Сведения о процессе испытаний	Формирование набора тестовых данных, не позволяющих выявить программную закладку.
		Формирование программной закладки, не обнаруживаемой с помощью используемой модели объекта.
		Вербовка сотрудников коллектива, проводящих испытания.
Контроль	Используемые процедуры и методы контроля	Формирование спускового механизма программной закладки, не включающего ее при контроле на безопасность.
		Маскировка программной закладки путем внесения в программную систему ложных непреднамеренных дефектов.
		Формирование программной закладки в ветвях программной системы, не проверяемых при контроле.
		Формирование вирусных программ, не позволяющих выявить их внедрение в программную систему путем контрольного суммирования

Продолжение таблицы 2

1	2	3
Эксплуатация	Сведения о персональном составе контролирующего подразделения	Внедрение злоумышленников в контролирующее подразделение и вербовка его сотрудников
		Сбор информации о испытываемой программной системе
	Сведения об обнаруженных незлоумышленных дефектах и программных закладках, о доработках программной системы, о среде функционирования программной системы и ее изменениях	

Интернет вещей является быстро развивающимся сегментом информационных технологий, что не может отображаться на росте угроз информационной безопасности. Корпорация Dr.WEB привела статистику зафиксированных атак на различные устройства, поддерживающие технологию интернета вещей.

Рисунок 1 – Статистика роста вирусных атак

На приведенной выше статистике четко виден рост вирусных атак с 2016 года до 2 квартала 2019 года. Как видно, только за полгода количество атак приблизилось к годовому значению 2018 года. Также важным является резкий скачок количества вирусных атак за 2018 год. По сравнению с 2017 годом циф-

ра увеличилась в 14 раз. Все выше описанное демонстрирует колоссальный рост интереса злоумышленников к миру интернета вещей. Нельзя не отметить, что по прогнозам многих корпораций и специалистов в области информационной безопасности в ближайшем время соответсвенно можно ожидать только рост атак на сферу интернета вещей.

Вредоносные программы, атакующие устройства с технологией интернета вещей можно разделить на несколько базовых категорий в соответствии с их основными функциями:

a) троянцы для проведения DDoS-атак;

b) троянцы, которые распространяют, загружают и устанавливают другие вредоносные приложения и вспомогательные компоненты;

c) троянцы, позволяющие удаленно управлять зараженными устройствами;

d) троянцы, превращающие устройства в прокси-серверы;

e) троянцы для майнинга криптовалют и т.д.

Следует понимать, что большое количество современных вредоносных программ представляют собой многофункциональные угрозы, поскольку многие из них могут сочетать в себе сразу несколько функций. Можно выделить сформировавшиеся тенденции в сфере угроз для интернета вещей:

a) рост количества новых вредоносных программ из-за доступности исходных кодов троянцев;

b) появление все большего числа вредоносных приложений, написанных на «нестандартных» языках программирования, например, Go и Rust;

c) доступность информации о множестве уязвимостей, эксплуатация которых помогает заражать устройства;

d) сохранение популярности так называемых майнеров, добывающих криптовалюты на устройствах интернета вещей.

2.4 Определение вероятного нарушителя безопасности

Для офиса крупного Интернет-провайдера, в соответствии с определением возможных нарушителей информационной безопасности от ФСТЭК России, можно выделить следующие виды возможных нарушителей:

Таблица 3 – Модели нарушителя информационной безопасности

Виды нарушителя	Типы нарушителя	Возможные цели
Внешние субъекты (физические лица)	Внешний	Идеологические или политические мотивы. Причинение ущерба путем мошенничества или иным преступным путем.
Конкурирующие организации	Внешний	Получение конкурентных преимуществ. Причинение ущерба путем обмана или злоупотребления доверием
Разработчики, производители программных, технических и программно-технических средств	Внешний	Внедрение дополнительных функциональных возможностей в программное обеспечение на этапе разработки. Непреднамеренные действия
Лица, привлекаемые для установки, наладки, монтажа	Внутренний	Причинение ущерба путем обмана или злоупотребления доверием. Непреднамеренные действия
Лица, обеспечивающие функционирование ИС или обслуживающие инфраструктуру	Внутренний	Причинение ущерба путем обмана или злоупотребления доверием. Непреднамеренные действия

Продолжение таблицы 3

1	2	3
Пользователи информационной системы	Внутренний	Причинение ущерба путем мошенничества или иным преступным путем. Месть за ранее совершенные действия. Непреднамеренные действия
Администраторы информационной системы и администраторы безопасности	Внутренний	Причинение ущерба путем мошенничества или иным преступным путем. Месть за ранее совершенные действия. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды. Непреднамеренные действия
Бывшие работники (пользователи)	Внешний	Причинение ущерба путем мошенничества или иным преступным путем. Месть за ранее совершенные действия
Преступные группы (криминальные структуры)	Внешний	Причинение ущерба путем мошенничества или иным преступным путем. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды

Четко определенный потенциал нарушителя необходим для определения его возможностей. В свою очередь, потенциал нарушителя формируется такими свойствами как компетентность, ресурсы и мотивация и разделяется на не-

сколько категорий: базовый (низкий), базовый повышенный (средний) и высокий.

Исполнение угроз безопасности информации реализуется за счет:

a) несанкционированного доступа и (или) воздействия на объекты на аппаратном уровне;

b) несанкционированного доступа и (или) воздействия на общесистемном уровне на базовые системы ввода-вывода и операционные системы;

c) несанкционированного доступа и (или) воздействия на прикладном уровне на системы управления базами данных, браузеры, web-приложения и иные прикладные программы общего и специального назначения;

d) несанкционированного доступа и (или) воздействия на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы);

e) несанкционированного физического доступа и (или) воздействия на линии, (каналы) связи, технические средства и машинные носители информации;

f) воздействия на пользователей, администраторов безопасности, администраторов информационной системы или обслуживающий персонал (социальная инженерия).

2.5 Определение архитектуры интернета вещей

Структура интернета вещей является сложной задачей. Это означает, что необходимо создание такой архитектуры, которая бы специфицировала основные компоненты и их взаимосвязь. Архитектура интернета вещей предоставляет следующие преимущества:

a) служить ориентиром для разработчиков в плане того, какие функции нужны в интернете вещей и как они взаимодействуют;

b) служить основой для стандартизации, стимулируя совместимость и сокращение расходов.

Популярность интернета вещей в мире с каждым годом возрастает и в дальнейшем будет только увеличиваться. Что предоставляет для злоумышленников масштабное поле для деятельности. На рисунке 2 представлен график роста распространённости интернета вещей в мире в биллионах.

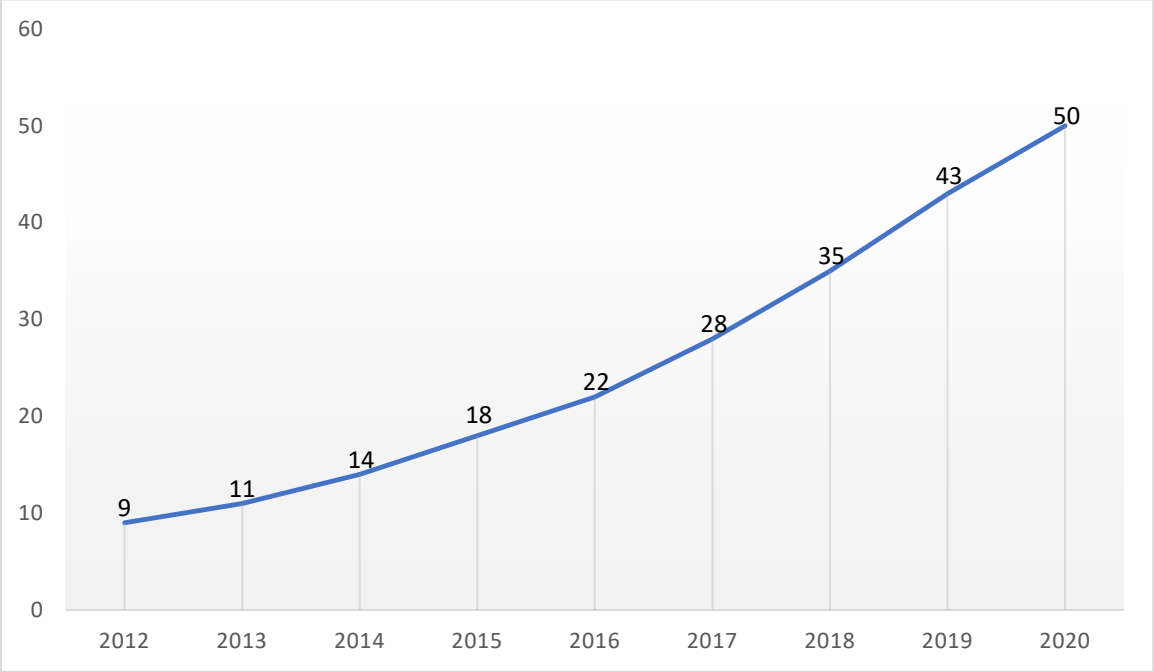

Рисунок 2 – Распространённость Интернета Вещей в мире

При этом сложность архитектуры интернета вещей также возрастает, но в тоже время до сих пор нет четного понимания об осуществлении безопасности информации для устройств поддерживающих эту технологию из-за большого количества применяемых моделей. Поэтому важность правильно составленной эталонной архитектуры интернета вещей занимает высокое место для обеспечения информационной безопасности.

2.5.1. Модель МСЭ-Т

Существует эталонная модель интернета вещей от МСЭ-Т, описание которой есть в рекомендациях Y.2060. Основным отличием от большинства дру-

гих моделей является то, что модель от МСЭ-т детализирует фактические физические компоненты экосистемы интернета вещей, что позволяет увидеть элементы экосистемы интернета вещей, которые должны быть соединены, интегрированы, управляемы и предоставлены приложениям.

Важным свойством, на которое заостряет внимание модель является то, что интернет вещей является определённой сетью устройств, взаимодействующих с физическими вещами, на ряду с прикладными платформами, такими как компьютеры, планшеты и смартфоны, которые, в свою очередь, взаимодействуют с этими устройствами.

В Рекомендации Y.2060 выделяют тот факт, что технологии, используемые для взаимодействия между устройствами как сбора данных, так и переноса данных, а также какими-либо носителями данных, включают такие возбуждения как оптическое, инфракрасное, радиочастотное, и гальваническое. Также следует выделить устройства общего назначения, которые обладают возможностями обработки данных и связи. Наиболее ярким примером можно считать технологии «умного дома», которые могут интегрировать большое количество различных устройств в единую сеть для централизованного или дистанционного управления.

2.5.2. Эталонная модель Всемирного форума IoT (IWT)

В 2014 году комитет по архитектуре Всемирного форума интернета вещей, составленный из лидеров индустрии информационных технологий, опубликовал эталонную модель интернета вещей, которую можно назвать общей структурой, предназначенной для того, чтобы стимулировать сотрудничество и способствовать созданию повторяемых моделей внедрения.

Данная эталонная модель является дополнением к модели МСЭ-Т. Документы МСЭ-Т делают упор на уровнях устройства и шлюза, описывая верхние уровни лишь в общих чертах, в то время как предложенная на форуме модель имеет иерархию из семи уровней:

а) Сотрудничество и процессы (включение людей и бизнес — процессов);

b) Приложения (отчеты, статистика и управление);

c) Абстракция данных (агрегация и доступ);

d) Накопление данных (устройства хранения данных);

e) Туманные вычисления (анализ элементов данных и преобразования);

f) Связь (передача и процессоры);

g) Физические устройства и контроллеры.

Модель имеет следующие характеристики:

a) упрощение: разбивает сложные системы на части для упрощения их понимания;

b) прояснение: предоставляет дополнительные сведения для точной идентификации уровней интернета вещей и выработки общей терминологии;

c) идентификация: определяет аспекты, в которых для различных частей системы типы обработки оптимизированы;

d) стандартизация: представляет собой основу для того, чтобы поставщики могли создавать продукты интернета вещей, способные взаимодействовать друг с другом;

e) организация: делает интернет вещей реальным и доступным, а не просто абстрактной концепцией.

Компания IWT считает эталонную модель интернета вещей принятой в отрасли базовой структурой, направленной на стандартизацию концепций и терминологии, связанных непосредственно с интернетом вещей.

3 АНАЛИЗ ЗАЩИТЫ ОТ УТЕЧКИ ИНФОРМАЦИИ

3.1 Анализ рисков утечки информации

Утечка информации представляет большую угрозу для предприятия, которая может произойти по причинам неосторожности и невнимательности сотрудников организации или из-за отрицательного замысла третьих лиц.

Для умышленной утечки информации характерны две цели:

a) это нанесение ущерба предприятию или обществу,

b) получение преимущества и тайных сведений конкурентами.

Непреднамеренная утечка происходит в основном по неосторожности сотрудников организации.

Аналитический центр InfoWatch провел статистический анализ зарегистрированных случаев утечки информации с 2006 года по 2019 год. За 13 лет число зарегистрированных случаев выросло в 10 раз. Это обусловлено ростом сферы информационных технологий и увеличением циркулирующей в ней информации за этот период времени. За 2019 год произошел довольно высокий скачок количества зарегистрированных случаев утечки информации по сравнению с приростом прошлых лет. Это можно связать с популяризацией устройств, поддерживающих технологию умных вещей, потому что за 2019 год было произведено большое количество устройств из интернета вещей, что сделало их более доступными для основной полосы населения, чья несерьезность по отношению к базовым принципам информационной безопасности могла сыграть определенную отрицательную роль. В дальнейшем, кривая регистрации случаев будет только увеличиваться и, возможно, в 2020 году будет ещё больший скачок по сравнению с 2019 годом. Все выше перечисленное только подчеркивает важность комплексного подхода к информационной безопасности, в том числе противодействие угрозам утечки информации через технические каналы связи.

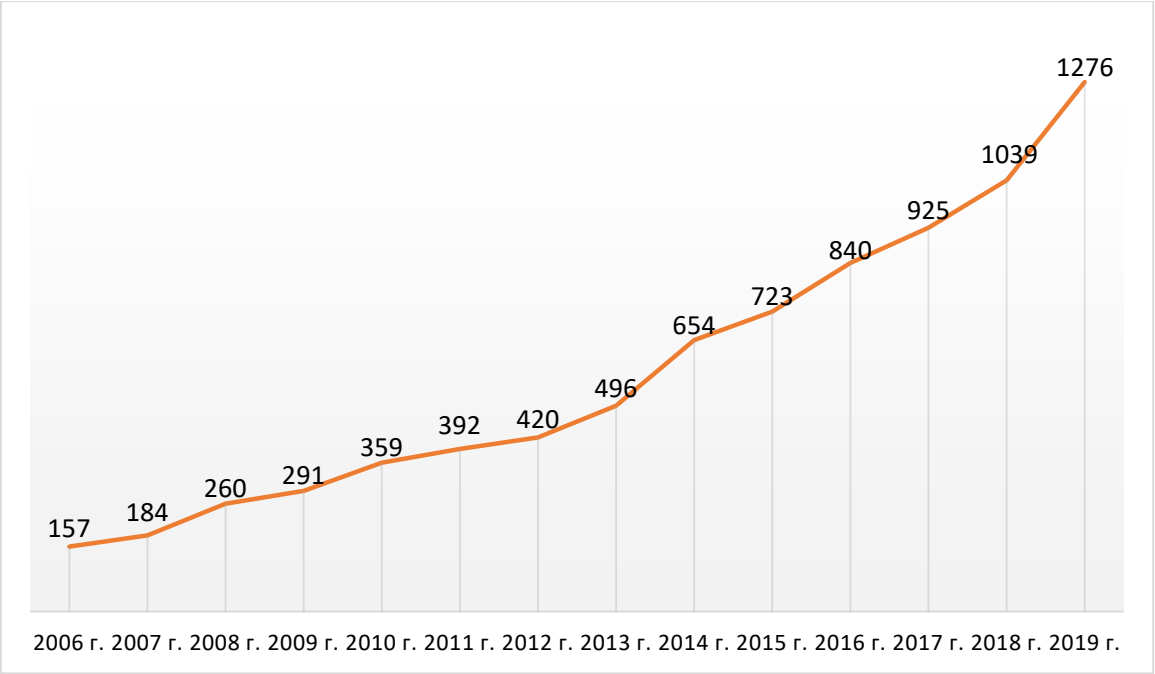

Рисунок 3 – График роста регистрации случаев утечки информации

Следует отметить, что также был проведен анализ причин зарегистрированных случаев. На рисунке 3 представлена диаграмма процентного соотношения причин утечек информации от общего числа зарегистрированных случаев. По сравнению с первым полугодием 2018 года произошел рост доли утечек информации, которые происходили под воздействием внешних атак. Нельзя не отметить, что процентное отношение атак, произведенных извне довольно близко к количеству воздействий внутренних нарушителей в организации. Данное исследование демонстрирует значимость комплексного подхода к обеспечению защиты информации, потому что четко показывает, что важны даже такие каланы утечек информации как оптический и материальный, потому что большинство внутренних угроз происходит именно по невнимательности сотрудников.

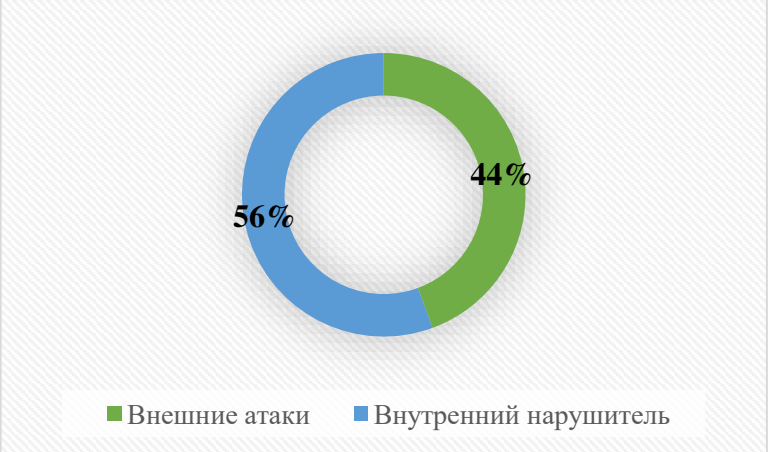

Рисунок 4 - Распределение утечек по вектору воздействия за первое полугодие 2019 года

Из всего вышеперечисленного следует вывод, что создание системы защиты от утечки информации обязательно проводить на профессиональном уровне специалистами высокого класса с применением современных технических средств.

3.1.1. Анализ рисков утечки информации по акустическим каналам

Акустическая информация наиболее не защищена от перехвата и утечки. При достижении преград, звуковая волна генерирует колебания, которые могут быть считаны специальными устройствами. Безопасность информации от утечки по акустическому каналу следует учитывать ещё на стадии планировки помещения. Для облегчения задачи обеспечения защиты помещения от утечки акустической информации используется ряд технических средств, а также звукоотражающие материалы, используемые для отделки помещения. Желательно установить генераторы шума по периметру незащищенных стен здания.

Специальные технические устройства также используются для выявления микрофонов и закладных прослушивающих устройств в контролируемом помещении. Зачастую для этого используют перехват цифрового трафика через телефонного оператора или через Интернет-провайдера. Принимаемой мерой, ориентированной на пресечение подобного рода утечек информации будет

являться создание специальных четких инструкций о границах конфиденциальной информации, которая может быть обсуждаема в помещении.

При планировке кабинета директора, необходимо учитывать такие технические каналы утечки речевой информации как:

a) закладное устройство;
b) воздухопровод и воздушная среда помещения.
c) стена в соседнее помещение или приоткрытая дверь;
d) стекло окна и модулированный лазерный луч с фотоприемником лазерной системы подслушивания;
e) случайный акустоэлектрический преобразователь в техническом средстве и побочное излучение технического средства;
f) проводные кабели, выходящие за пределы контролируемой зоны;

Для корректной оценки угроз безопасности речевой информации следует оценить уровень акустического сигнала в предполагаемых местах размещения перехватывающего акустического приемника в помещении. Также необходимо понимать, что любая речевая информация может быть считана по радиоканалу или проводам телефонной линии, а также по электропитанию закладных устройств и побочных электромагнитных излучениях как основных, так и вспомогательных технических средств, и систем, и средствами лазерного подслушивания к которым относятся даже установленные в помещении противоположного здания.

3.1.2. Анализ рисков утечки информации по электромагнитным каналам

Электромагнитные волны, распространяясь в пределах электромагнитного поля на небольшом расстоянии, могут быть перехвачены. Источником распространения могут являться:

a) аналоговые телефонные линии;
b) микрофоны телефонов и переговорных устройств;
c) волоконно-оптические каналы связи;

d) основные цепи заземления и питания;

e) другие источники.

На текущий момент, технологии могут осуществить подключение закладных устройств ПЭМИН напрямую к цепям питания или же незаметно установить в мониторе или корпусе компьютера, при этом будет происходить перехват данных через внутренние подсоединение к платам.

Способами борьбы является заземление проводов, экранирование наиболее явных источников электромагнитного излучения, использование специальных программных и аппаратных средств, позволяющих выявить закладки.

3.1.3. Анализ рисков утечки информации по визуальным каналам

Окна в кабинете или современные стеклянные перегородки офиса, через которые можно увидеть, как экран монитора, так и лежащие на столе документы являются легкодоступными путями для утечки информации. Любой световой поток, исходящий от источника информации, может быть перехвачен. В большинстве случаев, для борьбы с этим способом достаточно применять простые технические средства:

a) снижение отражательных характеристик и уменьшение освещенности объектов;
b) установка различных преград и маскировок;
c) использование светоотражающих стекол;
d) расположение объектов так, чтобы свет от них не попадал в зону возможного перехвата.

Существует риск утечки видовой информации: вынос документов из помещения для их фотографирования, иные формы копирования, скрины экранов баз данных, содержащих важные сведения, и другие способы. Основные меры борьбы с этими рисками относятся исключительно к организационной сфере.

3.1.4. Анализ рисков утечки информации по материальным каналам

Обыкновенный бумажный мусор и производственные отходы являются довольно ценным источником данных. Даже визуальный анализ отходов из офиса компании может стать источником получения конфиденциальных сведений. Для разработки системы борьбы с этим риском необходимо комплексное решение с использованием технологий переработки отходов.

3.2 Анализ существующих решений для защиты информации

Для обеспечения эффективной защиты от утечки информации, необходимо разработать комплекс системных мер безопасности, которых в дальнейшем необходимо строго придерживаться и в которую входят две основные группы действий и мероприятий:

a) организационные меры;
b) технические и программные меры.

Применяемые технические средства должны быть сертифицированы и допущены к обороту на территории РФ, недопустимо в целях защиты информации использовать или не опробованные, или запрещенные средства, относящиеся к категории «шпионских».

Система безопасности должна проектироваться оптимально, а все ее элементы должны составлять единый комплекс, контроль над работоспособностью которого должен быть возложен на компетентных сотрудников. Система мер по защите конфиденциальной информации от утечек должна являться комплексной и основываться на определенные принципах, таких как:

a) компоненты системы должны взаимодействовать между собой и управляться из единого центра;
b) наиболее серьезные меры защиты должны применяться для сведений, имеющих наивысшую ценность;
c) непрерывность работы системы в пространстве и времени, не допуская возникновения тех или иных разрывов или снижения уровня контроля;
d) ранжирование информации по степени значимости, применение разных по уровню воздействия методов защиты;

е) наиболее важные блоки и системы связи должны быть продублированы, чтобы в случае прорыва или уничтожения одного из звеньев защиты ему на смену пришел контрольный.

За соблюдение организационных мер должен нести ответственность руководитель компании, а также один из его заместителей, в чьем ведении находится служба безопасности. Все нормативно-правовые акты организации, посвященные защите информации, должны соответствовать самым строгим требованиям, необходимым для получения лицензии.

Самым уязвимым звеном в любой системе защиты информации является персонал. Необходимо составить перечень сведений, составляющих коммерческую тайну, и оформить его в качестве приложения к трудовому договору. При работе с информацией, содержащейся в базе данных, должны быть разработаны системы допуска. Необходимо ограничить все возможности копирования и доступ к внешней электронной почте. Все сотрудники должны быть ознакомлены с инструкциями о порядке работы со сведениями, содержащими коммерческую тайну, и подтвердить это росписями в журналах.

При планировании архитектуры помещения, в котором проводятся переговоры или находится защищаемая информация, должны соблюдаться все требования ГОСТа по способам защиты. Помещения переговорных должны быть способны пройти необходимую аттестацию, должны применяться все современные способы экранирования, звукопоглощающие материалы, использоваться генераторы помех.

Для защиты информации от утечки или хищения необходимо применять широкий спектр мер аппаратно-технического характера. Можно выделить четыре основные группы технических средств:

а) аппаратные (все, что позволяет выявить действующие каналы утечки информации, оценить эффективность их работы и выявить значимые характеристики);

b) инженерные (устройства, физически блокирующие возможность проникновения посторонних лиц к охраняемым объектам, системы видеонаблюдения, сигнализации и т.д.);
c) программные (специальные программы, обеспечивающие системную защиту информации, такие как DLP-системы (Data Leak Prevention, системы предотвращения утечек данных, обеспечивающие полную защиту от утраты конфиденциальной информации.) и SIEM-системы ((Security Information and Event Management) управляют информационными потоками и событиями в сети));
d) криптографические.

3.3 Анализ криптографических методов защиты информации

В современных информационных технологиях криптографические методы заняли обширную нишу, обеспечивающую защиту информации от несанкционированного доступа. Это перспективное направление разработок, помогающее повысить безопасность информации развивается и набирает обороты на современном рынке информационных услуг. На рисунке 5 приведены статистические данные от института Ponemon Institute за период с 2005 по 2013 год об использовании решений по криптозащите информации компаниями в мире. Эта статистика демонстрирует рост использования криптографических методов в мире, что только подчеркивает ее значимость для мер обеспечения защиты информации. Поэтому в вопросе применения криптографических методов для интернета вещей верным решением будет положительный ответ.

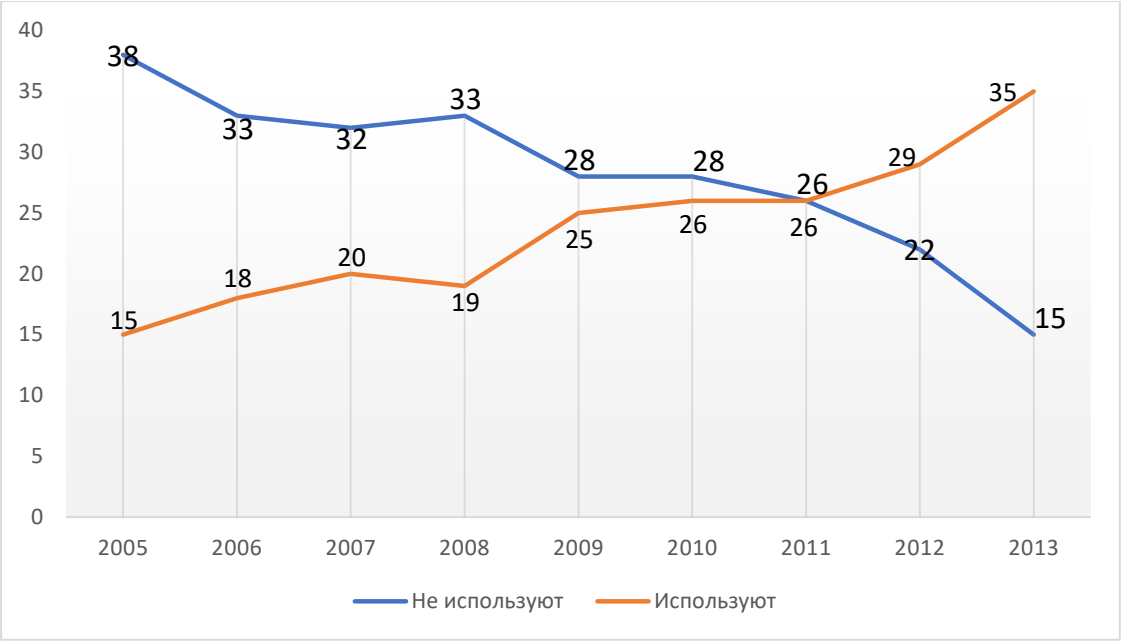

Рисунок 5 – Анализ мирового рынка криптографии

Можно выделить три основные направления развития задач в криптографии:

a) обеспечение анонимности, т.е неотслеживаемости;
b) обеспечение конфиденциальности;
c) обеспечение аутентификации информации и источника сообщения.

Задачи по обеспечению конфиденциальности относятся к защите информации от несанкционированного доступа по секретному ключу, где доступ к информации имеют только обладатели ключа. Задачи по обеспечению анонимности и аутентификации применяются для электронных способов обработки и передачи информации такие как банковская сфера и электронная коммерция.

Криптографическое преобразование состоит из двух этапов: прямого и обратного, т.е шифрования (или зашифрования) и дешифрования (или расшифрования). Исходное сообщение называется открытым текстом M. Зашифрованное сообщение называется шифртекстом или шифрограммой C. После обратного преобразования получаем исходный текст M’. Таким образом, в канал передается шифртекст C. Если пользоваться символьными

обозначениями, то Xk – данные до прямого преобразования, Xn – данные после прямого преобразования, т. е. положить Xk = M и Xn = C, то сравнительной характеристикой будет равенство k = n. Это означает, что длина открытого и зашифрованного сообщений не меняется.

Функция зашифрования E в математическом виде представляется следующим образом:

$$E(M) = C. \quad (1)$$

В обратном процессе функция расшифрования D восстанавливает M:

$$D(C) = M. \quad (2)$$

Поскольку смысл зашифрования и последующего расшифрования сообщения заключается в восстановлении исходного открытого текста, справедливо следующее равенство:

$$D(E(M)) = M. \quad (3)$$

В анализе процессов преобразования шифр отождествляется с криптографическим алгоритмом, который в тоже время является математическим алгоритмом и используется для шифрования и дешифрования информации.

Атака на основе шифртекста предполагает расположение шифртекстами нескольких сообщений, которые непосредственно зашифрованы единым алгоритмом. Задача криптоаналитика стоит в расшифровании сообщений или в определении ключа. При атаках на основе открытого текста криптоаналитик располагает шифртекстами нескольких сообщений и открытыми текстами этих же сообщений. Основной задачей является определение ключа. В случае атаки на основе подобранного ключа криптоаналитик должен обладать информацией о связях между ключами. Для определения сложности атак, нужно использовать следующие параметры:

a) сложность данных – оценивается объем данных, необходимых для реализации атаки;
b) сложность обработки – оценивается время, необходимое на реализацию атаки;

c) требования к памяти компьютера – оценивается минимально необходимый объем памяти компьютера для выполнения всех расчетно-аналитических операций.

Для того, чтобы криптографический алгоритм можно было считать стойким, что означает невозможность восстановления открытого текста при любом объеме шифтекста. Все остальные криптосистемы можно вскрыть с использованием только шифртекста простым перебором возможных ключей и проверкой осмысленности полученного открытого текста.

Выделяется несколько криптографических методов защиты информации:

a) аппаратные, реализующие криптоалгоритмы или их отдельные участки в микросхемах, процессорах и специализированных блоках, и аппаратных модулях, совмещенные со средствами вычислительной техники или встраиваемые в автоматизированные системы;
b) программные, представляющие собой реализацию одного или нескольких криптоалгоритмов на языке программирования высокого или низкого уровня;
c) программно-аппаратные, представляющие собой комплексы, состоящие из взаимосвязанных программной и аппаратной части с функциями криптографической защиты.

При организации защищенных информационных систем необходимо учитывать некоторые особенности размещения средств криптографической защиты информации. Следует отметить, что нет принципиальных различий между программными, программно-аппаратными и аппаратными средствами.

4 РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

4.1 Стадии цикла разработки

Жизненный цикл разработки ПО начинается со стадии анализа, во время которого происходит обсуждение требований, предъявляемых к конечному продукту между участниками процесса. Цель этой стадии является выявление детальных требований к системе. Способы определения переходов между стадиями отличаются в зависимости от выбранной модели разработки. От сюда следует, что этот этап предполагает, в основном, сбор различного рода требований к разрабатываемому программному обеспечению.

На следующей стадии на этапе проектирования разработчики руководствуясь сформулированными требованиями, создают высокоуровневый дизайн системы. На этом этапе определяются используемые в проекте технологии, а также ограничения, временные рамки и бюджет. Таким образом, в соответствии с уточненными требованиями выбираются наиболее подходящие проектные решения. Принятый в разработку дизайн системы определяет перечень необходимых к разработке программных компонентов, а также функциональные характеристики программы и методы использования базы данных. Как правило, на данном этапе для упрощения визуализации процесса проектирования используются так называемые нотации**,** т.е. схематическое выражение характеристик проектируемой системы. К основным используемым нотациям относятся:

a) Блок-схемы;
b) ER-диаграммы;
c) UML-диаграммы;
d) Макеты.

После того как все описанные требования утверждены, осуществляется переход к следующей стадии жизненного цикла – разработке, на котором начинается написание программистами кода программы, который соответствует ранее сформулированным требованиям. На этом этапе происходит

настройка программного окружения, разработка пользовательского интерфейса, а также логику взаимодействия программы с сервером. Все стадии цикла повторяется до тех пор, по не будут реализованы все поставленные ранее требования к продукту.

Программирование, как правило, состоит из четырех основных стадий:

a) Разработка алгоритмов, т.е фактически, создание логики работы программы;
b) Написание исходного кода;
c) Компиляция – преобразование в машинный код;
d) Тестирование и отладка.

Документацию как этап выделяют достаточно условно, поскольку различные документы создаются на всех стадиях жизненного цикла программы. Тем не менее, кроме проектной документации и различных сопровождающих разработку записей, существуют также и другая документация, которая может описывать, к примеру, функции программы или способы ее использования.

На следующем этапе тестирования происходит поиск дефектов и ошибок в программном обеспечении и сравнивание представленным в требованиях поведением системы с реальным. При обнаружении дефекта, тестировщик должен составить отчет об ошибке, который будет передан разработчикам, которые его исправляют. Этот цикл будет повторяться до тех пор, пока не будут откорректированы все возникающие ошибки и исключения, и не будет выявлено новых и пока не будут достигнуты критерии окончания тестирования. После успешного тестирования разработанной программы, наступает время релиза и передачи ее конечным пользователям. На этой стадии возможно обучение персонала работе с приложением. Также в работу включается отдел технической поддержки, сотрудники которого будут обеспечивать обратную связь с пользователями, а также осуществлять их консультирование и поддержку.

В случае обнаружения пользователями тех или иных пост-релизных ошибок, информация о них передается в виде отчетов об ошибках команде разработки. Разработчики в свою очередь оценивают сложность и серьезность проблемы и принимают решение либо немедленно выпустить исправление, либо отложить его до выпуска следующей версии программы.

4.2 Требования к разрабатываемому приложению

Приложение должно быть простым в использовании и содержать понятный интерфейс для пользователя. Также приложение должно осуществлять поддержку платформы Windows и иметь небольшой объём. Отображать схему помещения для переговоров, которое находится в приемной у президента организации.

4.2.1 Общие требования

Данный программный продукт может подвергаться модифицированию и улучшению на основе потребностей заинтересованных лиц, имеющих официальное разрешение. Пользователями системы могут быть разные люди, в том числе не имеющие особых профессиональных навыков в области защиты и безопасности

Требования к надежности оборудования и ПО:

a) проведение комплекса мероприятий отладки, поиска и исключения ошибок;
b) использование сертифицированных средств вычислительной техники, их комплектующих и средств передачи данных;
c) необходимо использование программ защиты от компьютерных вирусов;
d) обеспечение защиты от перехвата информации по техническому каналу;
e) с целью повышения отказоустойчивости системы в целом необходима обязательная комплектация серверов источником бесперебойного питания с возможностью автономной работы системы не менее 20 минут.

Требования к интерфейсу:

a) интерфейс должен быть простым и понятным, чтобы пользователю не требовалось объяснять, как им пользоваться;
b) удобство интерфейса и его элементов обеспечивает высокую скорость работы пользователя;
c) обеспечение защиты от человеческих ошибок;
d) быстрое обучение пользователя за счет эргономичности интерфейса;
e) цветовая гамма интерфейса должна быть приятной глазу и настраивать на рабочий лад;
f) возможность ввода данных с помощью клавиатуры и использование компьютерной мыши.

4.2.2 Требования к лингвистическому обеспечению

Программа должна быть полностью на русском языке. Ввод данных производится только арабскими цифрами и буквами русского алфавита. Для разработки программы выбран объектно-ориентированный язык программирования- C#.

4.2.3 Требования к информационному обеспечению

Программный продукт не нуждается в хранении большого объема данных, поэтому создание отдельной базы данных не требуется. В данном случае ресурсов компьютера будет достаточно.

4.2.4 Требования к математическому обеспечению

Разрабатываемая программа не требует специальное математическое обеспечение.

4.2.5 Требования к программному обеспечению

Основой разрабатываемой программы является операционная система. Выбор ОС, на которых работает эта система, разнообразен, но лучше всего использовать ОС Windows 7 компании Microsoft, поскольку она имеет следующие достоинства:

a) стабильная работа системы;
b) большая производительность;

c) многозадачность;
d) эргономичность интерфейса.

4.2.6 Требования к техническому обеспечению

Разрабатываемая программа не требует много места на компьютере и сильной загрузки процессора, ограничиваясь самыми минимальными требованиями, поэтому она более доступна для любого пользователя. Таким образом, минимальными требованиями к ПЭВМ пользователей будут следующими: – процессор – Intel Pentium 1.5 ГГц; – объем оперативной памяти – 256 Мб; – дисковая подсистема – 24 Гб; – устройство для работы с USB Flash носителями; – сетевой адаптер – 100 Мбит; – устройство чтения и записи компакт-дисков.

4.3 Обоснование выбора языка программирования, среды разработки и алгоритмов

Существующая свобода выбора платформы разработки предоставляет возможность рассматривать удобные разработчику варианты проектирования. Требования к программному интерфейсу позволяют выбрать в качестве платформы реализации Microsoft Visual Studio 2019. Благодаря ряду достоинств, использовать данную среду разработки представляется очень удобно и выгодно:

a) Понятный графический интерфейс, который позволяет как создать собственную базу данных, так и разрабатывать приложения на различных языках программирования;
b) Достаточная частота выхода обновлений программы, поддержка множества языков и алгоритмов, а также высокая производительность;
c) Абсолютная совместимость с операционной системой Windows;
d) Наличие развитых встроенных средств разработки приложений;
e) Автоматическое создание скриптов и возможность просматривать данные и изменять их без написания нового скрипта;

f) Возможность разработки как консольных приложений, так и приложений с графическим интерфейсом, в том числе с поддержкой технологии Windows Forms.

Visual Studio включает в себя редактор исходного кода и возможностью простейшего рефакторинга кода. Остальные встраиваемые инструменты включают в себя редактор форм для упрощения создания графического интерфейса приложения, веб-редактор, дизайнер классов и дизайнер схемы базы данных.

Языком разработки был выбран язык объектно-ориентированного программирования C#. Это обусловлено тем, что это языком программирования нового поколения, который включил в себя массу достоинств. Язык основан на строгой компонентной архитектуре и реализует передовые механизмы обеспечения безопасности кода.

C# - это полнофункциональный объектно-ориентированный язык программирования высого уровня, с поддержкой всех трех прицнипов объектно-ориентированного программирования: инкапсуляцию, наследование и полиморфизм.

4.4 Разработка ПО

Программа разработана в среде Microsoft Visual Studio C# 2019 Community. Все иллюстрации отрисованы в программе Adobe Illustrator 2019.

Функциональное назначение: программа представляет собой приложение «Iot-security» разработанное с целью обеспечения и поддержания информационной безопасности помещения и информации, циркулирующей в нем. Предусмотрена возможность шифрования и дешифровки текстовых символов для дальнейшего использования. Проверка изменений журнала событий Windows с краткой информацией о каждой ошибке и отражение погодных значений, а также значений системы, на которой запускается приложение. Все эти функции позволят своевременно реагировать на изменения данных экосистемы интернета вещей.

На контекстной диаграмме, представленной на рисунке 4,

отображаются объекты и информационные потоки, определяющие функциональную модель разработанного приложения.

Основными входящими потоками являются:

a) Входная информация

К основным выходящим потокам относятся:

a) криптографически зашифрованная информация;
b) данные о состоянии системы;
c) данные с сайта о погоде;
d) Учет подключенных устройств;
e) Журнал событий Windows.

На контекстной диаграмме также отражены управления и механизмы. В роли управления выступают стандарты сети Интернет и ОС Window, а также криптографические стандарты. В роли механизмов выступают пользователь, аппаратное и программное обеспечение.

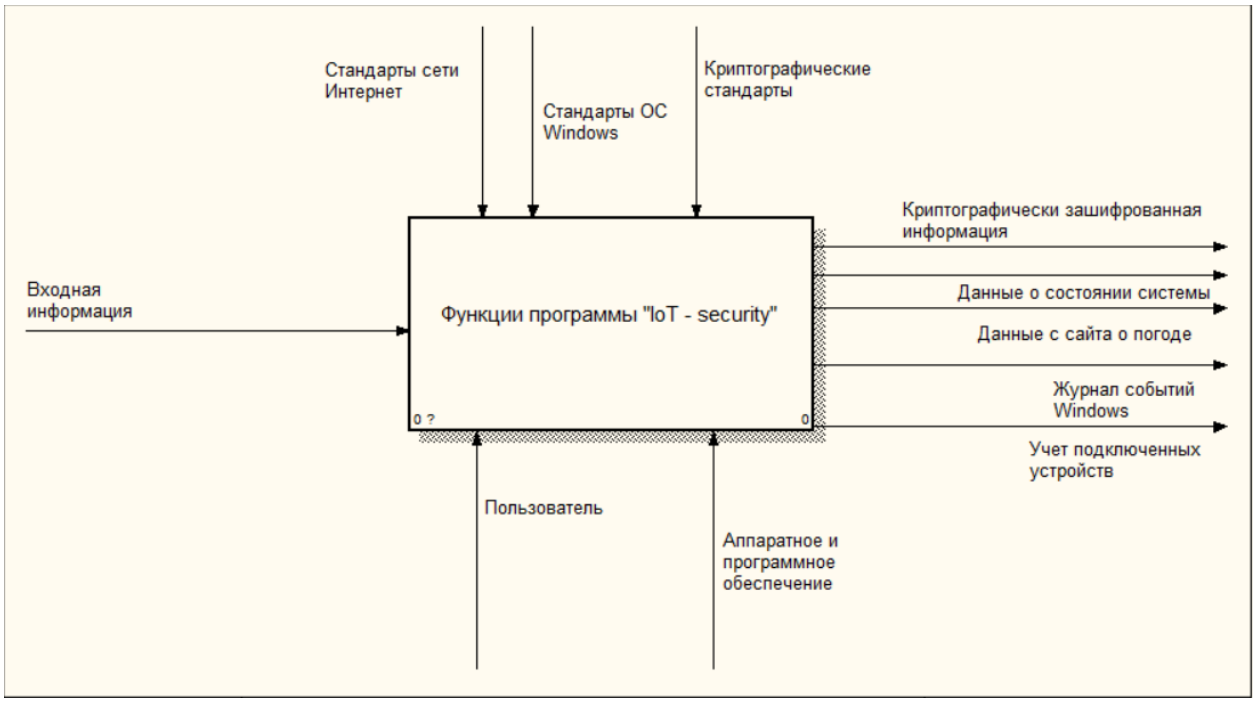

Рисунок 4 – Контекстная диаграмма функций приложения

Для более детального функционального анализа приложения следует декомпозировать контекстную диаграмму. Декомпозиция основного блока представлена на рисунке 5.

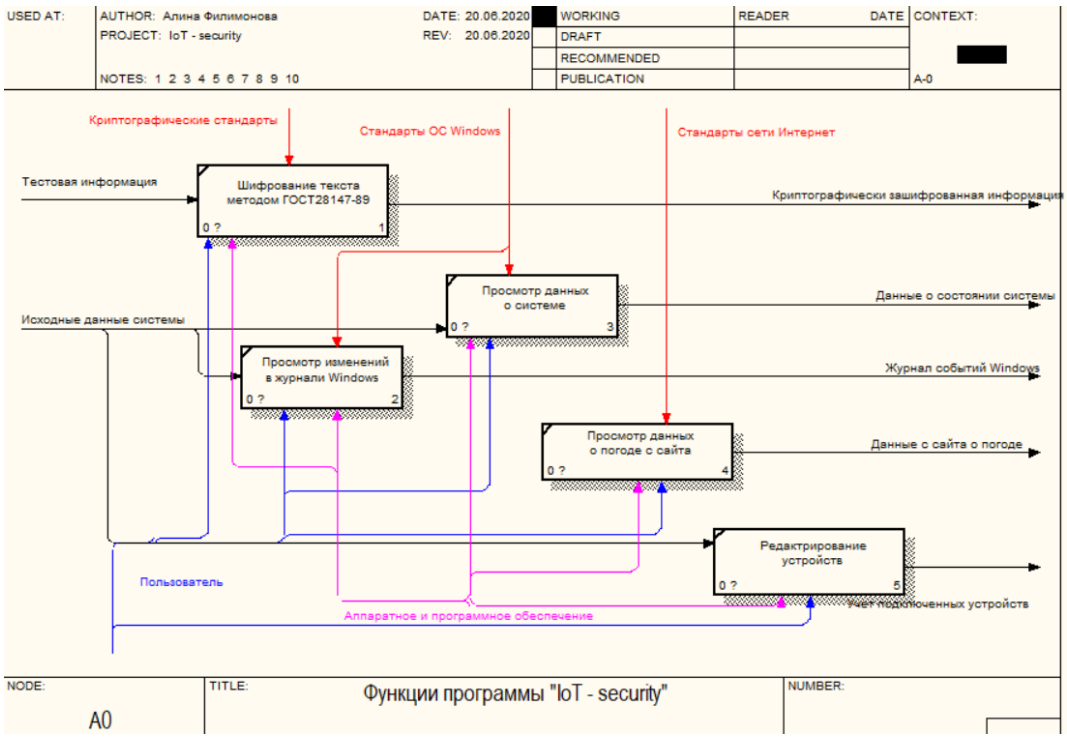

Рисунок 5 – Декомпозиция контекстной диаграммы приложения

Первым окном приложения является форма авторизации, представленная на рисунке 6. Пользователю необходимо ввести свои данные подразумевающие логин и пароль. В случае ошибки появляется окно, сообщающее о неправильности вводимых данных. В контекстном меню в левом верхнем углу есть вкладки «Справка» и «О разработчике», пример приведен на рисунках 7 и 8.

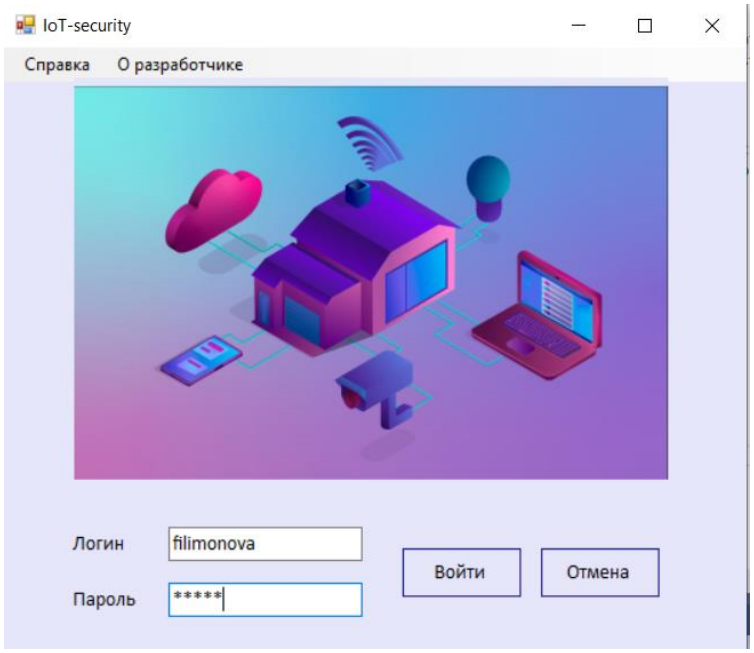

Рисунок 6 — Окно авторизации

Во вкладке «Справка» находится подсказка по заполнению формы авторизации. Во вкладке «О разработчике» информация о разработчике приложения.

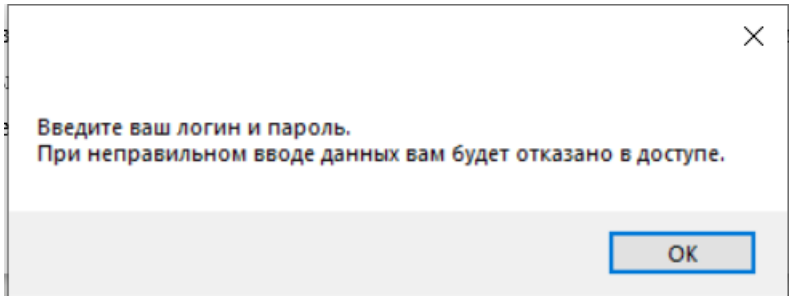

Рисунок 7 — Информационное сообщения из меню «Справка»

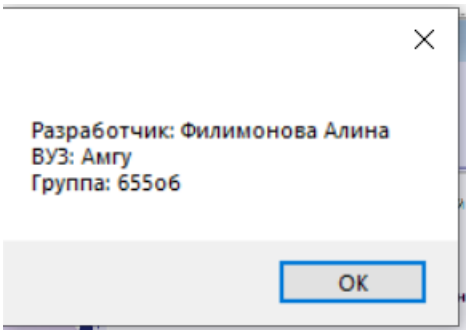

Рисунок 8— Информационное сообщения из меню «О разработчике»

После успешной авторизации, пользователю открывается главное меню с возможностью выбора необходимых действий, представленное на рисунке 9. В окне textBox отображаются показания температуры с сайта http://www.meteoservice.ru/weather/now/moskva.html.

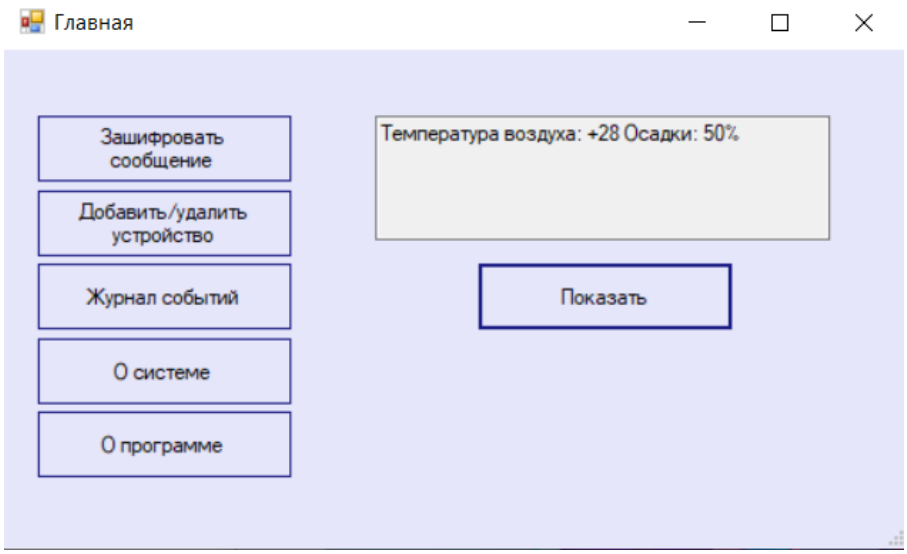

Рисунок 9 — Главное окно

При нажатии на кнопку «Зашифровать сообщение» открывается окно формы использования метода криптографического шифрования ГОСТ 28147-89. Окно формы показано на рисунке 10.

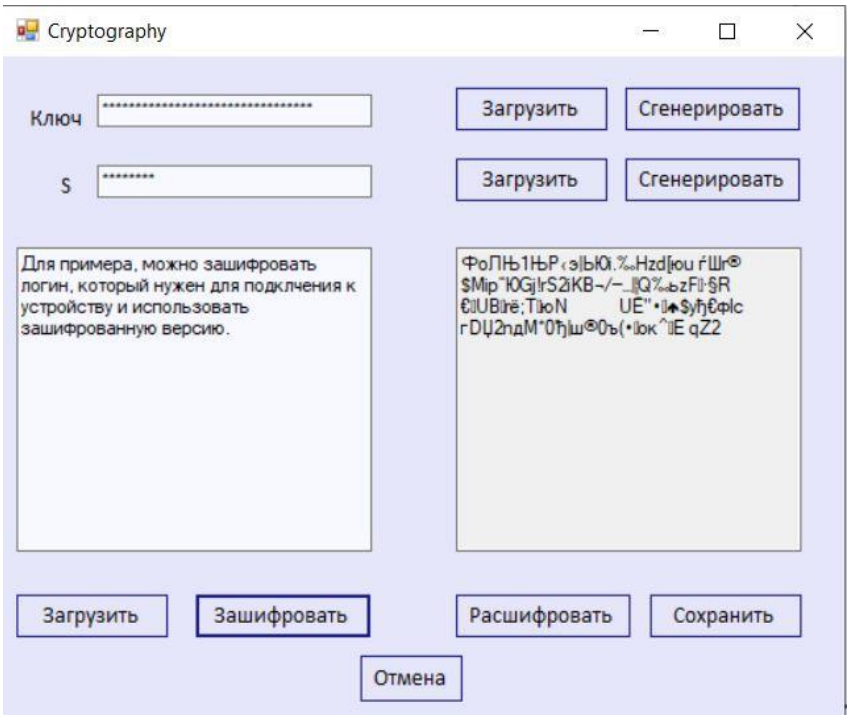

Рисунок 10 — Окно с криптографическим шифрованием

Также в приложении предусмотрена возможность ведения списка работающих устройств в помещении отображенное на рисунке 11.

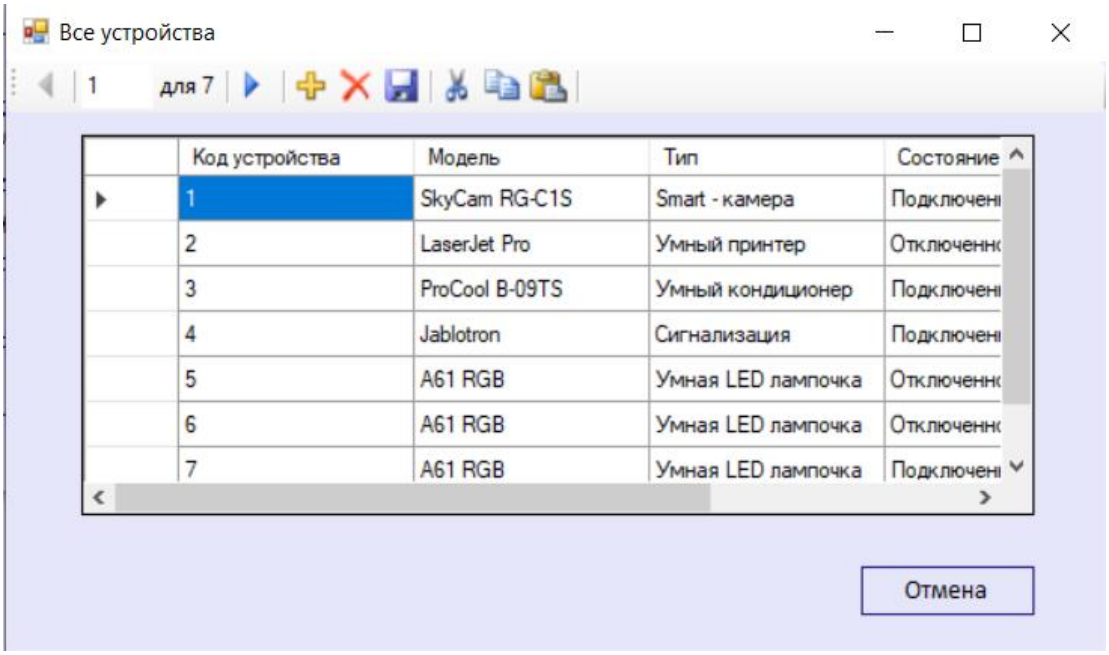

Рисунок 11 — Окно формы редактирования устройств

При нажатии на кнопку «О системе» на экране появляется окно с информацией о системе, на которой запускается приложение. Пример работы формы показано на рисунке 12.

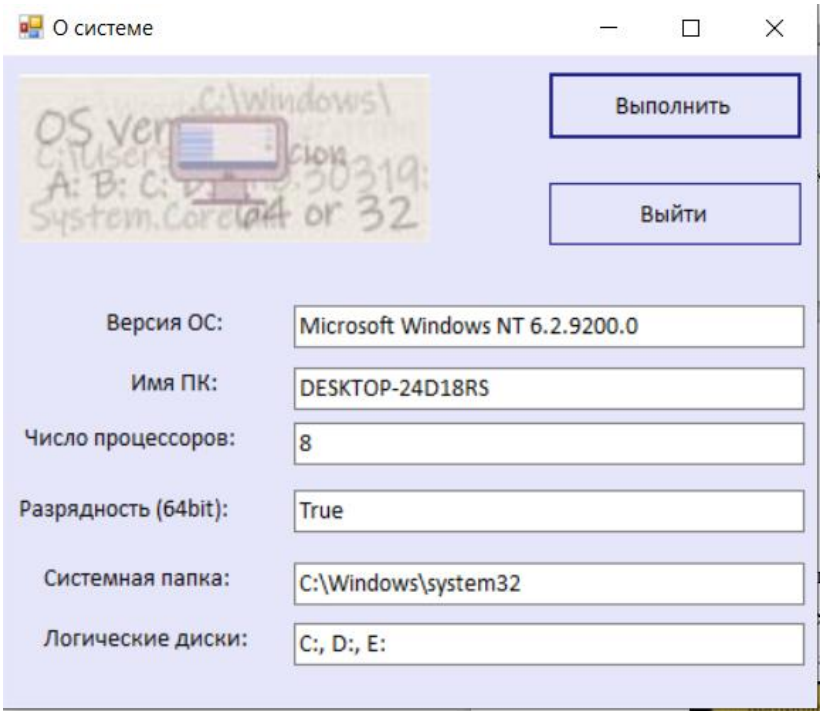

Рисунок 12 — Окно формы получения данных о системе

Также в приложении используется класс EventLog используемый для протоколирования событий журнала Windows. Использование приложения начинается с окна разрешения действий от имени администратора показанное на рисунке 13.

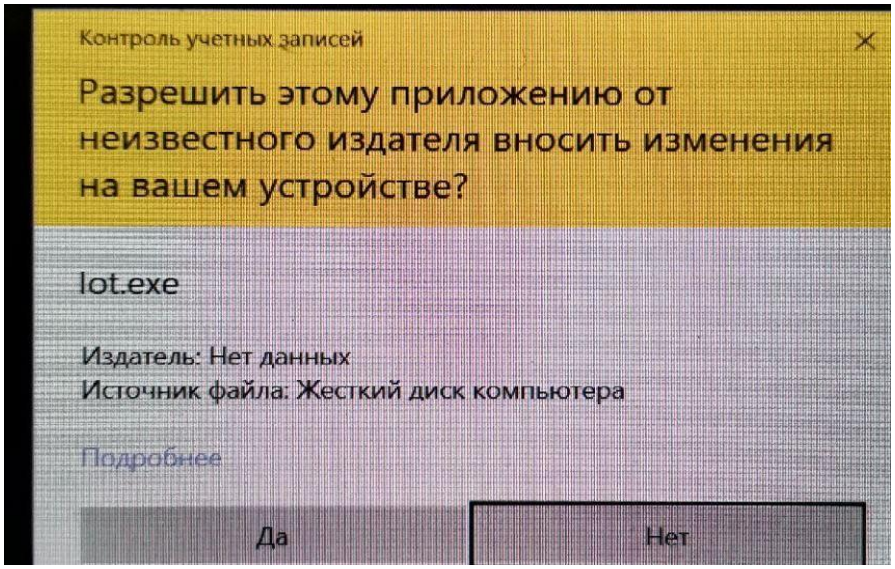

Рисунок 13 — Окно контроля учетных записей

При выборе кнопки «О программе» происходит вызов формы AboutBox с краткими сведениями о разработанном приложении. Форма представлена на рисунке 14.

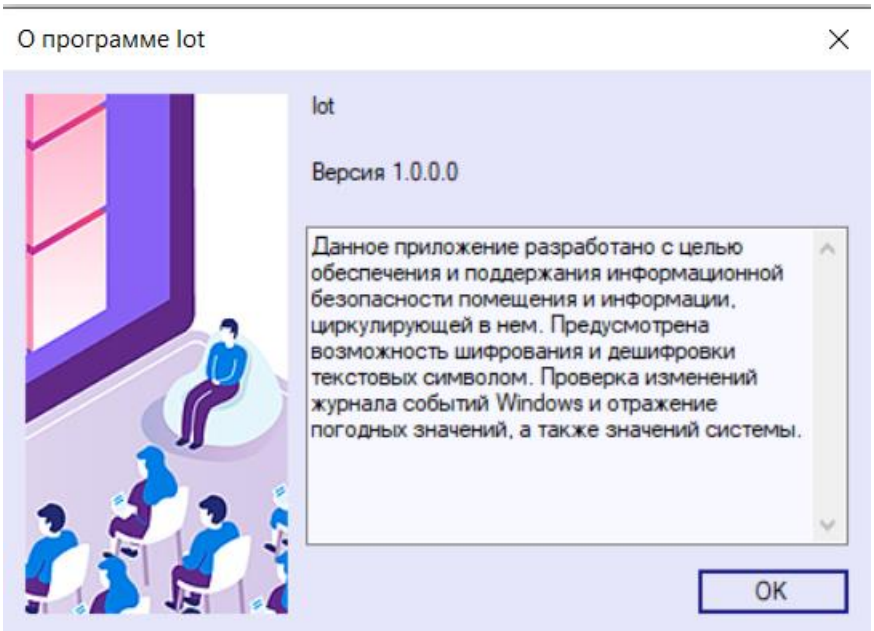

Рисунок 14 — Окно «О программе»

5. БЕЗОПАСНОСТЬ И ЭКОЛОГИЧНОСТЬ

В современном мире происходит повсеместное внедрение компьютерной техники во всех сферах жизни человека. В офисе цифрового интернет-провайдера изобилует различная техника, в том числе мощные ЭВМ. Среднестатистический работник при работе за компьютером сталкивается с такими проблемами, как

a) повышенное умственное напряжение
b) заболевания, связанные с мышцами и суставами
c) воздействие пыли и грызи
d) нервно-эмоциональная нагрузка
e) зрительное утомление и т.д.

Из всего выше перечисленного можно сделать вывод, что поддержание безопасности рабочего места человека очень важно.

5.1 Безопасность

Для того, чтобы производить корректное соблюдение правил к поддержанию рабочего места, необходимо выяснить, что и как влияет на организм человека и какие существуют методы защиты.

5.1.1 Электромагнитное излучение

Электромагнитное излучение концентрируется вокруг рабочего места компьютера в виде электромагнитного поля, которое невозможно ощутить органами чувств человека, но оно присутствует повсюду. Опасное влияние электромагнитного излучения остаётся спорным в научной среде. Это связанно с тем, что на данный момент, нет точных доказательств о его неоспоримом вреде или безопасности. Исходя из этого, нельзя давать гарантии того, что данное излучение никак не проявит себя на организм и здоровье человека, поэтому самым оптимальным вариантом является применение мер по защите от потенциальной угрозы. К ним относят:

a) использование жидкокристаллических мониторов вместо мониторов с электроннолучевой трубкой, поскольку их излучение значительно меньше
b) желательная установка компьютера в углу комнаты, чтобы излучение поглощалось стенами
c) выключать компьютер, если он больше не будет использоваться в ближайшее время
d) по возможности сокращение время работы за компьютером и каждый час делать 5-10 минутные перерывы
e) заземление компьютера.

5.1.2 Зрение

Одним из самых серьезных влияний компьютера на здоровье человека является воздействие на зрение. При работе за экраном монитора, глаза раскрываются шире, а моргание, в тоже время, происходит в три раза реже, чем при чтении текста с листа бумаги, приводящее к быстрому испарению защитной слезной пленки глаза, что способствует получению роговицей недостаточного количества влаги. Это является причиной возникновения таких симптомов, как снижение остроты зрения, появление тумана, двоение предметов, боли при движении глаз, боли в области глазниц и лба; сухость, жжение в глазах, светобоязнь, даже развитие ложной близорукости. Это и есть признаки компьютерного зрительного синдрома. При работе с компьютером человек полностью зависит от положения дисплея.

Требования к монитору: чем выше его разрешающая способность, тем точнее и четче изображение на экране, и тем оно меньше утомляет глаза; монитор должен находиться на расстоянии не менее 45 см от глаз (расстояние вытянутой руки);

Освещение рабочего места не должно вызывать блики на экране монитора, в то же время оно должно быть достаточным для того, чтобы хорошо видеть остальные предметы, с которыми вы работаете;

Регулярно проводите гимнастику для глаз. Вот несколько простых упражнений: зажмурьте глаза на 10 с., быстро моргайте в течение 10 с., сделайте несколько круговых движений глазами, несколько раз поменяйте фокус - переведите взгляд с близлежащего предмета вдаль;

Как можно чаще прерывайте работу и давайте глазам отдохнуть, желательно каждый час делать 10-15 минутный перерыв.

При разработке следует уделить внимание интерфейсу программы. Он должен быть эргономичным, т.е. удобный и понятный для пользователя, а также соответствовать критериям эргономичности, а именно:

a) интуитивность (естественность) – свойство приложения адаптироваться под требования пользователя;
b) непротиворечивость (последовательность;
c) визуализация;
d) система навигации;
e) гибкость;
f) поддержка пользователя.

Формы – основной элемент интерфейса, который проектируется для более удобного, более понятного и скорейшего достижения решения поставленной задачи. Размещение информационных единиц на пространстве формы должно соответствовать логике ее будущего использования: это зависит от необходимой последовательности доступа к информационным единицам, частотой их использования, а также от относительной важности элементов. Также важно использовать незаполненное пространство, чтобы создать равновесие и симметрию среди информационных элементов формы, для фиксации внимания пользователя в нужном направлении. Пример интерфейса программы приведен на рисунках 15 и 16.

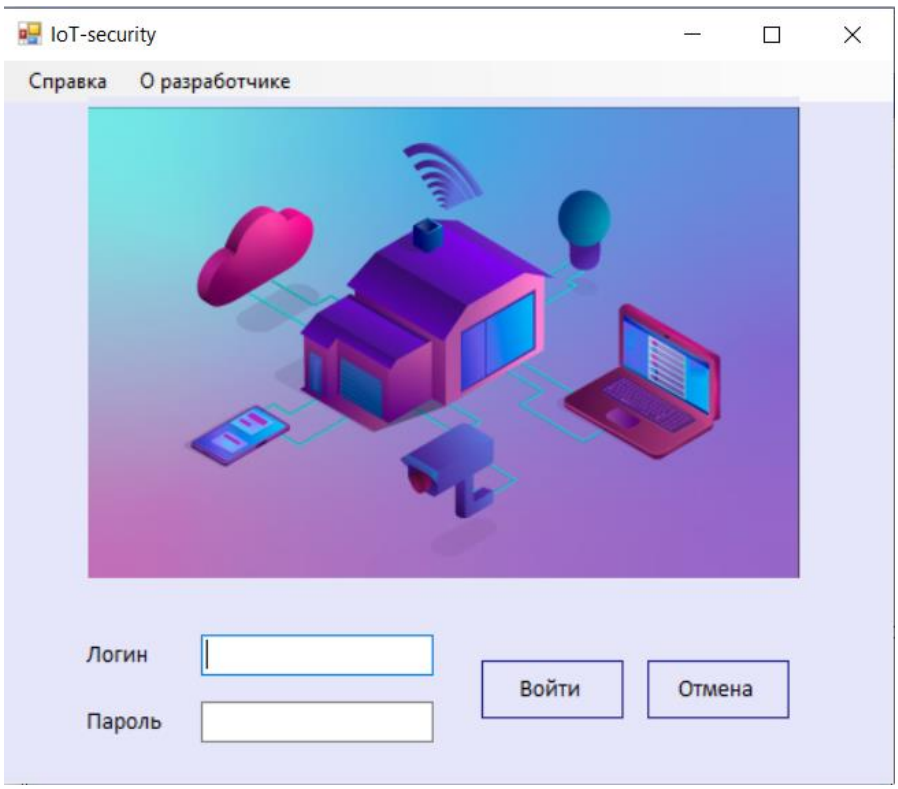

Рисунок 15 – Интерфейс программы (окно авторизации)

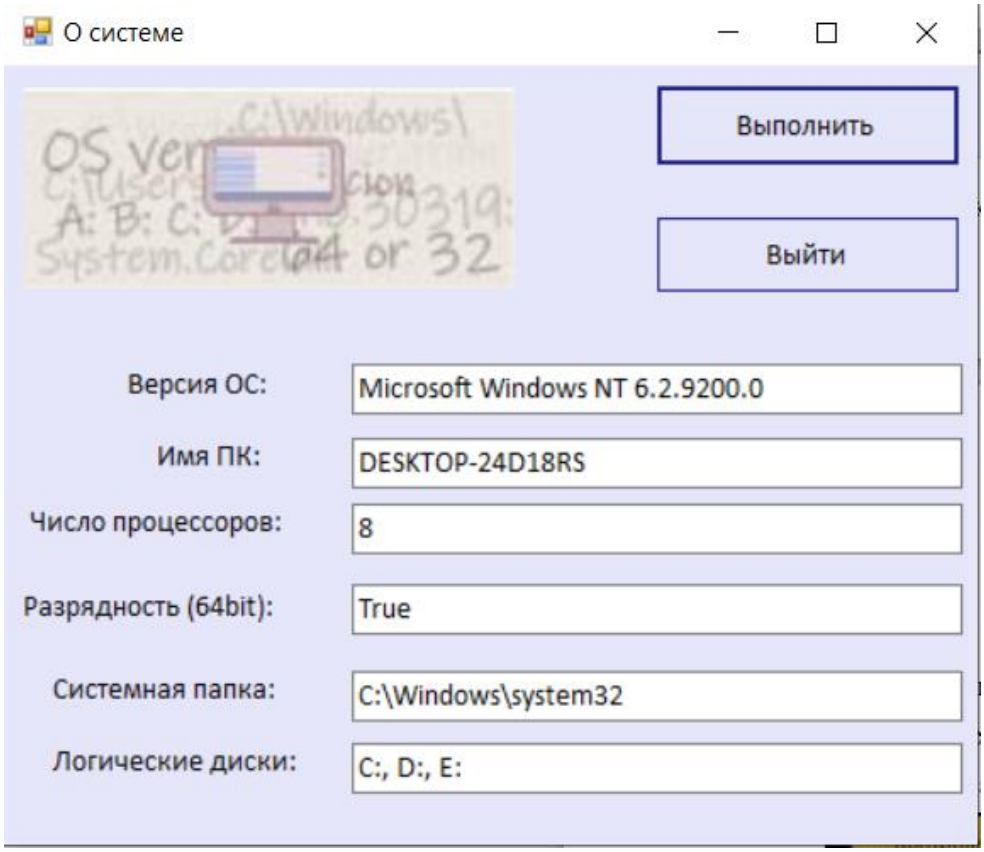

Рисунок 16 - Интерфейс программы (пример выполнения задания)

5.1.3 Заболевания, связанные с мышцами и суставами

У людей, зарабатывающих на жизнь работой на компьютерах, наибольшее число жалоб на здоровье связано с заболеваниями мышц и суставов. Чаще всего это просто онемение шеи, боль в плечах и пояснице или покалывание в ногах. Но бывают, однако, и более серьезные заболевания. Боль в руках, особенно в кисти правой руки, вызванная долгой работой за компьютером приобрела название туннельного синдрома или синдрома запястного канала. Причиной возникновения боли является защемление нерва в запястном канале, вызванное постоянной статической нагрузкой на одни и те же мышцы, которая может быть вызвана большим количеством однообразных движений или неудобным положением рук, во время работы с клавиатурой. Основными заболеваниями позвоночника, развивающимися вследствие долгого нахождения за компьютером, являются: остеохондроз и искривления позвоночника.

5.1.4 Стресс, бессонница, нервные расстройства.

Длительная работа за компьютером связанна с постоянным раздражением, источником которого могут быть разные ситуации. Наверное, нет такого человека, у которого никогда не зависал компьютер, с потерей, не сохраненной информации, не было проблем с какими-либо программами и т.д. Еще один важный фактор - нервно-эмоциональное напряжение у детей. Не секрет, что общение с компьютером, особенно с игровыми программами, сопровождается сильным нервным напряжением, поскольку требует быстрой ответной реакции.

5.1.5 Воздействие пыли и грязи.

Ученые утверждают, что клавиатура содержит большое количество микробов, что может вызвать так называемую "болезнь грязных рук". Следует вовремя убирать пыль в системном блоке, которая может привести к различным аллергическим реакциям.

5.1.6 Эргономичность рабочего места

В СанПиН 2.2.2/2.4.1340-03 «Гигиенические требования к ПЭВМ и организации работы» представлены ряд правил и норм для рабочих мест с ПЭВМ.

Общие требования к организации рабочих мест пользователей ПЭВМ:

a) при размещении рабочих мест с ПЭВМ расстояние между рабочими столами с видеомониторами (в направлении тыла поверхности одного видеомонитора и экрана другого видеомонитора), должно быть не менее 2,0 м, а расстояние между боковыми поверхностями видеомониторов - не менее 1,2 м;
b) рабочие места с ПЭВМ при выполнении творческой работы, требующей значительного умственного напряжения или высокой концентрации внимания, рекомендуется изолировать друг от друга перегородками высотой 1,5-2,0 м;
c) экран видеомонитора должен находиться от глаз пользователя на расстоянии 600-700 мм, но не ближе 500 мм с учетом размеров алфавитно-цифровых знаков и символов;
d) конструкция рабочего стула (кресла) должна обеспечивать поддержание рациональной рабочей позы при работе на ПЭВМ, позволять изменять позу с целью снижения статического напряжения мышц шейно-плечевой области и спины для предупреждения развития утомления. Тип рабочего стула (кресла) следует выбирать с учетом роста пользователя, характера и продолжительности работы с ПЭВМ. Рабочий стул (кресло) должен быть подъемно-поворотным, регулируемым по высоте и углам наклона сиденья и спинки, а также расстоянию спинки от переднего края сиденья, при этом регулировка каждого параметра должна быть независимой, легко осуществляемой и иметь надежную фиксацию;
e) модульными размерами рабочей поверхности стола для ПЭВМ, на основании которых должны рассчитываться конструктивные размеры,

следует считать: ширину 800, 1000, 1200 и 1400 мм, глубину 800 и 1000 мм при нерегулируемой его высоте, равной 725 мм.

5.1.7 Требования электробезопасности

Неукоснительное соблюдение правил электробезопасности закладывается ещё на стадии подключения ЭВМ к питающей сети. Существуют определенные правила подключения с точки зрения безопасности человека и безвредности для ЭВМ. Для исключения опасности поражения электрическим током электроустановки должны быть заземлены (занулены). При занулении необходимо быть уверенным в том, что «нуль» не станет фазой.

Основные требования к электробезопасности при работе с ЭВМ можно сформулировать следующими правилами:

a) Необходимо постоянно отслеживать и контролировать исправное состояние электропроводки, выключателей, розеток, проводов и заземления. При обнаружении неисправности немедленно обесточить электрооборудование, оповестить администрацию и прекратить работу.
b) Во избежание повреждения изоляции проводов и возникновения коротких замыканий не разрешается:
    1) вешать что-либо на провода;
    2) закрашивать и белить шнуры и провода;
    3) закладывать провода и шнуры за газовые и водопроводные трубы, за батареи отопительной системы;
    4) выдергивать штепсельную вилку из розетки за шнур, усилие должно быть приложено к корпусу вилки.
c) Для исключения поражения электрическим током запрещается:
    1) прикасаться к экрану и к тыльной стороне блоков компьютера;
    2) работать на ЭВМ мокрыми руками;
    3) работать на ЭВМ, имеющих нарушения целостности корпуса, нарушения изоляции проводов, неисправную индикацию включения питания, с признаками электрического напряжения на корпусе;

4) касаться одновременно каких-либо трубопроводов, батарей отопления, металлических конструкций, соединенных с землей.

d) Запрещается под напряжением очищать от пыли и загрязнения электрооборудование, а также проводить ремонт средств вычислительной техники и периферийного оборудования.

e) Ремонт электроаппаратуры производится только специалистами-техниками с соблюдением необходимых технических требований.

f) Во время ремонта вычислительной техники запрещается:

1) применять для соединения блоков и приборов провода с поврежденной изоляцией;

2) производить пайку и установку деталей в оборудовании, находящемся под напряжением;

3) измерять напряжение и ток переносными приборами с неизолированными проводами и щупами;

4) подключать блоки и приборы к оборудованию, находящемуся под напряжением;

5) заменять предохранители при включенном оборудовании;

6) работать на высоковольтных установках без защитных средств.

g) Спасение пострадавшего при поражении электрическим током главным образом зависит от быстроты освобождения его от действия током.

Соблюдение правил и требований электробезопасности позволит обеспечить качественную и полную защиту пользователя от поражения электрическим током. Необходимо помнить, что если произошел несчастный случай, в первую очередь необходимо любым способом немедленно прекратить действие тока. Например, выключить рубильник, отбросить электропровод от пострадавшего сухой палкой или чем-то подобным и обязательно вызвать врача. Если пострадавший в сознании и чувствует некоторое недомогание, до прихода врача следует обеспечить ему покой, свежий воздух, тепло. При тяжелом состоянии пострадавшего, то есть проявлении потери сознания, отсутствия пульса и прерывистого дыхания,

необходимо срочно начать искусственное дыхание по способу "изо рта в рот" с частотой 12-15 вдуваний в минуту и непрямой массаж сердца с частотой одно надавливание в секунду и продолжать эти действия до улучшения состояния больного. Следует продолжать оказывать помощь пострадавшему после его прихода в сознание еще 5-10 минут, затем уложить его в тепле и давать обильное питье в виде теплого чая.

5.2 Экологичность

Основополагающим документом, отвечающим за экологичность на предприятии, является Федеральный закон №89 «Об отходах производства и потребления» от 24.06.1998 (ред. От 28.12.2016). Согласно закону, отходы производства и потребления (далее - отходы) — это вещества или предметы, которые образованы в процессе производства, выполнения работ, оказания услуг или в процессе потребления, которые удаляются, предназначены для удаления или подлежат удалению в соответствии с Федеральным законом.

Отходы в зависимости от степени негативного воздействия на окружающую среду подразделяются в соответствии с критериями, установленными федеральным органом исполнительной власти, осуществляющим государственное регулирование в области охраны окружающей среды, на пять классов опасности:

a) I класс - чрезвычайно опасные отходы (полоний, бензапирен, фтороводород, соли свинца, таллий, диэтилртуть, плутоний, теллур, озон, циановодород и другие вещества)
b) II класс - высокоопасные отходы (литий, фенол, хлороформ, серную кислоту, селен, сероводород, барий, формальдегид, сурьму, стирол, все нитриты, мышьяк, молибден и другие вещества)
c) III класс - умеренно опасные отходы (соединения марганца, серебра, никеля, меди, бензосодержащие отходы, соляную кислоту, трихлорэтилен, фосфаты, этиловый спирт и другие вещества)
d) IV класс - малоопасные отходы (сульфаты, хлориды, алюминий, метан, аммиак, этанол и другие вещества)

e) V класс - практически неопасные отходы (Это неопасные вещества, которые в большинстве случаем можно утилизировать на свалках)

При производстве компьютеров и прочей офисной техники используются различные драгоценные металлы. Как правило, в одном компьютере, включающем системный блок, мышь, монитор и клавиатуру, содержится почти 0,1г золота и 1г серебра. В том числе, компьютер состоит из: свинца, ртути, кадмия, мышьяка, никеля и цинкома. Из этого следует, что компьютер, благодаря своим компонентам, относится к опасным отходам.

В связи с этими факторами, предприятие обязано пользоваться услугами организации, которая специализируется на уничтожении отходов. Предприятие не может выкинуть оборудование, содержащее даже сотую долю драгоценных металлов, потому что для такой утилизации необходимы соответствующие сертификаты, оборудование и документация. А также, выкинуть оборудование, содержащее опасные ядовитые вещества, потому что обезвреживать их следует в специальных условиях.

В процедуру утилизации входит:

a) непосредственный процесс переработки, включающий в себя удаление вредных компонентов вручную, сортировка и измельчение пластика, измельчение остальных составляющих компьютера;
b) аффинаж, представляющий собой металлургический процесс изъятия высокочистых благородных металлов при отделении от них загрязняющих примесей;
c) уничтожение компонентов, не допускающих повторного использования.

Согласно требованиям СанПиН 2.1.7.1322-03 сбор и временное хранение ртуть содержащих отходов должны осуществляться следующим образом:

a) специализированном контейнере с чехлом, расположенном в отдельном помещении с ограниченным доступом персонала. Помещение должно быть сухим и светлым, иметь естественную и принудительную вентиляцию. Допускается хранение отработанных содержащих ртуть

ламп в неповрежденной таре из-под новых ламп или в другой таре, обеспечивающей их сохранность при хранении, погрузочно-разгрузочных работах и транспортировании;

b) место временного хранения должно быть промаркировано и оборудовано средствами локализации и удаления загрязнения ртутью при разрушении ламп или других приборов;

c) хранение поврежденных содержащих ртуть ламп должно осуществляться в специальной таре, не допускается совместное их хранение с неповрежденными лампами.

За использование, функционирование и утилизацию приборов освещения несет ответственность организация, предоставляющее помещение для проведения соревнований.

Также деятельность компании связана с документами, поэтому необходимо утилизировать бумажные документы при помощи шредера.

5.3 Чрезвычайные ситуации

5.3.1 Пожарная безопасность при работе с ЭВМ

Каждый человек при работе с ЭВМ обязан строго соблюдать правила пожарной безопасности и не допускать действий, которые могут послужить причиной возникновения пожара. Следует придерживаться максимальной осторожности и концентрации во время обслуживающих, ремонтных и профилактических работ. Это обусловлено использованием различных смазочных материалов, легковоспламеняющихся жидкостей, прокладок, временных электропроводок, а также выполняются такие виды работ как пайка или чистка отдельных узлов и деталей. Оптимальным вариантом для предотвращения возгорания является прокладка всех видов кабелей в металлических газонаполненных трубах.

Не менее важным и обязательным пунктом профилактики возгорания является установка пожарных кранов в коридорах, на площадках лестничных клеток и у входов. Для скорейшего ликвидирования пожароопасной ситуации необходимо тушить пожар с помощью ручных углекислотных

огнетушителей, установленных в помещениях из расчета один огнетушитель на 40-50 м2.

5.3.2 Требования по обеспечению пожарной безопасности

На рабочем месте запрещается иметь огнеопасные вещества. В помещениях запрещается:

a) зажигать огонь;
b) включать электрооборудование, если в помещении пахнет газом;
c) курить;
d) сушить что-либо на отопительных приборах;
e) закрывать вентиляционные отверстия в электроаппаратуре.

При возникновении пожароопасной ситуации или пожара персонал должен немедленно принять необходимые меры для его ликвидации, одновременно оповестить о пожаре администрацию. Помещения с электрооборудованием должны быть оснащены огнетушителями типа ОУ-2 или ОУБ-3.

ЗАКЛЮЧЕНИЕ

Конфиденциальность информации на сегодняшний день занимает одно из важных мест в вопросе организации информационной безопасности. Поток информации увеличивается с каждым годом, что повышает опасность утечки данных, как для отдельного человека, так и для организаций. Поэтому очень важно подходить к вопросу об осуществлении безопасности данных с крайней важностью и вниманием, потому что последствия могут быть невосполнимы.

Для организации обеспечение информационной безопасности имеет наивысшую ценность и поэтому руководство обязано обеспечить многоуровневую и комплексную защиту от несанкционированного доступа. Начиная от планировки особо важных помещений, заканчивая методиками увольнения сотрудников.

При выполнении бакалаврской работы были проведены как анализ деятельности предприятия, так и анализ защиты от утечки информации. Соответственно, также было проведено исследование информационной безопасности в частности анализы комплекса информационных и технических средств, уровня безопасности, определение источников угроз и определение вероятного нарушителя безопасности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1 Использование настроек в приложениях на C#. [Электронный ресурс]. – Режим доступа: https://www.youtube.com/watch&v=MFmg6xVCu68&t

2 Авторизация в Form [Электронный ресурс]. – Режим доступа: https://www.youtube.com/watch?v=OQYSv_fcudI&t=14s

3 Гагарина, Л.Г. Информационные технологии / Л.Г. Гагарина, Я.О. Теплова, Е.Л. Румянцева, А.М. Баин — М.: Форум. Профессиональное образование, 2015. — 320 с.

4 Демидов, Л.Н. Информационные технологии. Учебник / Л.Н. Демидов, В.Б. Терновсков. — М.: КноРус. Бакалавриат, 2017. — 222 с.

5 Шаньгин, В.Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин — М.: ДМК Пресс, 2017. — 702 с.

6 Жук, Ю.А. Информационные технологии. Мультимедиа / Ю.А. Жук. — СПБ.: Лань Спб, 2018. — 208 с.

7 Плаксин, М.А. Тестирование и отладка программ для профессионалов будущих и настоящих / М.А. Плаксин. – М.: БИНОМ. Лаборатория знаний, 2013. – 167 с.

8 Родин, Ю.А. Доступные методы противодействия компьютерным угрозам / Ю.А. Родин, С.Г. Самохвалова // Вестник АмГУ. – 2014. – Т. 65. – С. 51–57.

9 Родин, Ю.А. Способы защиты от вредоносных компьютерных программ / Ю.А. Родин // Молодежь XXI века: шаг в будущее: материалы XIV региональной научно-практической конференции с межрегиональным и международным участием: в 7 т. – Благовещенск: ДальГАУ, 2013. – Т. 7: Физико-математические науки. Технические науки. – С. 48–49.

10 Жук, А.П. Защита информации. Учебное пособие / Жук А.П., Жук Е.П., Лепешкин О.М., Тимошкин А.И. – М.: Риор, 2019. – 499 с.

11 Белоус, А. И. Кибероружие и кибербезопасность. О сложных вещах

простыми словами / А.И. Белоус, В.А. Солодуха. – М.: Инфа-Инженерия, 2020. – 692 с.: ил.

12 http://internetinside.ru/internet-veshhey-setevaya-arkhitektura-i/: [Электронный ресурс]: Интернет вещей: сетевая архитектура и архитектура безопасности. – Дата обращения: 18.05.2020г.

13 Ященко, В. В. Введение в криптографию / Под общ. ред. В. В. Ященко. — 4-е изд., доп. М.: МЦНМО, 2012. — 348 с.

14 Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях: Учебное пособие / М.А. Иванов, И.В. Чугунков. – М.: НИЯУ МИФИ, 2012. – 400 с.: ил.

15 Шварц, М. Интернет вещей с ESP8266 / М. Шварц - БХВ-Петербург, 2018. – 192 с.

16 Грингард, С. Интернет вещей. Будущее уже здесь / С. Грингард - Альпина Паблишер, 2017. – 188 с.

17 Артемьев, И.Е. Интернет вещей. Исследования и область применения / И.Е. Артемьев, Е.П. Зараменских – Инфра-М – 2017. – 188 с.

18 Таненбаум, Э. Компьютерные сети / Э. Таненбаум, Д. Уэзеролл – 5-е изд. – Питер, 2016. – 960 с.

19 http://postscapes.com/internet-of-things-platforms?order=rhits/: [Электронный ресурс]: IoT Cloud Platform Landscape. – Дата обращения: 19.05.2020г.

20 https://www.kaspersky.ru/blog/internet-of-things-and-cybersecurity-of-infrastructure/7394/: [Электронный ресурс]: Интернет вещей и безопасность инфраструктуры. – Дата обращения: 19.05.2020г.

ПРИЛОЖЕНИЕ А

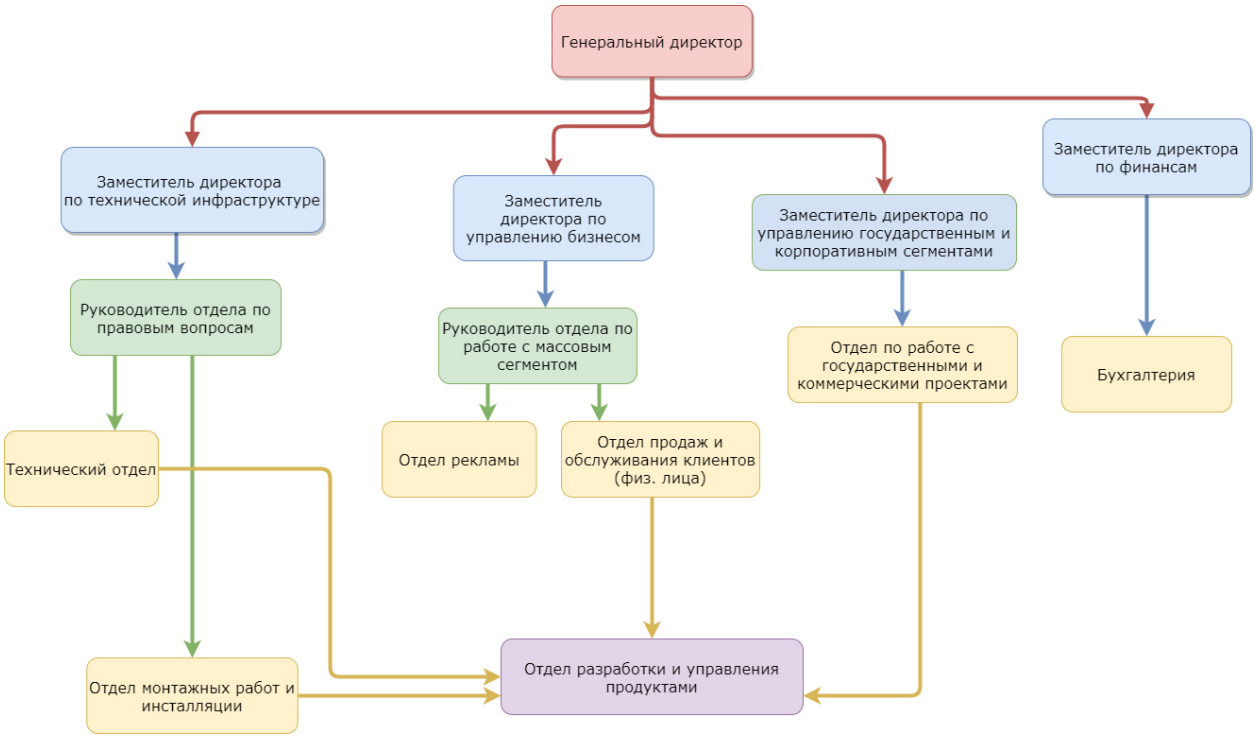

Рисунок А1 - Функциональная структура компании

ПРИЛОЖЕНИЕ Б

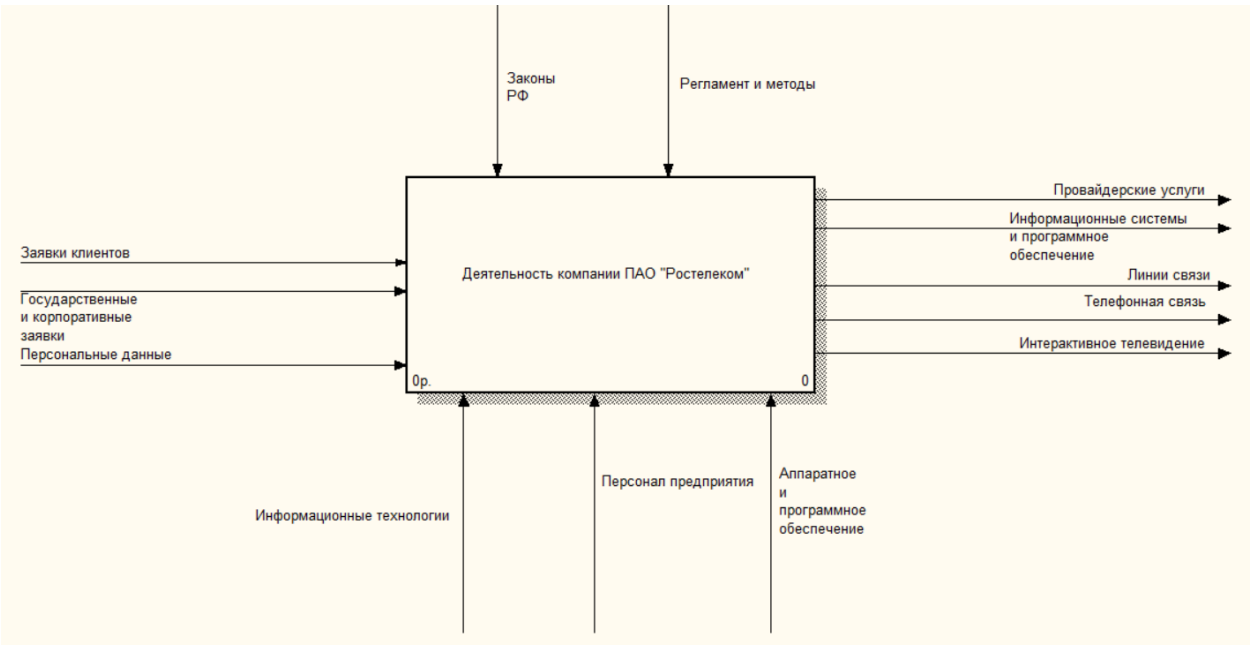

Рисунок Б1 - Функциональная структура компании

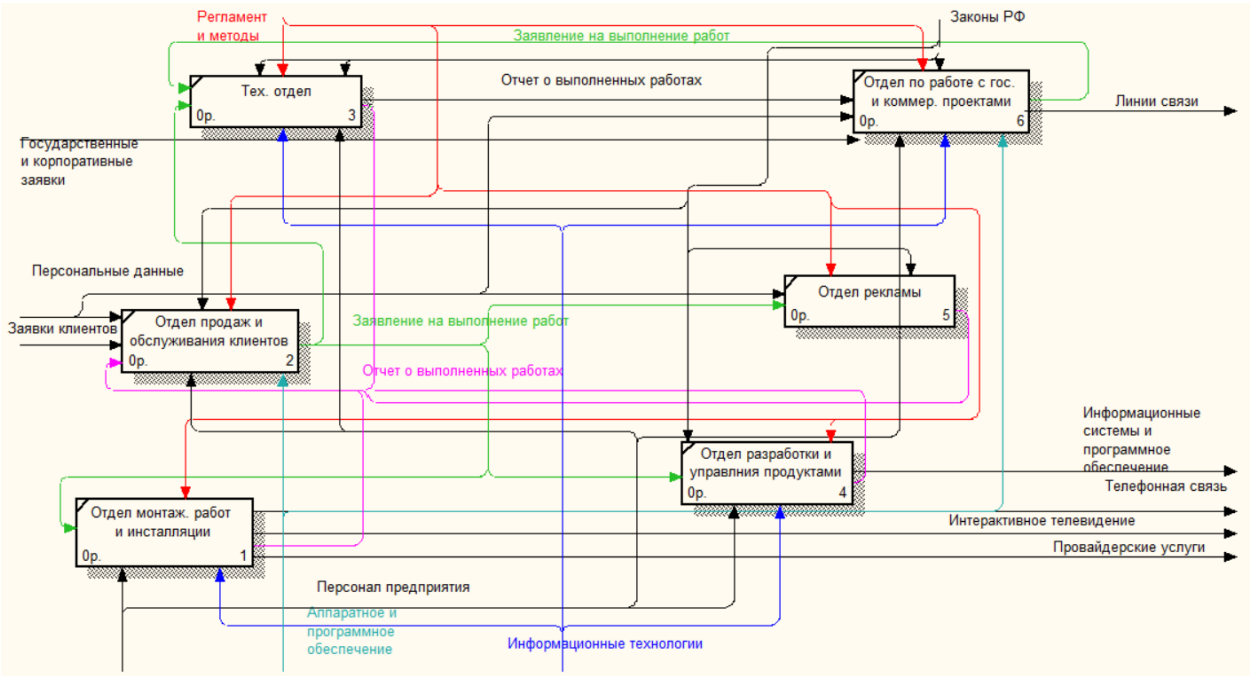

Рисунок Б2 - Декомпозиция функциональной модели

ПРИЛОЖЕНИЕ В

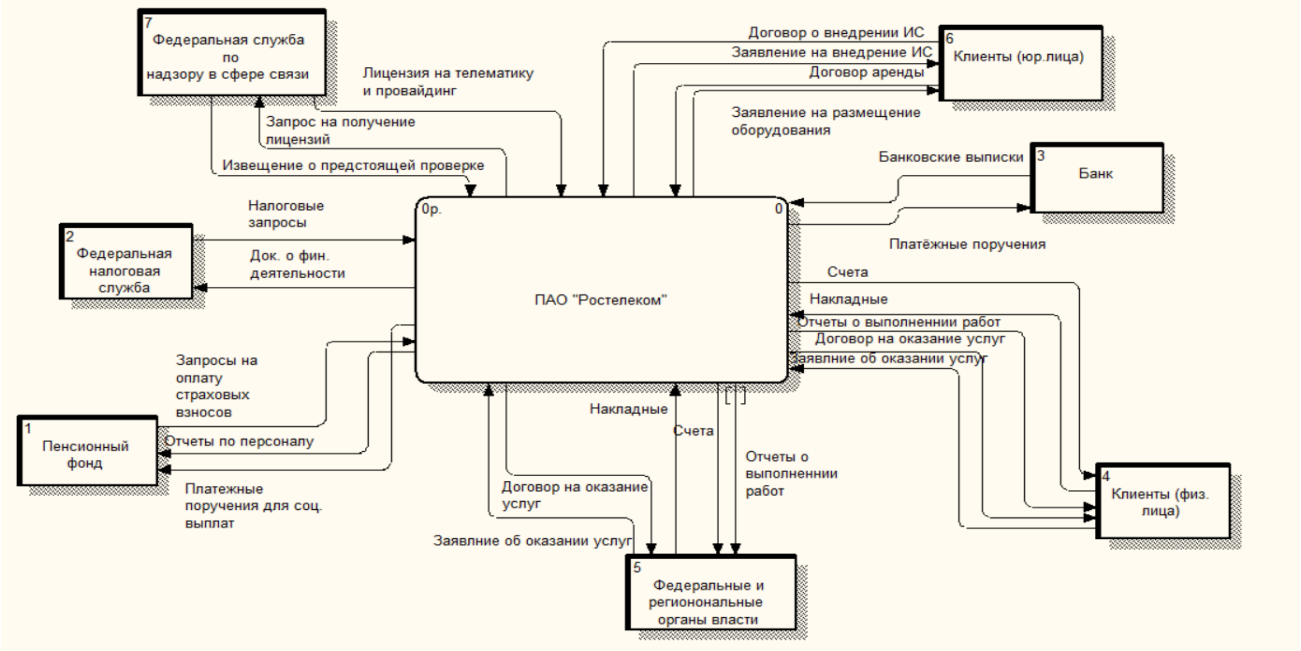

Рисунок В1 - Диаграмма внешнего документооборота

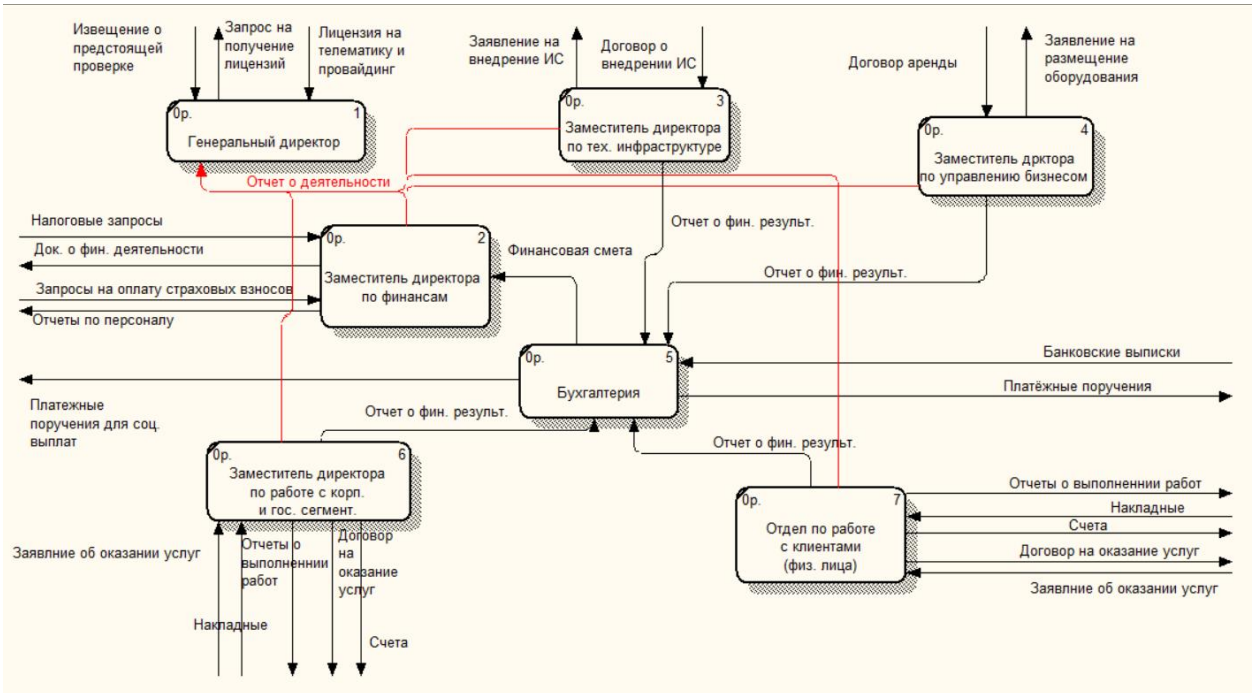

Рисунок В2 – Диаграмма внутреннего документооборота