МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

САМАРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПУТЕЙ СООБЩЕНИЯ (СамГУПС)

«Строительство железных дорог и информационные технологии»

(наименование института/факультета полностью)

Кафедра «Прикладная математика, информатика и информационные системы»

(наименование кафедры)

09.03.02 Информационные системы и технологии

(код и наименование направления подготовки)

(направленность (профиль))

ДИПЛОМНАЯ РАБОТА

на тему

«Централизованное управление мобильными устройствами. Обеспечение защиты мобильных устройств и информации на нем. Модуль обеспечения защиты мобильных устройств и информации на нем.»

Студент Д.А. Корунов

Руководитель Л.И. Папировская

Допустить к защите

Заведующий кафедрой доктор т. н., доцент, А.А.Тюгашев

(ученая степень, звание, И.О. Фамилия)

(личная подпись)

«_____» _____20____г.

CAMAPA 2020

З А Д А Н И Е

на выпускную квалификационную работу бакалавра

Студенту Корунов Д.А.

Руководитель Папировская Л.И., СамГУПС, доцент кафедры ПМИИС

1. Наименование темы:

«Централизованное управление мобильными устройствами. Обеспечение защиты мобильных устройств и информации на нем. Модуль обеспечения защиты мобильных устройств и информации на нем.»

2. Срок сдачи студентом законченной работы 14 июня 2020 г.

3. Техническое задание и исходные данные к работе

Проектирование модуля обеспечения защиты мобильных устройств и информации на нем.

Исходные данные:

- разработать файловую систему хранения данных;
- проектирование провести с использованием объектно–ориентированной нотации.

Модуль должен обеспечивать:

- авторизацию пользователя;
- систематизацию необходимых данных в файловой системе;
- передачу файлов в приложение на сервер администратора .

4. Содержание работы (перечень подлежащих разработке вопросов)

- провести анализ предметной области;
- провести анализ существующих информационных систем, использующихся на СамИВЦ;
- создать модуль защиты мобильных устройств и информации на нем.

5. Перечень графического материала (с указанием обязательного материала)

1. Обеспечение защиты мобильных устройств с использованием VipNET.
2. Схема работы модуля.
3. Архитектура EMM – McAfee.
4. Диаграмма развертывания.

5. Диаграмма деятельности.
6. Диаграмма последовательности действий.
7. Созданный файл.
8. Память мобильного устройства.
9. Процесс запроса доступа.
10. Процесс установки модуля.
11. Рабочая панель администратора.

6. Исходные материалы и пособия

- Методические рекомендации по выполнению выпускной квалификационной работы по направлению подготовки 09.03.02 «Информационные системы и технологии» / составители: А.П. Долгинцев, Е.А. Часовских - Самара: СамГУПС, 2017. - 39 с.
- ГОСТ 34.601-90. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания.
- ГОСТ 2.105-95 Единая система конструкторской документации. Общие требования к текстовым документам.
- Положение об адаптации и наставничестве работников в Главном вычислительном центре – филиале открытого акционерного общества «Российские железные дороги» и его структурных подразделениях– Москва, 2016.
- Инструкционный материал по системе ЕК АСУТР, АСУ ЕСПП.

7. Календарный план

№ п/п	Наименование этапов работы	Сроки выполнения	Прим.
1.	Цель и задачи выпускной квалификационной работы.	11.04.2020	
2.	Описание объекта исследования, обзор существующих методов решения.	30.04.2020	
3.	Обзор и анализ известных источников научно-технической информации по теме работы и смежным областям знаний.	30.04.2020	
4.	Анализ и формализация системы.	15.05.2020	
5.	Проектная часть оптимальных решений.	15.05.2020	
6.	Практические результаты выполнения работы	03.06.2020	

	и заключение.		

8. Дата выдачи задания 10 марта 2020 г.

Руководитель _____ /Л.И. Папировская/

(подпись)

Задание принял к исполнению _____ /Д.А. Корунов /

(подпись)

РЕФЕРАТ

Выпускная квалификационная работа.

Пояснительная записка: 67 страниц, 11 рисунков, 20 источников,
1 приложение.

Графическая документация: презентация.

Перечень ключевых слов: ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ИНФОРМАЦИОННАЯ СИСТЕМА, СИСТЕМА ОБЕСПЕЧЕНИЯ ЗАЩИТЫ МОБИЛЬНЫХ УСТРОЙСТВ И ИНФОРМАЦИИ НА НЕМ.

В выпускной квалификационной работе представлен спроектированный модуль защиты мобильных устройств и информации на нем.

Объект исследования: Защита информации на мобильном устройстве в ОАО «РЖД».

Цель работы: Создание модуля для обеспечения защиты мобильного устройства и информации на нем, для снижения утечки коммерческой информации.

Полученные результаты: Проектное решение, отвечающее поставленному техническому заданию.

Новизна результата: Упрощение процедуры контроля за мобильными устройствами.

Эффективность: Система централизованного управления и обеспечения защиты мобильного устройства и информации на нем, намного облегчит процесс контроля за самим устройством, и уменьшит вероятность утечки коммерческой информации.

СОДЕРЖАНИЕ

1)

Лист расшифровки

RMM - Remote monitoring and management (удалённый мониторинг и управление).

РЖД – Российские железные дороги.

МСК – Мобильное средство коммуникации.

ИС – Информационная система.

IPSEC – IP security.

СУБД – Система управления базы данных.

БД – База данных.

MDM – Mobile device management(Менеджер мобильного устройства).

ПО – Программное обеспечение.

ОС – Операционная система.

АСУ – Автоматизированная система управления.

АРМ – Автоматизированное рабочее место.

ИТ – Информационные технологии.

VPN - Virtual Private Network(виртуальная частная сеть).

АС ОЗ – Автоматизированная система обработки запросов.

ЦОД – Центр обработки данных.

КВД — Критически важные данные.

ПЭВМ – Персональная электронная вычислительная машина.

МУ – Мобильное устройство.

Введение

«Российские железные дороги» являются крупнейшим в нашей стране транспортным предприятием со 170-летней историей. Эксплуатационная длина принадлежащих холдингу магистралей составляет 85,5 тыс. км, по которым сейчас перевозится свыше 1,3 млрд пассажиров и 1,3 млрд т грузов в год. Таким образом, на долю РЖД приходится не менее 9% пассажирооборота и около 18% грузооборота всей мировой железнодорожной индустрии. В состав холдинга входят 17 филиалов (региональных железных дорог) и более 125 дочерних и ассоциированных компаний. Информационно техническим обеспечением ОАО «РЖД» занимаются 18 централизованно управляемых специализированных предприятий, в распоряжении которых находятся более 500 основных и несколько тысяч вспомогательных информационных систем, обеспечивающих комплексную автоматизацию внутренних бизнес-процессов холдинга и его деятельности по обслуживанию потребителей транспортных услуг. Совокупная мощность вычислительных ресурсов ОАО «РЖД» составляет 35 миллиардов операций в секунду.

В рамках проекта рассматривается деятельность Самарского информационно-вычислительного центра. Самарский информационно-вычислительный центр – структурное подразделение ГВЦ - филиала ОАО «РЖД» - предприятие, осуществляющее свою деятельность в сфере предоставления информационно-вычислительных услуг и обеспечивающее функционирование и дальнейшее развитие сложной компьютерной сети в регионе Куйбышевской

железной дороги. В составе сети находится центральный вычислительный комплекс баз данных и приложений, емкость центрального хранилища данных – более 200 Тбайт. Эксплуатируемые информационные технологии обеспечивают в режиме реального времени реализацию задач, связанных с управлением грузовыми и пассажирскими перевозками, инфраструктурой железнодорожного транспорта, продажей билетов на поезда, реализацией финансовых расчетов с клиентами, управления экономикой, материально-техническим снабжением и рядом других задач.

Основным видом деятельности технологов вычислительных центров является процесс технологического сопровождения систем, используемых холдингом ОАО «РЖД». В рамках этого процесса сотрудниками центра выполняются задачи администрирования и поддержки пользователей. В связи с реформацией деятельности вычислительного центра, отдельно взятый технолог обслуживает пользователей не только железной дороги, в состав которой входит его регион, но и клиентов других дорог. В настоящее время процесс удаленного управления мобильными устройствами и защиты информации на них реализован единственным встроенным решением в пакет антивирусной программы Kaspersky MDM. В рамках моей выпускной квалификационной работы уже разработан модуль мобильного приложения, который обеспечит полный доступ к устройству и позволит контролировать передаваемую информацию и уменьшить утечку коммерческой информации.

1. СИСТЕМОТЕХНИЧЕСКАЯ ЧАСТЬ

1.1 Мобильные устройства

Рассмотрим такие устройства, как смартфоны, интернет планшеты, электронные книги, телефоны, нетбуки. Главная их особенность - это размер. А если это качество сопоставить с количеством выполняемых устройством функций, мы получим основной критерий определяющий мобильное устройство.

Итак, наиболее важной особенностью мобильного устройства является его размер и способность к транспортированию. В случае смартфонов эта особенность находится на высоте. Они легко помещаются в карман или в сумочку. И имеют очень большой ряд функциональных возможностей. Транспортировать такое устройство легко и приятно. Можно ходить где угодно, а как только устройство понадобиться, достать и начать с ним работать. Но не все функции по силам смартфонам. Полноценный поиск по интернету, чтение электронных книг и еще много функций эти устройства просто не могут выполнить на желаемом уровне. И тут нам на помощь приходит новый класс мобильных устройств планшеты. По сути это те же смартфоны, только экран у них стал в разы больше. Соответственно возросла и производительность. Но вместе с этими параметрами увеличились и размеры мобильного устройства, а значит его мобильность немного пострадала, но и это спорное заявление ведь появившиеся возможности могут с лихвой компенсировать это. Итак, интернет-планшеты имея большой экран, позволяют во всей красе наслаждаться интернетом, книгами, офисными пакетами. Так

же мобильные устройства дают возможность работникам взаимодействовать с корпоративной системой компании удаленно, например когда они находятся в командировке. Мобильные устройства предоставляют саму возможность мобильности, то есть не привязанность работника к определённому месту. Конечно, размеры планшетов уже не позволяют носить их в кармане, для этого необходима сумка или портфель. Но для большинства людей это и так привычная экипировка. А функциональные возможности этих устройств просто поражают.

Электронные книги-это устройства, очень напоминающие по своему характеру интернет планшеты, только они узко специализированы. Основная их задача это чтение книг, электронных файлов. С этим они справляются на отлично. Мобильные устройства такого типа основаны на матрице «e-ink», которая по своим свойствам имитирует обычную бумагу. Это значит, что экран не имеет подсветки и на вид воспринимается глазом как обычный лист бумаги. Это положительным образом сказывается на зрении. Плюсом книг является так же то, что обычные книги занимают много места и очень много весят. А в электронную можно загрузить тысячи экземпляров, а вес при этом не изменится. Но не стоит забывать о таком факторе мобильности как время работы от батареи. В этом плане выигрываю электронные книги. За счет их дисплея они потребляют малое количество энергии, и время их автономной работы составляет от трех до десяти дней. На втором месте расположились смартфоны. Они потребляют приличное количество заряда. И «проживают» от одного до трех дней на одном заряде

батареи. И на третьем месте располагаются интернет планшеты. Их время автономной работы составляет не более 10 часов в зависимости от интенсивности нагрузки. Но и этого достаточно учитывая их возможности. Функционировать мобильному устройству дает множество установленных модулей и программ на него. Например, модуль GPS, он дает возможность пользователю в любой момент времени найти себя на огромной карте мира или же проложить маршрут в нужное пользователю место. Или же рассмотрим файловый менеджер, этот программный продукт дает вам возможность взаимодействия с папками, их изменение, добавление или удаление, благодаря ему мы можем переносить наши файлы с одного устройства на другое. Одной из самых важных частей МУ является операционная система, она является комплексом взаимосвязанных программ, предназначенных для управления устройством и ресурсами, а также организации взаимодействия с пользователем.

1.2 Особенности операционных систем (ОС) мобильных устройств

Разработчики ОС для мобильных устройств работают над тем, чтобы приблизить возможности мобильных ОС к возможностям ОС для настольных и портативных компьютеров. Однако в ОС для мобильных устройств есть своя специфика.

Вирусные эпидемии на мобильных устройствах затрагивают от нескольких сотен до миллионов устройств. Статистика исследователей компании Positive Technologies уравнивает риски ОС Android и ОС iOS, несмотря на строгую

политику Apple в части обеспечения информационной безопасности.

Рассмотрим примеры наиболее известного мобильного ВПО: «Агент Смит», Culprit, SockPuppet или Unc0ver, Ztorg, Monokle.

Заподозрить заражение «Агентом Смитом» можно по заметному увеличению показа нерелевантной рекламы. Пока это единственное зафиксированное вредоносное действие этого ВПО, хотя, технически, оно имеет огромный вредоносный потенциал. Масштаб заражения Агентом Смитом – 25 млн. устройств, преимущественно, в Азии. Поведение ВПО частично напоминает работу таких вирусов, как Gooligan, Hummingbad, CopyCat. «Агент Смит» действует следующим образом:

1. Пользователь скачивает дроппер в составе зараженного приложения (бесплатной игры или приложения с возрастным цензом).

2. Дроппер проверяет наличие на мобильном устройстве популярных приложений, таких как WhatsApp, MXplayer, ShareIt.

3. Дроппер скачивает и распаковывает архив, который превращается в APK-файл, при необходимости, обновляет и заменяет легитимное популярное приложение на зараженный вариант.

Culprit – ВПО под ОС Android, представляющее собой встроенный в видеофайл код, эксплуатирующий уязвимость CVE-2019-2107 в ОС Android 7.0 до 9.0 (Nougat, Oreo, Pie). Достаточно открыть видеофайл, полученный в фишинговом

MMS или сообщении из мессенджера, и ВПО получает полные права в системе.

SockPuppet или Unc0ver – ВПО, позволяющее получить злоумышленнику права суперпользователя для систем iOS и MacOS (Jailbreak). ВПО скачивается в составе зараженного приложения, которое определенный промежуток времени было доступно даже в официальном магазине Apple. ВПО регулярно обновляется и эксплуатирует уязвимость CVE-2019-8605, которая наследуется новыми версиями iOS. В версиях iOS 12.2 и 12.3 уязвимость была закрыта, после чего вновь появилась в версии 12.4 и была пропатчена в версии 12.4.1.

Старый троян Ztorg под ОС Android после установки собирает сведения о системе и устройстве, отправляет их на командный сервер, откуда приходят файлы, позволяющие получить на устройстве права суперпользователя (Jailbreak). ВПО распространяется через зараженные приложения и рекламные баннеры.

Monokle под ОС Android и iOS – троян, позволяющий вести полноценный шпионаж за жертвой: записывать нажатия клавиатуры, фотографии и видео, получать историю интернет-перемещений, приложений социальных сетей и мессенджеров, вплоть до записи экрана в момент ввода пароля. Троян снабжен рядом эксплойтов для реализации необходимых прав в системе, распространяется, предположительно, с помощью фишинга и зараженных приложений. Первые версии ВПО появились под ОС Android, но уже появились версии для устройств Apple.

На основе анализа описанных примеров мобильного ВПО, а также каналов проникновения других образцов ВПО можно выделить следующие основные пути компрометации устройства:

- Установка пакета приложений APK из неофициальных маркетов.
- Установка зараженного приложения из официального магазина. В данном случае, после обнаружения зараженного приложения службой безопасности магазина, оно будет оперативно удалено, а установленное пользователями приложение будет обновлено на безопасную версию.
- Фишинг и социальная инженерия – SMS, MMS с привлекательными для жертвы вредоносным контентом или ссылкой. Или звонок от ложного «оператора связи» или «служащего банка» с требованием передать учетные данные. Известны несколько нашумевших случаев добровольной установки пользователями программы удаленного управления TeamViewer, якобы, по просьбе службы безопасности банка. После установки программы пользователи передавали злоумышленникам учетные данные для удаленного управления, что равнозначно передаче разблокированного телефона в чужие руки.

Концепция Bring Your Own Device, BYOD (использование для работы с корпоративными документами личного устройства) привносит в корпоративный сегмент целый класс угроз – мобильное устройство сотрудника становится точкой входа во внутреннюю сеть предприятия и источником утечек информации.

1.3 Мобильные приложения и информационная безопасность

Мобильные приложения - новый формат общения.

Почему они выгодны? Потому, что и в России, и по всему миру фактически произошла революция в мире мобильных устройств - это увеличило аудиторию потенциальных пользователей. Мультисенсорные экраны, свободный выход в интернет, легкий обмен информацией, объем памяти позволяют хранить и использовать на своем телефоне или смартфоне множество полезных приложений.

Для разработки концепции обеспечения информационной безопасности (ИБ) под информацией понимают сведения, которые доступны для сбора, хранения, обработки (редактирования, преобразования), использования и передачи различными способами, в том числе в компьютерных сетях и других информационных системах.

Информационные риски, вызванные распространением мобильных технологий, отличаются от стандартных проблем ИТ-безопасности компаний. Их уникальная природа требует нового подхода и новых решений.

Смартфоны содержат больше личной информации, чем любое другое устройство. Тем не менее лишь малое количество этих устройств должным образом защищено. Риску подвергаются и корпоративные данные. Смартфоны могут получать доступ к сети через различные каналы (Bluetooth, SMS, Wi-Fi, NFC), большинство из которых являются открытыми и позволяют взаимодействовать с другими устройствами. Таким образом, один зараженный

смартфон может быть использован для заражения другого устройства.

Аппаратная платформа смартфонов значительно более разнообразная, чем у стационарных компьютеров и ноутбуков, программное обеспечение часто бывает с открытым кодом. Более того, пользователи сами определяют необходимость установки обновлений, в результате чего система безопасности мобильного устройства остается нестабильной.

Алгоритм обеспечения безопасности планшетников также несовершенен. Зачастую в них не предусмотрены такие системы по контролю безопасности, как полное шифрование диска, персональные межсетевые экраны, контроль доступа к сети и защита от шпионских и вредоносных программ.

Прочие мобильные устройства имеют свои зоны уязвимости, которые индивидуальны для каждого прибора и сложно поддаются контролю. Возможность использования различных каналов связи, многообразие операционных систем, смешение личной и рабочей информации и постоянное нахождение в сети создают благодатную почву для кибератак. Еще больше усложняет задачу ИТ-служб тот факт, что многие устройства, используемые сотрудниками в рабочих целях для доступа к корпоративным сетям, являются их личной собственностью. Это ограничивает возможность контроля над работой устройств и затрудняет техническую поддержку.

Многоуровневый подход к безопасности

Для того чтобы гарантировать информационную безопасность мобильных устройств, простого шифрования и применения старых политик безопасности может оказаться недостаточно. Изучение опыта многих компаний позволяет утверждать, что для разработки эффективной стратегии защиты необходимо работать над обеспечением безопасности на четырех уровнях: сети, устройства, приложения, программная часть - системы.

Сети

Беспроводные сети относительно незащищены, поэтому с легкостью становятся объектом атаки. Следует убедиться, что политика безопасности сетевых провайдеров полностью отвечает стандартам, принятым в компании. ИТ-специалистам рекомендуется выбирать тех провайдеров, которые работают по принципу "чистый трафик" (clean pipe). Сервис "чистый трафик" позволяет анализировать сетевой трафик и своевременно вычислять и другие проблемы.

Необходимо также учитывать все виды мобильных устройств, которые могут подсоединиться к сети. Здесь ИТ-отдел могут ждать сюрпризы, например в лице сканеров штрих-кода с доступом к Wi-Fi, проверять которые в голову приходит немногим. Кроме того, стоит отказаться от мысли, что шифрование может решить проблему защиты. В мобильных коммуникациях существуют такие виды атак, которые могут обойти шифрование: например, вредоносные мобильные приложения, загруженные на устройство и запускаемые в момент шифрования.

Устройства

Комплексный подход к безопасности необходим на всех этапах жизненного цикла мобильного устройства - от его производства и доставки покупателю до использования и утилизации. Для начала должны быть установлены базовые средства защиты, шифрование и удаленная очистка информации. Инцидент с фармацевтической компанией Cardinal Health подтверждает важность этих мер. В июне 2010 г. стало известно, что один из ноутбуков, проданных на аукционе eBay, содержал конфиденциальные данные о компании. Политика безопасности Cardinal Health предусматривала необходимость уничтожения всех данных ИТ-департаментом на списанных ноутбуках. Однако IT-специалист компании признался, что пренебрег этой процедурой и продал злополучный ноутбук и еще 10 компьютеров на аукционе eBay. Ноутбук содержал личную информацию сотрудников, и получить его обратно не удалось. Автоматические процедуры очистки устройства помогли бы избежать таких неприятностей.

Компании также должны быть готовым к тому, что сотрудники используют в рабочих целях свои личные смартфоны, которые могут быть приобретены не вполне благонадежными путями - например, по объявлению в Интернете или в неофициальной точке продаж. Иногда пользователи сами нарушают правила безопасности и устанавливают переадресацию корпоративных сообщений на личные адреса электронной почты, чтобы получать к ним доступ со смартфона. Кроме того, многие пользователи взламывают защиту своих мобильный устройств от компании Apple (jail-break), нарушая стандартные контрактные

ограничения компании Apple и делая устройства уязвимее к атакам.

Компаниям рекомендуется устанавливать специальные антивирусные программы и допускать к сетевому подключению только устройства с проверенной конфигурацией. Специальные интеллектуальные системы помогут анализировать события и трафик и предупреждать ИТ-специалистов о потенциально опасном поведении пользователей.

Приложения

Уязвимости в безопасности могут быть вызваны неправильной работой мобильных приложений. Большинство приложений разрабатывается без учета требований безопасности, так как предполагается, что использоваться они будут в защищенном периметре.

При разработке мобильных приложений для корпоративных целей компании должны убедиться в том, что они исключают обмен конфиденциальной информацией с другими приложениями.

Пристальное внимание должно уделяться безопасности работы приложений, скачиваемых пользователями в сети. Положительную роль могут сыграть регулярные дистанционные проверки установленных приложений. Инструменты по предотвращению утечки данных могут особо помечать конфиденциальную информацию и предотвращать ее неразрешенное использование.

Программная часть -системы

Сегодня все больше элементов программная часть - систем работает по принципу облачных технологий. Перед

выбором облачного провайдера компании следует ответить на такие вопросы: сможет ли провайдер обеспечить должные меры безопасности? Существуют ли специфические нормативные требования к хранению информации, ее передаче и доступу к ней? Какие системы управления, мониторинга, предупреждения и реагирования должны применяться для лучшей защиты?

В любом случае, для разработки и внедрения в компании комплексного подхода к безопасности требуется время.

1.4 Обеспечение информационной безопасности холдинга ОАО «РЖД»

Безопасность Информационных Систем – свойство, заключающееся в способности системы обеспечить конфиденциальность и целостность информации, т.е. защиту информации от несанкционированного доступа с целью её раскрытия, изменения или разрушения.

Информационную безопасность часто указывают среди основных информационных проблем XXI в. Действительно, вопросы хищения информации, её сознательного искажения и уничтожения часто приводят к трагическим для пострадавшей стороны последствиям, ведущим к разорению и банкротству фирм и даже к человеческим жертвам. В законе Российской Федерации «Об информации, информатизации и защите информации», например, подчёркивается, что «...информационные ресурсы являются объектами собственности граждан, организаций, общественных объединений, государства» и защищать

информационные ресурсы, естественно, следует, как личную, коммерческую и государственную собственность.

Все угрозы информационным системам можно объединить в обобщающие их три группы:

1. Угроза раскрытия – возможность того, что информация станет известной тому, кому не следовало бы её знать.

2. Угроза целостности – умышленное несанкционированное изменение (модификация или удаление) данных, хранящихся в вычислительной системе или передаваемых из одной системы в другую.

3. Угроза отказа в обслуживании – возможность появления блокировки доступа к некоторому ресурсу вычислительной системы.

При обеспечении безопасности важной составляющей является обеспечение безопасности персональных данных.

Согласно федеральному закону N 152 ФЗ «О персональных данных», персональные данные - любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

В законе рассматривается порядок работы с данными, что позволяет обеспечивать защиту прав и свобод человека и гражданина.

В работе железной дороги используется внутренняя сеть Intranet.

Подключение пользователя к информационным ресурсам осуществляется только после согласования заявки АС ОЗ.

Подключение предоставляется на два года с момента создания заявки.

В рамках обеспечения информационной безопасности холдинга ОАО «РЖД» к пользователям предъявляются следующие требования:

Внутренний пользователь при работе в информационных системах ОАО «РЖД» обязан:

1) сохранять в тайне свои пароли (ключевые носители) доступа к ПЭВМ, а также к автоматизированным рабочим местам;

2) во время перерывов в работе с информационными системами ОАО «РЖД», содержащими сведения, составляющие коммерческую тайну ОАО «РЖД», обеспечивать блокирование ПЭВМ парольной экранной заставкой;

3) обеспечивать при помощи установленного антивирусного программного обеспечения проверку используемых съемных носителей информации на наличие вредоносных программ;

4) при подозрении на появление на ПЭВМ вредоносных программ, автоматически не выявленных и не обезвреженных системой антивирусной защиты, незамедлительно отключать ПЭВМ от сети передачи данных и сообщать об этом в единую службу поддержки пользователей;

5) в случае полного или частичного прекращения работы антивирусного программного обеспечения незамедлительно сообщать об этом в единую службу поддержки пользователей;

6) при обнаружении некорректной работы программного обеспечения на ПЭВМ обращаться в единую службу поддержки пользователей.

Внутреннему пользователю при работе в информационных системах ОАО «РЖД» запрещается:

1) допускать использование ПЭВМ иными лицами, кроме работников Главного вычислительного центра ОАО «РЖД» (информационно-вычислительного центра – структурного подразделения Главного вычислительного центра ОАО «РЖД»), обслуживающих данную ПЭВМ, и работников Департамента безопасности ОАО «РЖД» (регионального центра безопасности – структурного подразделения ОАО «РЖД»), осуществляющих контрольные функции;

2) осуществлять несанкционированное подключение к ПЭВМ и сетевому оборудованию внешних устройств, в том числе устройств телекоммуникации и обработки информации;

3) использовать ПЭВМ в непроизводственных целях;

4) передавать информацию конфиденциального характера по незащищенным каналам сети передачи данных ОАО «РЖД»;

5) отключать «агента безопасности» либо вносить изменения в его настройки (кроме специалистов Главного вычислительного центра ОАО «РЖД» или информационно-вычислительного центра – структурного подразделения Главного вычислительного центра ОАО «РЖД», обслуживающих данную ПЭВМ), а также самостоятельно устанавливать любые программные продукты на ПЭВМ или

разрешать это кому-либо, кроме специалистов Главного вычислительного центра ОАО «РЖД» или информационно-вычислительного центра – структурного подразделения Главного вычислительного центра ОАО «РЖД»;

6) использовать ПЭВМ с частично или полностью неработающим антивирусным программным обеспечением, а также некорректной работой программного обеспечения;

7) использовать на ПЭВМ сменные носители информации, в том числе внешние средства хранения информации, без предварительной проверки на наличие вредоносных программ;

8) предоставлять сетевой доступ к своему автоматизированному рабочему месту другим пользователям.

Внутреннему пользователю при работе в информационных системах общего пользования запрещается:

1) публиковать свои адреса (электронной почты, IP-адреса и т.п.), а также адреса других работников ОАО «РЖД» на общедоступных Интернет-ресурсах (форумы, конференции и т.п.);

2) использовать общедоступные электронные почтовые системы и иные службы обмена сообщениями в личных целях, а также для распространения любой информации;

3) подключать к информационным системам общего пользования автоматизированные рабочие места, на которых осуществляется обработка информации конфиденциального характера;

4) передавать сведения, создающие угрозу безопасности и обороноспособности государства, здоровью и безопасности людей;

5) запускать на ПЭВМ исполняемые файлы, полученные из информационных систем общего пользования (файлы с расширением exe, com, bat, scr, reg и т.п.);

6) обращаться к потенциально опасным ресурсам информационных систем общего пользования.

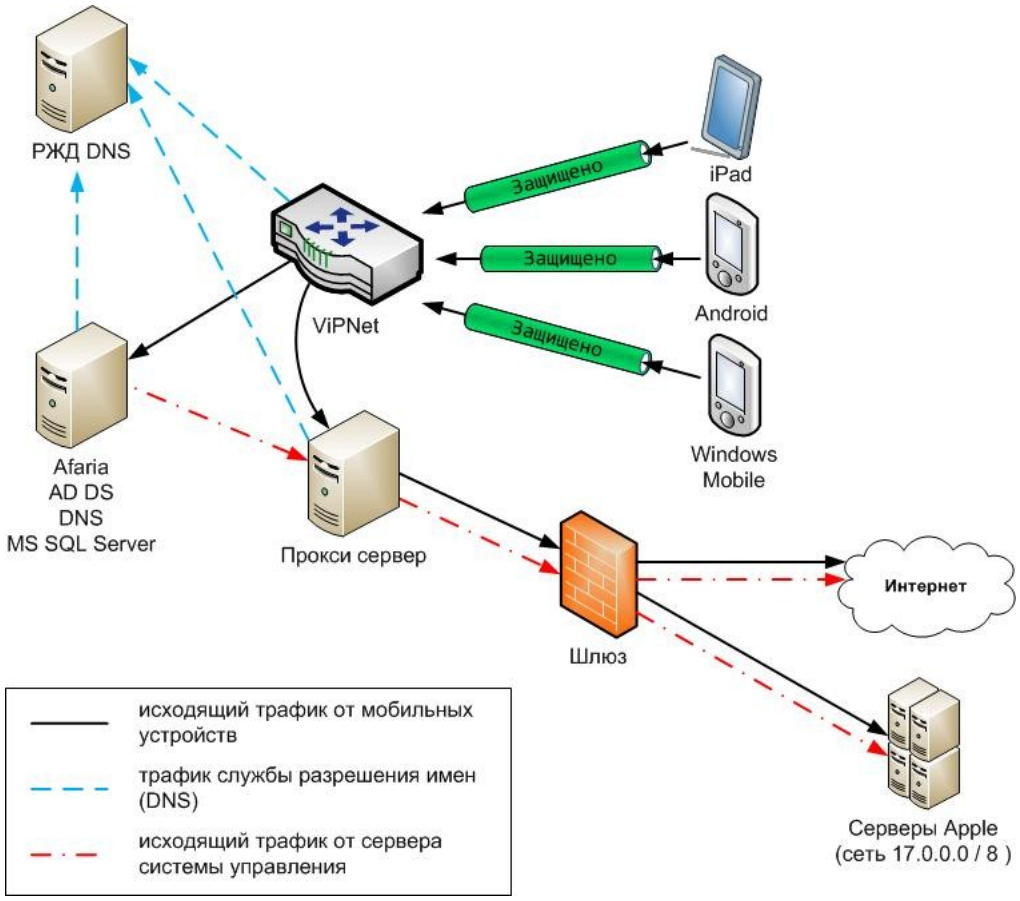

Рис. 1 Обеспечение защиты мобильных устройств с использованием VipNET.

1.5 Применение мобильных средств коммуникации при организации информационного взаимодействия с Информационными системами ОАО «РЖД».

Одной из главных причин популярности мобильных технологий является возрастающая мобильность сотрудников. Организации хотят создать более гибкие условия работы для своих сотрудников. Однако, по их оценкам, 76% сотрудников все ещё работают полный день в офисе, а 53% не работают на выезде. Новые принципы работы персонала предполагают не только использование новых технологий, но и изменение рабочего процесса и политики компаний.

Современные мобильные средства коммуникации (МСК) обладают различными интерфейсами: media: аудиозапись, фото- и видеосъёмка (камера); средства беспроводной связи (GPRS/EDGE/3G/LTE,Wi-Fi), Bluetooth, GPS, биодатчики и др., обеспечивающими разноплановые возможности его использования, но в то же время, создающими множество угроз информационной безопасности.

Организация должна иметь корпоративную политику использования мобильных устройств в бизнес-процессах. Политика может быть в диапазоне от «Всё запрещено» до «Всё разрешено», но правильно будет - «Всё разрешено, кроме того, что явно запрещено».

Не секрет, что сейчас МСК в ОАО «РЖД» подключаются к информационной системе компании различными способами, и с использованием технологии ViPNet, и с использованием средств VPN IPSEC, а это всего лишь

шифрование трафика, и таких процедур как контроль от утечки информации, доступа к Интернет ресурсам с мобильного устройства никак не производится. Часто на самих МСК, без установленных на них средств защиты, передаётся конфиденциальная информация с использованием публичных почтовых и файловых сервисов, и неудивительно, что передаваемые, казалось бы, конкретному адресату документы оказываются доступными всему миру – а это прямой ущерб имиджу компании, это и экономические потери для бизнеса (возможно вплоть до политических).

Применение мобильных технических средств в ОАО «РЖД», на сегодняшний день, регулируется Распоряжением ОАО «РЖД» от 01.11.2013г. №2347р «Об утверждении Порядка использования мобильных технических средств в ОАО «РЖД» [19], в котором изложены требования и условия возможного применения этих устройств при организации взаимодействия с корпоративными ресурсами.

Включение личных мобильных устройств и планшетов в бизнес-среду требует огромных ресурсов для управления настройками и обеспечения безопасности. Рационально учесть бизнес-потребности и при этом дать возможность специалистам информационной безопасности эффективное средство контроля за парком устройств, которые используют корпоративные ресурсы, способны только специализированные решения класса Mobile Device Management (MDM).

Разработанные для управления инфраструктурой мобильных устройств MDM-решения задают настройки

соответствия политикам безопасности и настройки доступа в корпоративную сеть для всех одобренных мобильных устройств. При этом с помощью этих настроек осуществляется регистрация и мониторинг устройств, а в случае потери или кражи смартфона или планшета с помощью MDM с него можно удалить корпоративные, либо вообще все данные.

В решениях MDM используются встроенные механизмы обеспечения безопасности мобильных операционных систем – профили безопасности. Профиль безопасности представляет собой аккаунт который ограничен администратором системы, с его помощью происходит защита информации на устройстве, ограничения установленные на профиль не позволяют скачивать и устанавливать несертифицированное ПО, переходить по небезопасным ссылкам. В случае необходимости они позволяют выполнить определённые настройки, запретить доступ к определённым программам и функциям устройства. Таким образом, загружая данный функционал, пользователь получает защищённое мобильное устройство.

MDM-решение представляет собой программно-аппаратный комплекс: сервер управления на стороне компании, прокси-сервер для передачи почтового трафика, клиент для мобильного устройства. Установив это приложение, администратор вводит корпоративные логин и пароль, и на устройство в зависимости от прав пользователя передаётся пакет настроек, связанных с получением доступа к корпоративным ресурсам (например, настройки VPN или почтового клиента). Информация о регистрации поступает

администратору, и устройство начинает отображаться в консоли управления.

С помощью MDM-систем можно реализовать запрет на получение приложений из недоверенных источников. MDM также может быть витриной доверенных приложений для пользователя.

Ещё одна важная функция MDM – обнаружение и контроль прошивок устройства. Можно определить, получены ли на устройстве Root-права (в случае с устройством на базе Android) и проводился ли на устройстве Jailbreak (в случае с iPhone и iPad).

Каким же образом система управления мобильными устройствами облегчает жизнь компании? Во-первых, она позволяет вести полуавтоматическую регистрацию пользователей и мониторинг использования мобильных устройств. Можно отслеживать, какие пользователи, с каких мобильных устройств и в какое время заходят в сеть. Самое главное – можно определять, соответствует ли все это политикам безопасности.

MDM-системы, при необходимости, позволяют использовать геолокационную информацию с мобильного устройства и определять точное местонахождение пользователя, а также, в случае использования био-датчиков, подключаемых к мобильному устройству (типа фитнес-браслетов) отображать основные параметры физического состояния пользователя (пульс, температура тела, давление), к примеру можно использовать для машинистов, службы охраны объекта).

В последнее время все чаще возникает вопрос владения мобильными устройствами. Раньше компания покупала сотруднику коммуникатор и имела полное моральное право требовать соблюдения корпоративных требований. Сейчас все усложнилось, поскольку устройство у сотрудника собственное. Поэтому активно используется подход user agreement: если пользователь хочет использовать корпоративные ресурсы, ему необходимо соответствовать определённым требованиям.

MDM: набор сервисов и технологий, обеспечивающих контроль и защиту мобильных устройств, используемых организацией и её сотрудниками. Понятие «мобильные устройства» в данном случае подразумевает смартфоны, планшеты и специализированные компьютеры, такие как терминалы сбора данных или мобильные платёжные системы. Управление мобильными устройствами преследует две основные задачи: обеспечение безопасности корпоративных данных на устройствах, находящихся вне сетевой инфраструктуры, а также контроль состояния самих устройств.

В виде готовых коммерческих (платных) решений на IT-рынке представлен широкий круг этих продуктов: SafePhone (разработчик ООО «НИИ СОКБ», единственный EMM-комплекс, сертифицированный ФСТЭК РФ), Kaspersky MDM, SAP Afaria, Symantec Mobile Management Suite, McAfee Enterprise Mobility Management, MobileIron, AirWatch® Mobile Device Management, Fiberlink MaaS360 (an IBM Company) MDM, XenMobile by CITRIX, MobiControl* by EXCITOR, Meet FAMOC™ by FancyFon и т.д.

Свободно распространяемые или Open Source MDM-системы, представленные на IT-рынке: OpenMEAP™, Convertigo Mobility Platform, WSO2 Enterprise Mobility Manager, OpenMobster, Free Mobile Device Management by Spiceworks, Meraki Systems Manager и т.д., хотя для расширенных версий (Enhanced или Enterprise), которые и представляют интерес, то за них все равно приходится платить деньги.

Общий сравнительный анализ MDM-систем, по их функциональным возможностям, возможностям доработки под нужды заказчика, сервисам технической поддержки и т.п., показывает, что наибольший интерес представляют всё же коммерческие решения.

В данный момент в ОАО «РЖД» существует только одна MDM система встроенная в пакет Kaspersky, под названием «Kaspersky MDM». Kaspersky Security для мобильных устройств помогает сотрудникам выполнять свои рабочие задачи на смартфонах и планшетах в любой точке мира, не подвергая риску важные бизнес-данные или критические бизнес-процессы.

Приложение обеспечивает многоуровневую защиту мобильных устройств, которая включает в себя защиту от вредоносных программ, антиспам, веб-контроль, контроль программ и устройств, а также предоставляет функционал Анти-Вора. Чтобы упростить задачи администрирования, все функции управляются из единой консоли.

Отслеживание, управление и защита мобильных устройств, используемых сотрудниками для работы, может требовать значительных ресурсов.

При этом надежная защита мобильных устройств в сегодняшних условиях просто необходима: количество угроз для них активно растет, а мобильные устройства для рабочего процесса порой не менее важны, чем настольные компьютеры.

Kaspersky Security для мобильных устройств обеспечивает их защиту и позволяет контролировать политики безопасности на каждом смартфоне или планшете, получающем доступ к корпоративным данным вашей сети.

Преимуществами системы является:

Защита мобильных устройств от специализированных угроз. Передовые технологии «Лаборатории Касперского» защищают мобильные устройства от широкого спектра угроз, в том числе от троянцев, вирусов-шифровальщиков и фишинговых атак. Гибкие настройки позволяют указать, какие приложения можно запускать на каждом мобильном устройстве. Кроме того, в корпоративной среде можно применять различные политики для определенных групп или отдельных пользователей.

Снижение риска потери данных. На мобильных устройствах могут храниться большие объемы конфиденциальной бизнес-информации. Это очень большой риск, учитывая, что ежегодно похищаются или теряются до трети мобильных устройств. Слабые пароли, использование опасных приложений и незашифрованные данные также могут привести к тому, что конфиденциальные сведения окажутся в чужих руках. Kaspersky Security для мобильных устройств упрощает введение обязательных сложных паролей, а также блокирование запуска

несанкционированных или нежелательных приложений. Решение включает функции Анти-Вора, которые защищают конфиденциальные данные в случае кражи или потери устройства. Администраторы (или пользователи через портал самообслуживания) могут удаленно блокировать приложения и доступ к данным, выборочно или полностью удалять информацию, а также отслеживать местонахождение устройства.

Эффективное и удобное управление. С учетом того, что в среднем каждый сотрудник использует три и более мобильных устройства, их отслеживание, управление и защита могут представлять собой сложную задачу. Kaspersky Security для мобильных устройств позволяет управлять всеми устройствами из единой консоли – той же самой, которая используется для администрирования всех рабочих мест, защищаемых с помощью технологий «Лаборатории Касперского». Такое решение снижает нагрузку на ваших IT-специалистов за счет централизации настройки и администрирования смартфонов и планшетов Android и iOS.

Так же одним из лидеров в данной сфере на российском рынке является предложение от ООО «НИИ СОКБ», их системы SafePhone сертифицирована ФСТЭК РФ.

SafePhone - сертифицированная ФСТЭК РФ, EMM-комплексная платформа для управления и обеспечения безопасности мобильной экосистемы предприятия (кратко):

Эффективность использования EMM SafePhone в организации:

1. Обеспечение бесперебойной работы сотрудников за счет централизованного управления их мобильными

устройствами, а также оперативной установки и обновления необходимых для работы корпоративных приложений;

2. Уникальная функциональность банка корпоративного программного обеспечения;

3. Снижение затрат на оплату мобильных телефонных переговоров;

4. Использование единого номера в компании при интеграции с корпоративной АТС;

5. Сокращение затрат на постройку сложной ИТ-инфраструктуры, за счёт использования сервисной модели, с размещением серверной части решения в защищённом ЦОД;

6. Контроль использования служебных мобильных устройств;

7. Предотвращение утечки конфиденциальной информации компании в случае утери или кражи мобильного устройств;

1.6 Разработка алгоритма модуля защиты мобильных устройств.

При разработке мобильного приложения следует учитывать, что данные, которыми оперирует это приложение, могут представлять определенный интерес для третьих лиц. Степень ценности этих данных варьируется в широких пределах, тем не менее, даже наиболее простая приватная информация, например, пароль входа в приложение, требует проработки ее защиты. Особенно это важно в свете распространения мобильных приложений на все сферы электронных услуг, включая финансовые, банковские операции, хранение и передачу личных данных и так далее. Защита мобильного приложения

Основные виды атак на мобильное приложение:

- Декомпиляция файла приложения (.ipa-файлы для Apple iOS и .apkфайлы для Google Android) и разбор локально сохраненных данных. Защита этого, наиболее важного в настоящее время, уровня целиком лежит на плечах мобильного разработчика.
- Перехват данных, передаваемых по сети (MITM-атаки). Большинство мобильных приложений являются клиент-серверными, следовательно, постоянно передают и принимают большие объемы информации. И хотя современная мобильная и веб-разработка активно завершают переход на HTTPS-протокол общения, тем не менее, не стоит полагаться на единственный рубеж защиты в виде защищенного канала связи.

- Настройки разработчика устройства и атака на приложение и применяемые в нем алгоритмы через внешние отладочные инструменты.

Рассмотрим уязвимости общего характера, без привязки к конкретной платформе. КВД — критически важные данные пользователей. К КВД относятся любые данные, которые не должны быть доступны третьей стороне, это касается как персональных данных пользователя (дата рождения, адрес проживания, личная переписка), так и его приватных данных (пароли, данные кредитных карт, номера банковских счетов, номера заказов и так далее).

Перечень основных уязвимостей:

1. Использование незащищенных локальных хранилищ.

Опасность: Очень высокая. Комментарий: Встречается повсеместно, выражается в хранении КВД в незащищенных или слабо защищенных локальных хранилищах, специфических для конкретной платформы. Вскрытие третьей стороной — элементарное, и, как правило, не требуется наличие специальных навыков у атакующего. Защита: Хранить КВД можно только в защищенных хранилищах платформы.

2. Хранение КВД в коде.

Опасность: Высокая. Комментарий: Уязвимость касается хранения КВД внутри кода (в статических константных строках, в ресурсах приложения и т.п.). Яркие примеры: хранение соли для пароля (password salt) в константе или макросе, которая применяется по всему коду для шифрования паролей; хранение приватного ключа для асимметричных алгоритмов; хранение паролей и логинов для

серверных узлов или баз данных. Легко вскрывается третьей стороной при наличии базовых навыков декомпиляции. Защита: Не хранить никакие КВД в коде или ресурсах приложения.

3. Применение алгоритмов с хранением приватного ключа.

Опасность: Высокая. Комментарий: Уязвимость актуальна в случае, если приватная информация алгоритма (приватный ключ) вынужденно сохраняется в коде или ресурсах мобильного приложения (чаще всего так и бывает). Легко вскрывается методом декомпиляции. Защита: В мобильной разработке желательно применять только современные симметричные алгоритмы с генерируемым случайным одноразовым ключом, обладающие высокой стойкостью с взлому методом грубой силы, либо выводить асимметричный приватный ключ за пределы приложения, либо персонализировать этот ключ (как пример — приватным ключом может выступать пользовательский код входа, сохраненный в зашифрованном виде в защищенном хранилище операционной системы).

Есть несколько общих для всех мобильных платформ моментов, которые следует соблюдать при разработке:

1. Защита пользовательским кодом. Если приложение защищено пользовательским паролем (PIN-кодом, сканом отпечатка пальца, графическим паролем и т.д.), то при уходе приложения в фон ("сворачивании") оно должно немедленно отображать окно ввода этого защитного кода, перекрывая собой весь экран приложения.

2. Функционирование клиент-серверного приложения. Для клиент-серверных приложений очень полезно применять сессионный механизм с ограниченным временем жизни сессии. Это позволит избежать "простаивания" приложения в незащищенном режиме, если пользователь просто забыл закрыть его и оставил устройство в свободном доступе.

3. Работа с датами. Абсолютные значения следует передавать с применением универсальных способов обмена подобной информацией, без привязки к часовому поясу конкретного пользовательского устройства. Чаще всего, оптимальным вариантом является поведение приложения, при котором данные отображаются пользователю в его локальном часовом поясе, но их хранение и передача осуществляется в формате, не привязанном к тайм-зоне.

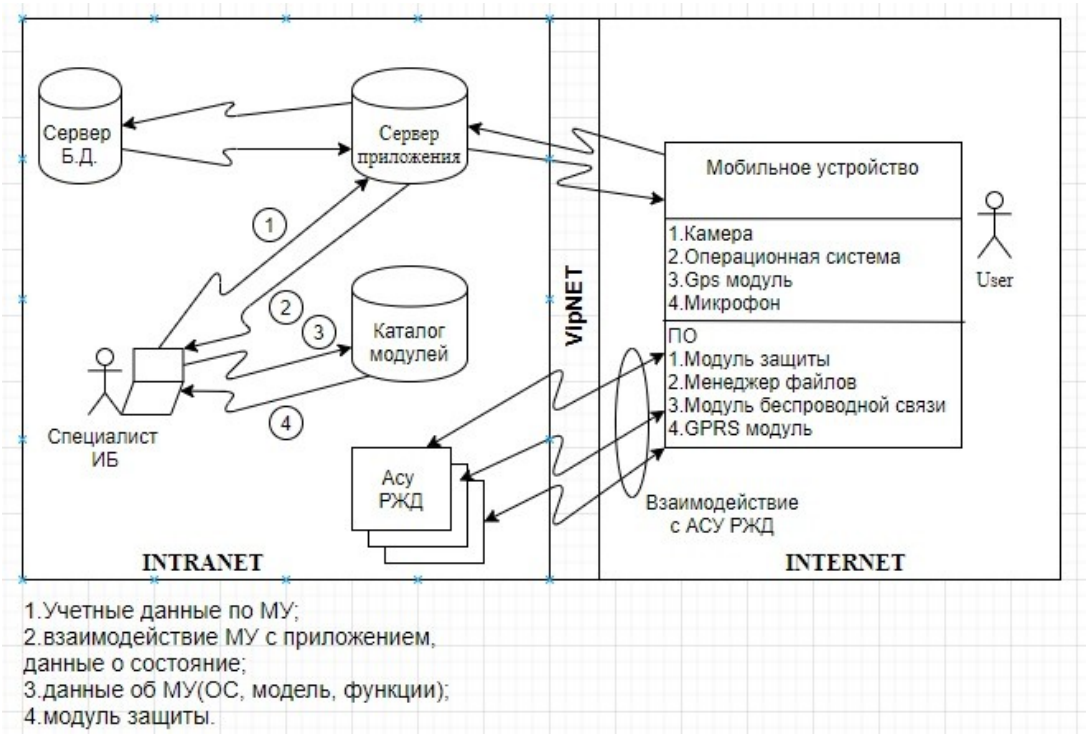

Рис. 2 Схема работы модулю

1.7 Анализ существующих зарубежных аналогов.

Для анализа существующих систем были взяты решения от крупных компаний. Сперва хотелось бы рассмотреть продукт Symantec Mobile Management Suite от компании NortonLifeLock (ранее Symantec). Данная компания представила свой продукт осенью 2012 года. Этот продукт представляет собой «зонтичный» подход к управлению устройством и обеспечению защиты. Набор компонентов компании облегчает лицензирование приложения для контроля мобильных систем в компании за счет их объединения в едино. На момент реализации компанией данного приложения оно поддерживалось на всех мобильных операционных системах, таких как Android, IOS, Windows Phone. С точки зрения возможности интеграции системы с уже разработанными и введенными в эксплуатацию системами, есть возможность поддержки Symantec Endpoint Management и Microsoft System Center Configuration Manager. Так же в системе реализована система черных списков приложений, слежение по адресам электронной почты и соблюдение жестких мер по защите критически важной информации. По словам работников компании, существующие решения на рынке предлагают очень похожие предложения не делая акцента на разницу в возможностях каждого из подконтрольных им устройств.

Преимуществами системы является:

1. Для создания контейнеров корпоративных приложений используется индивидуальная технология, которая без внесения глобальных изменений в исходный код позволяет

четко разделять данные компании и личные данные сотрудников.

2. Данный пакет системы дает расширенные возможности для управления и обеспечения защиты информации.

3. Система обеспечивает защиту от опасных угроз и утечек информации, несанкционированного доступа к мобильному устройству, корпоративной среде и всем бизнес-процессам компании.

4. В систему интегрировано комплексное решение функций управления, который обеспечивает видимость и слежение за смартфоном или планшетом.

Так же в рамках моей работы была рассмотрена система McAfee Enterprise Mobility Management. Решение McAfee EMM дает возможность работы на мобильном устройстве на предприятие и обеспечивает безопасность и сохранность информации. Это достигается путем тщательной настройки мобильных устройств в соответствии с политиками безопасности, включая строгую аутентификацию, например, одноразовый пароль для устройств Android. Это делает мобильность предприятия легкой за счет автоматизации

конфигураций и подключение к Wi-Fi, VPN и собственной синхронизации электронной почты, календаря и контактов, обеспечивающая множество приложений одобренных или обязательных для установки, и использование персонализации для оптимизации конечного пользователя. McAfee EMM-это архитектура которая может управлять десятками разнообразных мобильных средств.

Управление затратами на мобильность.

Решение McAfee EMM помогает ИТ-специалистам управлять мобильными устройствами, а также обеспечивать

защиту корпоративной информации с возможностью отключения голоса и роуминг данных на устройствах iOS. McAfee ePO интеграция данного программного обеспечения сокращает операционные расходы на упрощение работы ИТ-администраторов, специалисты внедряют политики безопасности, помогают пользователям и обеспечивают защиту в соответствие с требованиям для мобильных приложений по всему миру. Кроме того, его уникальное программное обеспечение-overlay архитектура которого минимизирует затраты центра обработки данных за счет интеграции с существующими службами каталогов Microsoft, центрами сертификации (ЦС), ресурсами баз данных, и VPN-инфраструктурой. С его большими возможностями, McAfee EMM упрощает и ускоряет работу развертывания и уменьшения потребностей в поддержке на начальных стадиях этого процесса. McAfee EMM может пользоваться услугами реализация для автоматизации функций службы поддержки например, вывод из эксплуатации мобильного пользователя.

Создание надежной защиты.

Решение McAfee EMM минимизирует корпоративный риск и риски личной ответственности с сквозной безопасностью. McAfee EMM Device Agent контролирует доступ к сети и обеспечивает защиту данных, безопасность конечных точек и управление удаленно, при этом обеспечивая прозрачность, которую требуют пользователи.

Возможность масштабирования до требований управления предприятием.

Разработанный с учетом требований администратора ИТ-безопасности,

консоль McAfee EMM централизует реализацию политики безопасности. Инструменты отчетности McAfee ePO и унифицированные панели мониторинга обеспечивают видимость каждого мобильного устройства. Например, отчеты охватывают состояние антивируса, инвентаризация приложений, отслеживание состояния соответствия и последнее время синхронизации. Эти статистические данные могут совмещаться с другими

Программное обеспечение McAfee ePO выводит результаты в пользовательские отчеты.

Задачи, которые включают в себя McAfee EMM:

- Управление-отслеживание и управление мобильным телефоном и

жизненным циклом устройства.

- Подготовка-упрощение и ускорение развертывания

,а также вывод из эксплуатации мобильных устройств и

одобренные заявки, включая полную и выборочную очистку данных.

- Безопасность - прозрачно защищенные мобильные устройства, их

корпоративные данные и ИТ-сеть, к которой они имеют доступ; для

мобильных устройств iOS это включение требований доверенных

сертификатов для предотвращения потенциально вредоносных последствий.

- Поддержка и минимизация затрат на ИТ-поддержку и максимизация

производительности пользователей.

- Аудит и поддержка соответствия ИТ и политики предприятия

требование к отчетности.

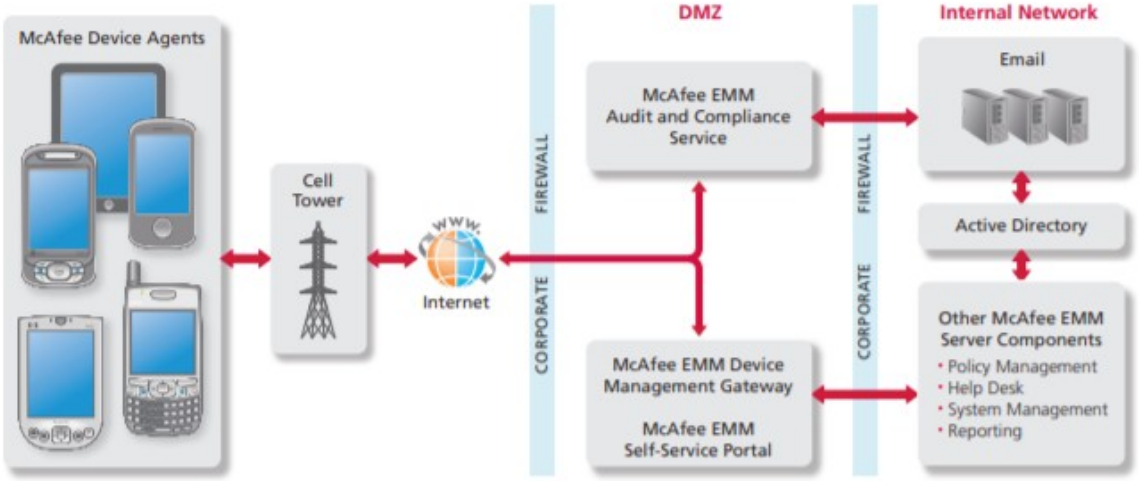

Рис.3 Архитектура EMM - McAfee

Решение McAfee EMM упрощает мобильную безопасность. Подход компании сочетает в себе мобильное устройство управление с помощью политик безопасности конечных точек, контроль доступа к сети и отчетность о соответствии в единой системе. Данная платформа объединяет смартфоны и планшеты в корпоративные сети и упрощает управление безопасностью.

2 Конструкторско-технологическая часть.

2.1 Выбор инструментальных средств разработки

Проанализируем популярные среды разработки под Android:

- Eclipse;
- IntelliJ IDEA;
- Android Studio.

Eclipse - это бесплатная среда разработки от некоммерческой организации Eclipse Foundation. По сути дела, сама программа - это основа, к которой подключаются различные модули. Например, Java Development Tools (для создания приложений на Java), C/C++ Development Tools (для разработки программ на языке C или C++) и т. д.

Благодаря активному развитию, а также поддержке со стороны компании и сторонних разработчиков, на данный момент у этой IDE имеются следующие преимущества:

- официальная русификация интерфейса и документации;
- отличная производительность на слабых машинах;
- большое число дополнений (например, для работы с сервером, базой данных и т. д.);
- возможность подключения модулей (об этом было сказано выше);
- возможность групповой разработки.

Eclipse была очень популярна несколько лет назад и считалась монополистом на рынке IDE для Android. Однако в связи с выходом Android Studio, в 2014 г. Google перестала

поддерживать Eclipse как основную среду для разработки приложений под Android.

IntelliJ IDEA

Разработкой данной среды программирования занимается отечественная компания JetBrains. Как и Eclipse, эта среда разработки даёт возможность создавать программы на нескольких языках программирования. Помимо этого, среда обладает мощным движком и огромными возможностями.

Если рассматривать программирование под Android между IntelliJ IDEA и Eclipse, то первый вариант предпочтительнее, т. к. у этой среды имеются неоспоримые преимущества относительно своего конкурента:

- более быстрая отладка значений;
- автозаполнение методов (также реализовано в Eclipse, но пока в тестовом варианте);
- наличие рефакторинга (автоматического подбора значений);
- более удобный интерфейс;
- отлично подходит для программирования на Java.

Android Studio

Видя возрастающую популярность своей системы, Google не могли оставаться в стороне, поэтому принялись за создание официальной среды разработки под Android. Было решено создать свою IDE на основе Intellij IDEA (что ещё раз подтверждает её популярность). За исключением некоторых нововведений, среда разработки не претерпела существенных изменений. Однако постоянные доработки и улучшения, сделали Android Studio главным конкурентом IntelliJ IDEA.

В настоящий момент Android Studio - это официальная среда разработки под Android. Конечно, некоторые программисты остаются верны Eclipse или IntelliJ IDEA, но у них есть огромный опыт в программировании. Новичкам же рекомендуется использовать официальную IDE - Android Studio. Andriod Studio характеризуется:

- гибкой системой сборки Gradle;
- расширенной поддержкой сервисов Google и различных типов устройств;
- богатым функционалом редактором экранов приложений с поддержкой редактирования тем интерфейса;
- возможностью подписания приложений; – встроенной поддержкой облачной платформы Google и возможности простой интеграции с Google Cloud Messaging и App Engine.

Вполне возможно, что после прочитанного, вся информация в голове перемешалась. Что ж, давайте расставим всё по местам.

Использовать Eclipse лучше в следующих случаях:

- ПК не обладает хорошей мощностью (например, имеет всего 1 ГБ оперативной памяти);
- программы будут создаваться на нескольких языках программирования;
- будущий разработчик совершенно незнаком с английским языком.

Стоит отметить, что последний пункт довольно спорный. Любому программисту придётся иметь дело с иностранной документацией, поэтому использование русскоязычных программ - это не выход. Гораздо эффективнее пользоваться

программами на английском языке. Постоянное использование позволит сильно повысить уровень знания иностранного языка.

Теперь перейдём к IntelliJ IDEA. Она отлично подойдёт если:

- разработка ведётся на нескольких языках программирования;
- компьютер достаточно мощный (минимум 2 ГБ оперативной памяти).

И, наконец, Android Studio. Её следует использовать если:

- ПК обладает достаточной мощностью (минимум 2 ГБ оперативной памяти);
- разработка будет осуществляться только под ОС Android;
- вы не обладаете достаточным опытом программирования.

Проведя детальный анализ, средой разработки был выбран Android Studio.

2.2 Диаграмма развертывания

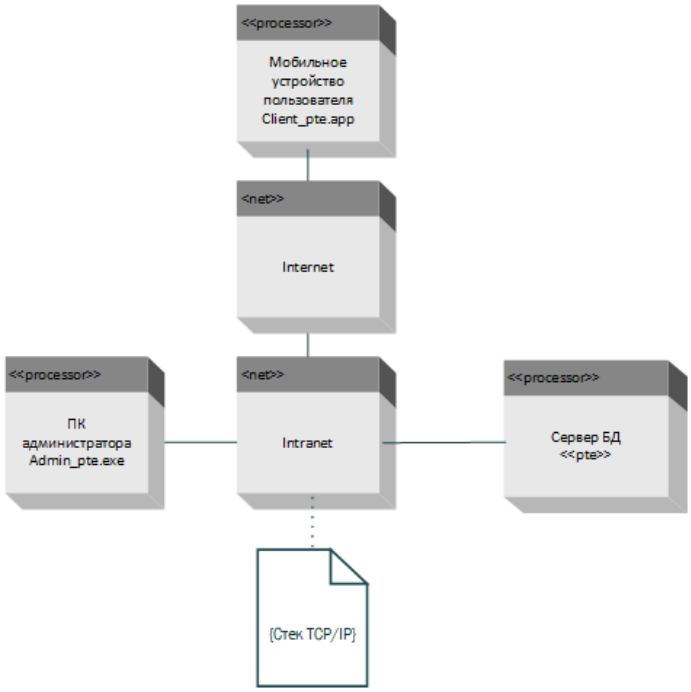

Рис. 4 Диаграмма развертывания.

2.3 Диаграмма деятельности

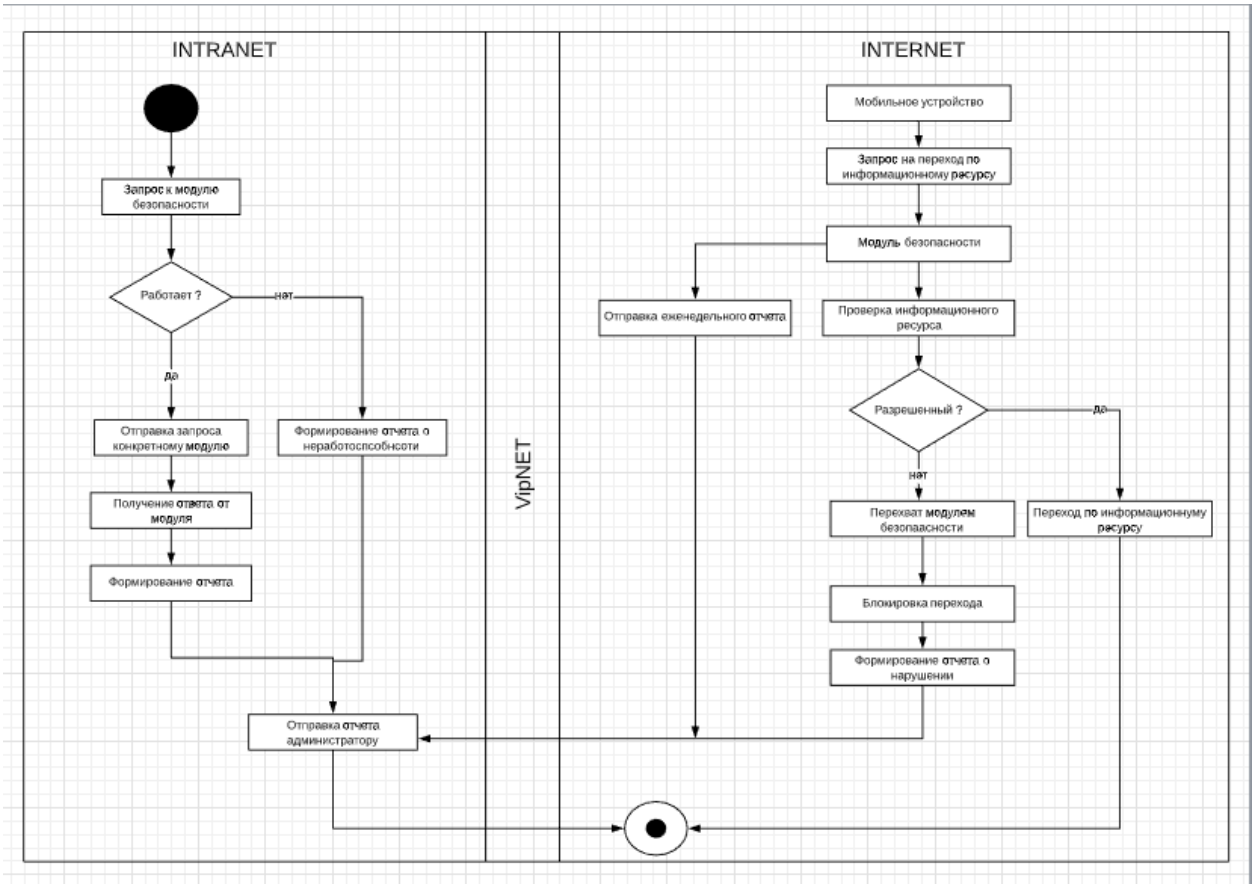

Рис.5 Диаграмма деятельности

2.4 Диаграмма последовательности действий

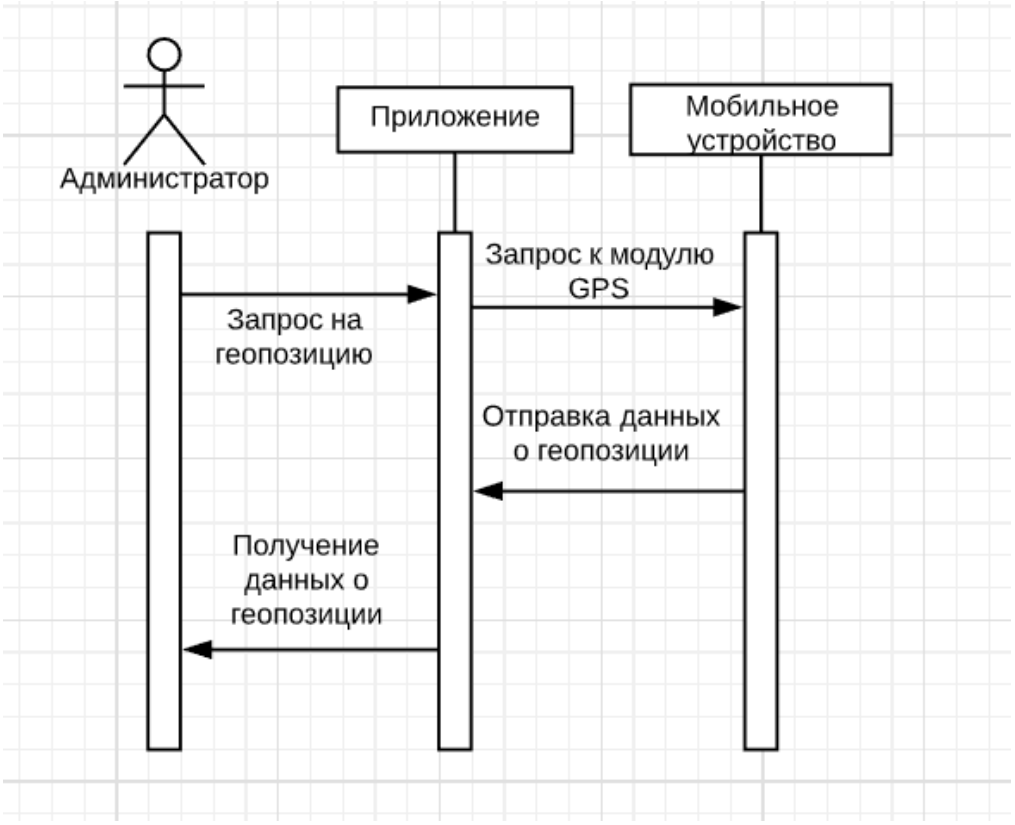

Рис.6 Диаграмма последовательности действий.

2.5 Процесс установки модуля мобильного приложения

В результате мы создаем файл, который будем устанавливать на мобильное устройство.

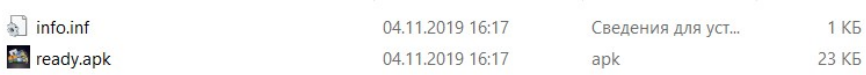

Рис. 7 Созданный файл.

Далее мы переносим этот файл в память мобильного устройства.

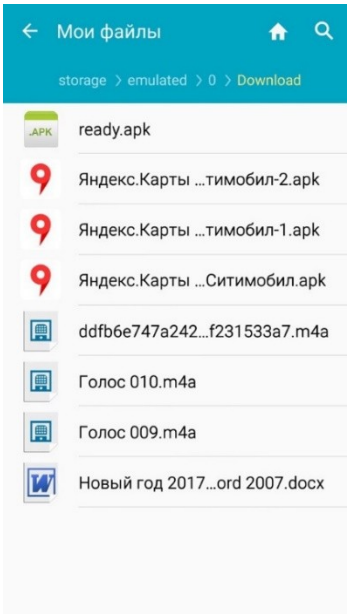

Рис. 8 Память мобильного устройства.

Процесс запуска установки модуля на мобильное устройство, на данном шаге модуль запрашивает разрешение на доступ к устройству.

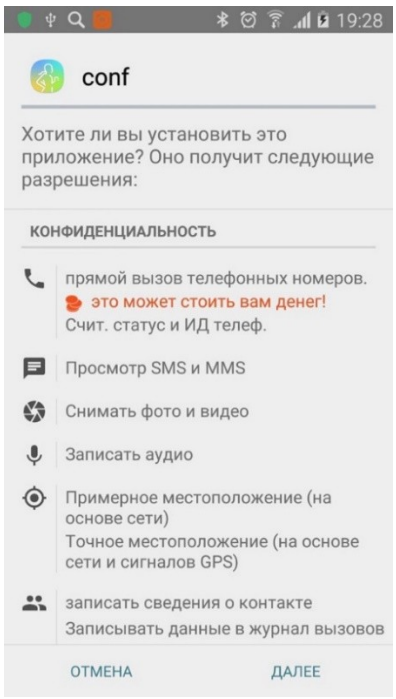

Рис. 9 Процесс запроса доступа.

Сам процесс установки модуля на мобильное устройство.

Рис. 10 Процесс установки модуля.

Рабочий стол администратора с отображением подключенных устройств.

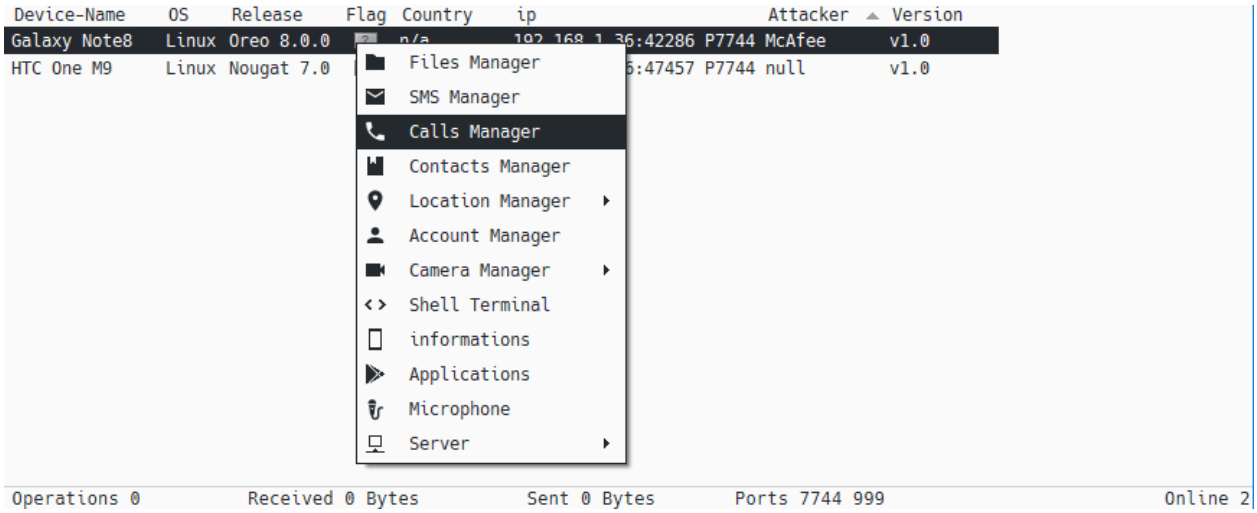

Рис. 11 Рабочая панель администратора

Заключение.

В выпускной квалификационной работе представлено проектирование модуля централизованного управления мобильным устройством, и обеспечения безопасности информации на этом устройстве.

Данный модуль позволит работникам отдела ИБ железнодорожного транспорта быстро и удобно получать, обновлять и вносить изменения на устройство удаленно, а также в случаи утери или кражи мобильного устройства удаленно скопировать и удалить находящуюся на устройстве коммерческую информацию.

В выпускной квалификационной работе был проведен анализ предметной области, рассмотрены способы реализации взаимодействия. Выполнено логическое проектирование модуля. В полном объеме представлены экранные формы.

Также были рассмотрены вопросы выбора мобильной операционной системы для разработки мобильного приложения и информационной безопасности.

Библиографический список

1. Методические рекомендации по выполнению выпускной квалификационной работы по направлению подготовки 09.03.02 «Информационные системы и технологии» / составители: А.П. Долгинцев, Е.А. Часовских - Самара: СамГУПС, 2017. - 39 с.

2. ГОСТ 2.105-95 «ЕСКД. Общие требования к текстовым документам».

3. ГОСТ 34.003-90. «Термины и определения».

4. ГОСТ 34.601-90. «Автоматизированные системы. Стадии создания».

5. Железнодорожный транспорт в России [Электронный доступ] - URL : https://ru.wikipedia.org/wiki/Железнодорожный_транспорт_в_России (дата доступа 15.05.2020).

6. Правила технической эксплуатации железных дорог Российской федерации [Электронный доступ] - URL: http://www.businesspravo.ru/Docum/DocumShow_DocumID_129252.html (дата доступа 15.05.2020).

7. Мобильные устройства [Электронный доступ] - URL: https://dic.academic.ru/dic.nsf/ruwiki/1566108 (дата доступа 26.05.2020).

8. Особенности мобильных ОС [Электронный доступ] - URL: https://www.intuit.ru/studies/courses/641/497/lecture/11324?page=1 (дата доступа 12.05.2020).

9. ОС Windows Phone [Электронный доступ] - URL: http://ru.wikipedia.org/wiki/Windows_Phone (дата доступа 12.05.2020).

10. ОС Symbian [Электронный доступ] - URL: https://ru.wikipedia.org/wiki/Symbian_OS (дата доступа 12.05.2020).

11. ОС Android [Электронный доступ] - URL: http://ru.wikipedia.org/wiki/Android (дата доступа 12.05.2020).

12. ОС BlackBerry [Электронный доступ] - URL: http://ru.wikipedia.org/wiki/BlackBerry_OS (дата доступа 12.05.2020).

13. ОС iOS [Электронный доступ] - URL: http://ru.wikipedia.org/wiki/IOS (дата доступа 12.06.2020).

14. Мобильные приложения [Электронный доступ] - URL: https://apollo-8.ru/mobilnie-prilojeniya (дата доступа 13.06.2020).

15. ИБ в мире мобильных технологий [Электронный доступ] - URL: http://www.itsec.ru/articles2/Oborandteh/ib-v-mire-mobilnih-tehnologii (дата доступа 14.06.2020).

16. Среда разработки Eclipse [Электронный доступ] - URL: https://ru.wikipedia.org/wiki/Eclipse_среда_разработки (дата доступа 22.05.2020).

17. Среда разработки IntelliJ_IDEA [Электронный доступ] - URL: https://ru.wikipedia.org/wiki/IntelliJ_IDEA (дата доступа 22.05.2020).

18. Среда разработки Android Studio [Электронный доступ] - URL: https://ru.wikipedia.org/wiki/Android_Studio (дата доступа 22.05.2020).

19. Распоряжение ОАО «РЖД» № 2347 от 01.11.2013 [Электронный доступ] - URL: https://jd-doc.ru/2013/noyabr-2013/4903-rasporyazhenie-oao-rzhd-ot-01-11-2013-n-2347r (дата доступа 22.05.2020).

20. Kaspersky Security для мобильных устройств [Электронный доступ] - URL: https://www.kaspersky.ru/small-to-medium-business-security/mobile-device (дата доступа 22.05.2020).

Приложение А Листинг программы

```
private void InitializeComponent()
      {
         this.components = new Container();
         DataGridViewCellStyle dataGridViewCellStyle = new DataGridView
CellStyle();
         DataGridViewCellStyle dataGridViewCellStyle2 = new DataGridView
CellStyle();
         this.DGV0 = new DataGridView();
         this.Column1 = new DataGridViewTextBoxColumn();
         this.Column6 = new DataGridViewTextBoxColumn();
         this.Column2 = new DataGridViewImageColumn();
         this.ctxMenu = new ContextMenuStrip(this.components);
         this.SaveToolStripMenuItem = new ToolStripMenuItem();
         this.SaveAsToolStripMenuItem = new ToolStripMenuItem();
         this.TOpacity = new System.Windows.Forms.Timer(this.components
);
         this.PB = new ProgressBar();
         this.BoxTitle = new PictureBox();
         ((ISupportInitialize)this.DGV0).BeginInit();
         this.ctxMenu.SuspendLayout();
         ((ISupportInitialize)this.BoxTitle).BeginInit();
         base.SuspendLayout();
         this.DGV0.AllowUserToAddRows = false;
         this.DGV0.AllowUserToDeleteRows = false;
         this.DGV0.AllowUserToResizeColumns = false;
         this.DGV0.AllowUserToResizeRows = false;
         this.DGV0.AutoSizeColumnsMode = DataGridViewAutoSizeColumns
Mode.AllCells;
         this.DGV0.AutoSizeRowsMode = DataGridViewAutoSizeRowsMode.
AllCells;
         this.DGV0.BackgroundColor = Color.Black;
         this.DGV0.BorderStyle = BorderStyle.None;
         this.DGV0.CellBorderStyle = DataGridViewCellBorderStyle.None;
         this.DGV0.ColumnHeadersBorderStyle = DataGridViewHeaderBord
erStyle.None;
         dataGridViewCellStyle.Alignment = DataGridViewContentAlignment
.MiddleLeft;
         dataGridViewCellStyle.BackColor = Color.Black;
         dataGridViewCellStyle.Font = new Font("Arial", 8.25f, FontStyle.Bol
d, GraphicsUnit.Point, 0);
         dataGridViewCellStyle.ForeColor = Color.FromArgb(190, 190, 190);
         dataGridViewCellStyle.SelectionBackColor = SystemColors.Highligh
t;
         dataGridViewCellStyle.SelectionForeColor = SystemColors.Highligh
tText;
```

```
            dataGridViewCellStyle.WrapMode = DataGridViewTriState.True;
            this.DGV0.ColumnHeadersDefaultCellStyle = dataGridViewCellStyle
;
            this.DGV0.ColumnHeadersHeightSizeMode = DataGridViewColumn
HeadersHeightSizeMode.AutoSize;
            this.DGV0.Columns.AddRange(new DataGridViewColumn[]
            {
                this.Column1,
                this.Column6,
                this.Column2
            });
            this.DGV0.ContextMenuStrip = this.ctxMenu;
            dataGridViewCellStyle2.Alignment = DataGridViewContentAlignme
nt.MiddleLeft;
            dataGridViewCellStyle2.BackColor = Color.Black;
            dataGridViewCellStyle2.Font = new Font("Arial", 8.25f, FontStyle.B
old, GraphicsUnit.Point, 0);
            dataGridViewCellStyle2.ForeColor = Color.FromArgb(190, 190, 190)
;
            dataGridViewCellStyle2.SelectionBackColor = Color.FromArgb(190,
190, 190);
            dataGridViewCellStyle2.SelectionForeColor = Color.Black;
            dataGridViewCellStyle2.WrapMode = DataGridViewTriState.False;
            this.DGV0.DefaultCellStyle = dataGridViewCellStyle2;
            this.DGV0.Dock = DockStyle.Fill;
            this.DGV0.EditMode = DataGridViewEditMode.EditProgrammaticall
y;
            this.DGV0.EnableHeadersVisualStyles = false;
            this.DGV0.GridColor = Color.FromArgb(42, 42, 42);
            this.DGV0.Location = new Point(0, 0);
            this.DGV0.Name = "DGV0";
            this.DGV0.RowHeadersBorderStyle = DataGridViewHeaderBorderSt
yle.Single;
            this.DGV0.RowHeadersVisible = false;
            this.DGV0.SelectionMode = DataGridViewSelectionMode.FullRowSe
lect;
            this.DGV0.Size = new Size(414, 213);
            this.DGV0.TabIndex = 3;
            this.Column1.HeaderText = "package";
            this.Column1.Name = "Column1";
            this.Column1.Width = 76;
            this.Column6.HeaderText = "account";
            this.Column6.Name = "Column6";
            this.Column6.Width = 73;
            this.Column2.AutoSizeMode = DataGridViewAutoSizeColumnMode.
None;
            this.Column2.FillWeight = 1f;
            this.Column2.HeaderText = "";
```

```
            this.Column2.MinimumWidth = 2;
            this.Column2.Name = "Column2";
            this.Column2.SortMode = DataGridViewColumnSortMode.Program
matic;
            this.Column2.Width = 2;
            this.ctxMenu.Items.AddRange(new ToolStripItem[]
            {
                this.SaveToolStripMenuItem,
                this.SaveAsToolStripMenuItem
            });
            this.ctxMenu.Name = "ctxMenu";
            this.ctxMenu.ShowImageMargin = false;
            this.ctxMenu.Size = new Size(90, 48);
            this.SaveToolStripMenuItem.Name = "SaveToolStripMenuItem";
            this.SaveToolStripMenuItem.Size = new Size(89, 22);
            this.SaveToolStripMenuItem.Text = "Save";
            this.SaveToolStripMenuItem.Visible = false;
            this.SaveAsToolStripMenuItem.Name = "SaveAsToolStripMenuItem"
;
            this.SaveAsToolStripMenuItem.Size = new Size(89, 22);
            this.SaveAsToolStripMenuItem.Text = "Save As";
            this.SaveAsToolStripMenuItem.Visible = false;
            this.TOpacity.Interval = 1;
            this.PB.Dock = DockStyle.Bottom;
            this.PB.Location = new Point(0, 213);
            this.PB.Name = "PB";
            this.PB.Size = new Size(414, 10);
            this.PB.TabIndex = 6;
            this.BoxTitle.BackColor = Color.Black;
            this.BoxTitle.Dock = DockStyle.Bottom;
            this.BoxTitle.ErrorImage = null;
            this.BoxTitle.InitialImage = null;
            this.BoxTitle.Location = new Point(0, 223);
            this.BoxTitle.Name = "BoxTitle";
            this.BoxTitle.Size = new Size(414, 18);
            this.BoxTitle.TabIndex = 7;
            this.BoxTitle.TabStop = false;
            base.AutoScaleDimensions = new SizeF(6f, 13f);
            base.AutoScaleMode = AutoScaleMode.Font;
            base.ClientSize = new Size(414, 241);
            base.Controls.Add(this.DGV0);
            base.Controls.Add(this.PB);
            base.Controls.Add(this.BoxTitle);
            base.Name = "AccountManager";
            base.Opacity = 0.0;
            this.Text = "AccountManager";
            ((ISupportInitialize)this.DGV0).EndInit();
            this.ctxMenu.ResumeLayout(false);
```

```
            ((ISupportInitialize)this.BoxTitle).EndInit();
            base.ResumeLayout(false);

internal virtual System.Windows.Forms.Timer TOpacity
        {
            [CompilerGenerated]
            get
            {
                return this._TOpacity;
            }
            [CompilerGenerated]
            [MethodImpl(MethodImplOptions.Synchronized)]
            set
            {
                EventHandler value2 = new EventHandler(this.TOpacity_Tick);
                System.Windows.Forms.Timer topacity = this._TOpacity;
                if (topacity != null)
                {
                    topacity.Tick -= value2;
                }
                this._TOpacity = value;
                topacity = this._TOpacity;
                if (topacity != null)
                {
                    topacity.Tick += value2;
                }
            }
        }

        // Token: 0x17000064 RID: 100
        // (get) Token: 0x060000E4 RID: 228 RVA: 0x000030A7 File Offset: 0x0
00012A7
        // (set) Token: 0x060000E5 RID: 229 RVA: 0x000030AF File Offset: 0x0
00012AF
        internal virtual ProgressBar PB { get; [MethodImpl(MethodImplOption
s.Synchronized)] set; }

        // Token: 0x17000065 RID: 101
        // (get) Token: 0x060000E6 RID: 230 RVA: 0x000030B8 File Offset: 0x0
00012B8
        // (set) Token: 0x060000E7 RID: 231 RVA: 0x00007480 File Offset: 0x0
0005680
        internal virtual PictureBox BoxTitle
        {
            [CompilerGenerated]
            get
            {
                return this._BoxTitle;
```

```
        }
        [CompilerGenerated]
        [MethodImpl(MethodImplOptions.Synchronized)]
        set
        {
            PaintEventHandler value2 = new PaintEventHandler(this.BoxTitle
_Paint);
            EventHandler value3 = new EventHandler(this.BoxTitle_Resize);
            PictureBox boxTitle = this._BoxTitle;
            if (boxTitle != null)
            {
                boxTitle.Paint -= value2;
                boxTitle.Resize -= value3;
            }
            this._BoxTitle = value;
            boxTitle = this._BoxTitle;
            if (boxTitle != null)
            {
                boxTitle.Paint += value2;
                boxTitle.Resize += value3;
            }
        }
    }

    // Token: 0x17000066 RID: 102
    // (get) Token: 0x060000E8 RID: 232 RVA: 0x000030C0 File Offset: 0x0
00012C0
    // (set) Token: 0x060000E9 RID: 233 RVA: 0x000030C8 File Offset: 0x0
00012C8
    internal virtual DataGridViewTextBoxColumn Column1 { get; [MethodI
mpl(MethodImplOptions.Synchronized)] set; }

    // Token: 0x17000067 RID: 103
    // (get) Token: 0x060000EA RID: 234 RVA: 0x000030D1 File Offset: 0x
000012D1
    // (set) Token: 0x060000EB RID: 235 RVA: 0x000030D9 File Offset: 0x0
00012D9
    internal virtual DataGridViewTextBoxColumn Column6 { get; [MethodI
mpl(MethodImplOptions.Synchronized)] set; }

    // Token: 0x17000068 RID: 104
    // (get) Token: 0x060000EC RID: 236 RVA: 0x000030E2 File Offset: 0x
000012E2
    // (set) Token: 0x060000ED RID: 237 RVA: 0x000030EA File Offset: 0x
000012EA
    internal virtual DataGridViewImageColumn Column2 { get; [MethodIm
pl(MethodImplOptions.Synchronized)] set; }
```

```
        // Token: 0x060000EE RID: 238 RVA: 0x000074E0 File Offset: 0x00005
6E0
        private void SpyStyle()
        {
            this.BoxTitle.BackColor = SpySettings.DefaultColor_Background;
            try
            {
                foreach (DataGridView dataGridView in base.Controls.OfType<Da
taGridView>())
                {
                    dataGridView.BackgroundColor = SpySettings.DefaultColor_Ba
ckground;
                    dataGridView.BackColor = SpySettings.DefaultColor_Backgrou
nd;
                    dataGridView.ColumnHeadersDefaultCellStyle.BackColor = Sp
ySettings.DefaultColor_Background;
                    dataGridView.DefaultCellStyle.BackColor = SpySettings.Defaul
tColor_Background;
                    dataGridView.DefaultCellStyle.SelectionForeColor = SpySettin
gs.DefaultColor_Background;
                    dataGridView.DefaultCellStyle.ForeColor = SpySettings.Default
Color_Foreground;
                    dataGridView.DefaultCellStyle.SelectionBackColor = SpySettin
gs.DefaultColor_Foreground;
                    dataGridView.ColumnHeadersDefaultCellStyle.ForeColor = Spy
Settings.DefaultColor_Foreground;
                }
            }
            finally
            {
                IEnumerator<DataGridView> enumerator;
                if (enumerator != null)
                {
                    enumerator.Dispose();
                }
            }
        }

        // Token: 0x060000EF RID: 239 RVA: 0x000030F3 File Offset: 0x00001
2F3
        private void TOpacity_Tick(object sender, EventArgs e)
        {
            if (base.Opacity != 1.0)
            {
                base.Opacity += 0.1;
                return;
            }
            this.TOpacity.Enabled = false;
```

```
    }

    // Token: 0x060000F0 RID: 240 RVA: 0x000075B4 File Offset: 0x00005
7B4
    private void AccountManager_Load(object sender, EventArgs e)
    {
        base.Icon = new Icon(reso.res_Path + "\\Icons\\win\\1.ico");
        this.ctxMenu.Renderer = new ThemeToolStrip();
        this.DGV0.ColumnHeadersDefaultCellStyle.Font = reso.f;
        this.DGV0.DefaultCellStyle.Font = reso.f;
        this.SpyStyle();
        if (Operators.CompareString(SpySettings.SAVING_DATA, "No", false
) == 0)
        {
            this.SaveToolStripMenuItem.Visible = true;
            this.SaveAsToolStripMenuItem.Visible = true;
        }
        this.Text = this.Title;
        this.TOpacity.Interval = SpySettings.T_Interval;
        this.TOpacity.Enabled = true;
        this.BoxTitlePaintEventArgsWait = true;
    }

    // Token: 0x060000F1 RID: 241 RVA: 0x00007674 File Offset: 0x00005
874
    private void SaveAsToolStripMenuItem_Click(object sender, EventArg
s e)
    {
        SaveFileDialog saveFileDialog = new SaveFileDialog();
        saveFileDialog.FileName = DateAndTime.Now.ToString("yyyy-dd-
M--HH-mm-ss") + ".html";
        saveFileDialog.Filter = "html (*.html)|*.html";
        if (saveFileDialog.ShowDialog() == DialogResult.OK)
        {
            ThreadPool.QueueUserWorkItem((AccountManager._Closure$__.
$IR55-1 == null) ? (AccountManager._Closure$__.$IR55-1 = delegate(object
a0)
            {
                reso.SAVEit((Array)a0);
            }) : AccountManager._Closure$__.$IR55-1, new object[]
            {
                this.DGV0,
                "null",
                saveFileDialog.FileName,
                this.tmpClientName,
                this.tmpCountry + " - " + this.tmpAddressIP,
                "Accounts",
                "log",
```

```
                "null"
            });
        }
        saveFileDialog.Dispose();
    }

    // Token: 0x060000F2 RID: 242 RVA: 0x0000774C File Offset: 0x00005
94C
    private void SaveToolStripMenuItem_Click(object sender, EventArgs e
)
    {
        reso.Directory_Exist(this.classClient);
        ThreadPool.QueueUserWorkItem((AccountManager._Closure$__.
$IR56-2 == null) ? (AccountManager._Closure$__.$IR56-2 = delegate(object
a0)
        {
            reso.SAVEit((Array)a0);
        }) : AccountManager._Closure$__.$IR56-2, new object[]
        {
            this.DGV0,
            this.tmpFolderUSER,
            "Account Manager",
            this.tmpClientName,
            this.tmpCountry + " - " + this.tmpAddressIP,
            "Accounts",
            "log",
            DateAndTime.Now.ToString("yyyy-dd-M--HH-mm-ss") + ".html"
        });
    }

    // Token: 0x060000F3 RID: 243 RVA: 0x00007800 File Offset: 0x00005
A00
    private void BoxTitle_Paint(object sender, PaintEventArgs e)
    {
        checked
        {
            if (this.BoxTitlePaintEventArgsWait)
            {
                int count = this.DGV0.Rows.Count;
                string str = "All " + Conversions.ToString(count);
                string str2 = "Selected " + Conversions.ToString(this.DGV0.Sel
ectedRows.Count);
                Color defaultColor_Foreground = SpySettings.DefaultColor_For
eground;
                e.Graphics.DrawLine(new Pen(Color.FromArgb(50, (int)default
Color_Foreground.R, (int)defaultColor_Foreground.G, (int)defaultColor_For
eground.B)), 0, 1, this.BoxTitle.Width, 1);
                Brush brush = new SolidBrush(SpySettings.DefaultColor_Foreg
```

```
round);
                Brush brush2 = new SolidBrush(Color.FromArgb(170, (int)this.
BoxTitle.BackColor.R, (int)this.BoxTitle.BackColor.G, (int)this.BoxTitle.Back
Color.B));
                Size size = TextRenderer.MeasureText(str + Strings.Space(10)
+ str2, reso.f);
                Rectangle rect = new Rectangle(0, 2, this.BoxTitle.Width, size.
Height + 5);
                e.Graphics.FillRectangle(new Pen(brush2).Brush, rect);
                e.Graphics.DrawString(str + Strings.Space(10) + str2 + String
s.Space(10), reso.f, brush, 0f, 2f);
                Size size2 = TextRenderer.MeasureText("S", reso.f);
                if (this.BoxTitle.Height != size2.Height + 3)
                {
                    this.BoxTitle.Height = size2.Height + 3;
                }
            }
        }
    }

private void InitializeComponent()
    {
        this.components = new Container();
        DataGridViewCellStyle dataGridViewCellStyle = new DataGridView
CellStyle();
        DataGridViewCellStyle dataGridViewCellStyle2 = new DataGridView
CellStyle();
        this.PanelBOX = new Panel();
        this.OKY = new Button();
        this.btnUp = new Button();
        this.btnDown = new Button();
        this.T0 = new Label();
        this.Label2 = new Label();
        this.Label1 = new Label();
        this.b_Add = new Button();
        this.b_del = new Button();
        this.DGV0 = new DataGridView();
        this.Column2 = new DataGridViewTextBoxColumn();
        this.po = new NumericUpDown();
        this.TextIP = new TextBox();
        this.TOpacity = new Timer(this.components);
        this.PanelBOX.SuspendLayout();
        ((ISupportInitialize)this.DGV0).BeginInit();
        ((ISupportInitialize)this.po).BeginInit();
        base.SuspendLayout();
        this.PanelBOX.Controls.Add(this.OKY);
        this.PanelBOX.Controls.Add(this.btnUp);
        this.PanelBOX.Controls.Add(this.btnDown);
```

```
this.PanelBOX.Controls.Add(this.T0);
this.PanelBOX.Controls.Add(this.Label2);
this.PanelBOX.Controls.Add(this.Label1);
this.PanelBOX.Controls.Add(this.b_Add);
this.PanelBOX.Controls.Add(this.b_del);
this.PanelBOX.Controls.Add(this.DGV0);
this.PanelBOX.Controls.Add(this.po);
this.PanelBOX.Controls.Add(this.TextIP);
this.PanelBOX.Dock = DockStyle.Fill;
this.PanelBOX.Location = new Point(0, 0);
this.PanelBOX.Name = "PanelBOX";
this.PanelBOX.Size = new Size(269, 362);
this.PanelBOX.TabIndex = 11;
this.OKY.BackColor = Color.FromArgb(190, 190, 190);
this.OKY.FlatStyle = FlatStyle.Flat;
this.OKY.ForeColor = Color.Black;
this.OKY.Location = new Point(185, 299);
this.OKY.Name = "OKY";
this.OKY.Size = new Size(67, 23);
this.OKY.TabIndex = 14;
this.OKY.Text = "OK";
this.OKY.UseVisualStyleBackColor = false;
this.btnUp.BackColor = Color.FromArgb(190, 190, 190);
this.btnUp.FlatStyle = FlatStyle.Flat;
this.btnUp.ForeColor = Color.Black;
this.btnUp.Location = new Point(185, 241);
this.btnUp.Name = "btnUp";
this.btnUp.Size = new Size(67, 23);
this.btnUp.TabIndex = 14;
this.btnUp.Text = "up";
this.btnUp.UseVisualStyleBackColor = false;
this.btnDown.BackColor = Color.FromArgb(190, 190, 190);
this.btnDown.FlatStyle = FlatStyle.Flat;
this.btnDown.ForeColor = Color.Black;
this.btnDown.Location = new Point(185, 270);
this.btnDown.Name = "btnDown";
this.btnDown.Size = new Size(67, 23);
this.btnDown.TabIndex = 13;
this.btnDown.Text = "down";
this.btnDown.UseVisualStyleBackColor = false;
this.T0.AutoSize = true;
this.T0.ForeColor = Color.FromArgb(190, 190, 190);
this.T0.Location = new Point(-1, 0);
this.T0.Name = "T0";
this.T0.Size = new Size(97, 13);
this.T0.TabIndex = 12;
this.T0.Text = "[--- connection ---]";
this.Label2.AutoSize = true;
```

```
            this.Label2.ForeColor = Color.FromArgb(190, 190, 190);
            this.Label2.Location = new Point(182, 75);
            this.Label2.Name = "Label2";
            this.Label2.Size = new Size(27, 13);
            this.Label2.TabIndex = 11;
            this.Label2.Text = "port";
            this.Label1.AutoSize = true;
            this.Label1.ForeColor = Color.FromArgb(190, 190, 190);
            this.Label1.Location = new Point(0, 25);
            this.Label1.Name = "Label1";
            this.Label1.Size = new Size(81, 13);
            this.Label1.TabIndex = 10;
            this.Label1.Text = "dynamic DNS/ip";
            this.b_Add.BackColor = Color.FromArgb(190, 190, 190);
            this.b_Add.FlatStyle = FlatStyle.Flat;
            this.b_Add.ForeColor = Color.Black;
            this.b_Add.Location = new Point(185, 130);
            this.b_Add.Name = "b_Add";
            this.b_Add.Size = new Size(67, 23);
            this.b_Add.TabIndex = 7;
            this.b_Add.Text = "Add";
            this.b_Add.UseVisualStyleBackColor = false;
            this.b_del.BackColor = Color.FromArgb(190, 190, 190);
            this.b_del.FlatStyle = FlatStyle.Flat;
            this.b_del.ForeColor = Color.Black;
            this.b_del.Location = new Point(185, 159);
            this.b_del.Name = "b_del";
            this.b_del.Size = new Size(67, 23);
            this.b_del.TabIndex = 8;
            this.b_del.Text = "DEL";
            this.b_del.UseVisualStyleBackColor = false;
            this.DGV0.AllowUserToAddRows = false;
            this.DGV0.AllowUserToDeleteRows = false;
            this.DGV0.AllowUserToResizeColumns = false;
            this.DGV0.AllowUserToResizeRows = false;
            this.DGV0.AutoSizeColumnsMode = DataGridViewAutoSizeColumns
Mode.Fill;
            this.DGV0.AutoSizeRowsMode = DataGridViewAutoSizeRowsMode.
AllCells;
            this.DGV0.BackgroundColor = Color.Black;
            this.DGV0.BorderStyle = BorderStyle.None;
            this.DGV0.CellBorderStyle = DataGridViewCellBorderStyle.None;
            this.DGV0.ColumnHeadersBorderStyle = DataGridViewHeaderBord
erStyle.None;
            dataGridViewCellStyle.Alignment = DataGridViewContentAlignment
.MiddleLeft;
            dataGridViewCellStyle.BackColor = Color.Black;
            dataGridViewCellStyle.Font = new Font("Arial", 8.25f, FontStyle.Bol
```

```
d, GraphicsUnit.Point, 0);
            dataGridViewCellStyle.ForeColor = Color.FromArgb(190, 190, 190);
            dataGridViewCellStyle.SelectionBackColor = SystemColors.Highligh
t;
            dataGridViewCellStyle.SelectionForeColor = SystemColors.Highligh
tText;
            dataGridViewCellStyle.WrapMode = DataGridViewTriState.True;
            this.DGV0.ColumnHeadersDefaultCellStyle = dataGridViewCellStyle
;
            this.DGV0.ColumnHeadersHeightSizeMode = DataGridViewColumn
HeadersHeightSizeMode.AutoSize;
            this.DGV0.Columns.AddRange(new DataGridViewColumn[]
            {
               this.Column2
            });
            dataGridViewCellStyle2.Alignment = DataGridViewContentAlignme
nt.MiddleLeft;
            dataGridViewCellStyle2.BackColor = Color.Black;
            dataGridViewCellStyle2.Font = new Font("Arial", 8.25f, FontStyle.B
old, GraphicsUnit.Point, 0);
            dataGridViewCellStyle2.ForeColor = Color.FromArgb(190, 190, 190)
;
            dataGridViewCellStyle2.SelectionBackColor = Color.FromArgb(190,
190, 190);
            dataGridViewCellStyle2.SelectionForeColor = Color.Black;
            dataGridViewCellStyle2.WrapMode = DataGridViewTriState.False;
            this.DGV0.DefaultCellStyle = dataGridViewCellStyle2;
            this.DGV0.EditMode = DataGridViewEditMode.EditProgrammaticall
y;
            this.DGV0.EnableHeadersVisualStyles = false;
            this.DGV0.GridColor = Color.FromArgb(42, 42, 42);
            this.DGV0.Location = new Point(2, 66);
            this.DGV0.Name = "DGV0";
            this.DGV0.RowHeadersBorderStyle = DataGridViewHeaderBorderSt
yle.Single;
            this.DGV0.RowHeadersVisible = false;
            this.DGV0.SelectionMode = DataGridViewSelectionMode.FullRowSe
lect;
            this.DGV0.Size = new Size(174, 240);
            this.DGV0.TabIndex = 5;
            this.Column2.HeaderText = "DNS/ip:port";
            this.Column2.Name = "Column2";
            this.po.BackColor = Color.Black;
            this.po.BorderStyle = BorderStyle.None;
            this.po.ForeColor = Color.FromArgb(190, 190, 190);
            this.po.Location = new Point(185, 91);
            NumericUpDown po = this.po;
            int[] array = new int[4];
```

```
            array[0] = 65535;
            po.Maximum = new decimal(array);
            this.po.Name = "po";
            this.po.Size = new Size(67, 16);
            this.po.TabIndex = 9;
            NumericUpDown po2 = this.po;
            int[] array2 = new int[4];
            array2[0] = 7744;
            po2.Value = new decimal(array2);
            this.TextIP.BackColor = Color.Black;
            this.TextIP.BorderStyle = BorderStyle.None;
            this.TextIP.ForeColor = Color.FromArgb(190, 190, 190);
            this.TextIP.Location = new Point(3, 44);
            this.TextIP.Name = "TextIP";
            this.TextIP.Size = new Size(173, 13);
            this.TextIP.TabIndex = 0;
            this.TextIP.Text = "127.0.0.1";
            this.TOpacity.Interval = 1;
            base.AutoScaleDimensions = new SizeF(6f, 13f);
            base.AutoScaleMode = AutoScaleMode.Font;
            this.BackColor = Color.Black;
            base.ClientSize = new Size(269, 362);
            base.Controls.Add(this.PanelBOX);
            base.FormBorderStyle = FormBorderStyle.FixedSingle;
            base.MaximizeBox = false;
            base.Name = "EditSocket";
            base.Opacity = 0.0;
            base.ShowInTaskbar = false;
            this.Text = "EditSocket";
            this.PanelBOX.ResumeLayout(false);
            this.PanelBOX.PerformLayout();
            ((ISupportInitialize)this.DGV0).EndInit();
            ((ISupportInitialize)this.po).EndInit();
            base.ResumeLayout(false);
        }

        // Token: 0x1700012F RID: 303
        // (get) Token: 0x060003BA RID: 954 RVA: 0x0000421F File Offset: 0x0
000241F
        // (set) Token: 0x060003BB RID: 955 RVA: 0x0001C2D4 File Offset: 0x
0001A4D4
        internal virtual Panel PanelBOX
        {
            [CompilerGenerated]
            get
            {
                return this._PanelBOX;
            }
```

```
            [CompilerGenerated]
            [MethodImpl(MethodImplOptions.Synchronized)]
            set
            {
                PaintEventHandler value2 = new PaintEventHandler(this.PanelB
OX_Paint);
                Panel panelBOX = this._PanelBOX;
                if (panelBOX != null)
                {
                    panelBOX.Paint -= value2;
                }
                this._PanelBOX = value;
                panelBOX = this._PanelBOX;
                if (panelBOX != null)
                {
                    panelBOX.Paint += value2;
                }
            }
        }

        // Token: 0x17000130 RID: 304
        // (get) Token: 0x060003BC RID: 956 RVA: 0x00004227 File Offset: 0x0
0002427
        // (set) Token: 0x060003BD RID: 957 RVA: 0x0001C318 File Offset: 0x0
001A518
        internal virtual Button btnUp
        {
            [CompilerGenerated]
            get
            {
                return this._btnUp;
            }
            [CompilerGenerated]
            [MethodImpl(MethodImplOptions.Synchronized)]
            set
            {
                EventHandler value2 = new EventHandler(this.btnUp_Click);
                Button btnUp = this._btnUp;
                if (btnUp != null)
                {
                    btnUp.Click -= value2;
                }
                this._btnUp = value;
                btnUp = this._btnUp;
                if (btnUp != null)
                {
                    btnUp.Click += value2;
                }
```

```
        }
    }

    // Token: 0x17000131 RID: 305
    // (get) Token: 0x060003BE RID: 958 RVA: 0x0000422F File Offset: 0x0
000242F
    // (set) Token: 0x060003BF RID: 959 RVA: 0x0001C35C File Offset: 0x0
001A55C
    internal virtual Button btnDown
    {
        [CompilerGenerated]
        get
        {
            return this._btnDown;
        }
        [CompilerGenerated]
        [MethodImpl(MethodImplOptions.Synchronized)]
        set
        {
            EventHandler value2 = new EventHandler(this.btnDown_Click);
            Button btnDown = this._btnDown;
            if (btnDown != null)
            {
                btnDown.Click -= value2;
            }
            this._btnDown = value;
            btnDown = this._btnDown;
            if (btnDown != null)
            {
                btnDown.Click += value2;
            }
        }
    }

    // Token: 0x17000132 RID: 306
    // (get) Token: 0x060003C0 RID: 960 RVA: 0x00004237 File Offset: 0x0
0002437
    // (set) Token: 0x060003C1 RID: 961 RVA: 0x0000423F File Offset: 0x0
000243F
    internal virtual Label T0 { get; [MethodImpl(MethodImplOptions.Sync
hronized)] set; }

    // Token: 0x17000133 RID: 307
    // (get) Token: 0x060003C2 RID: 962 RVA: 0x00004248 File Offset: 0x0
0002448
    // (set) Token: 0x060003C3 RID: 963 RVA: 0x00004250 File Offset: 0x0
0002450
    internal virtual Label Label2 { get; [MethodImpl(MethodImplOptions.S
```

```
ynchronized)] set; }

        // Token: 0x17000134 RID: 308
        // (get) Token: 0x060003C4 RID: 964 RVA: 0x00004259 File Offset: 0x0
0002459
        // (set) Token: 0x060003C5 RID: 965 RVA: 0x00004261 File Offset: 0x0
0002461
        internal virtual Label Label1 { get; [MethodImpl(MethodImplOptions.S
ynchronized)] set; }

        // Token: 0x17000135 RID: 309
        // (get) Token: 0x060003C6 RID: 966 RVA: 0x0000426A File Offset: 0x0
000246A
        // (set) Token: 0x060003C7 RID: 967 RVA: 0x0001C3A0 File Offset: 0x0
001A5A0
        internal virtual Button b_Add
        {
            [CompilerGenerated]
            get
            {
                return this._b_Add;
            }
            [CompilerGenerated]
            [MethodImpl(MethodImplOptions.Synchronized)]
            set
            {
                EventHandler value2 = new EventHandler(this.b_Add_Click);
                Button b_Add = this._b_Add;
                if (b_Add != null)
                {
                    b_Add.Click -= value2;
                }
                this._b_Add = value;
                b_Add = this._b_Add;
                if (b_Add != null)
                {
                    b_Add.Click += value2;
                }
            }
        }

        // Token: 0x17000136 RID: 310
        // (get) Token: 0x060003C8 RID: 968 RVA: 0x00004272 File Offset: 0x0
0002472
        // (set) Token: 0x060003C9 RID: 969 RVA: 0x0001C3E4 File Offset: 0x0
001A5E4
        internal virtual Button b_del
        {
```

```
            [CompilerGenerated]
            get
            {
                return this._b_del;
            }
            [CompilerGenerated]
            [MethodImpl(MethodImplOptions.Synchronized)]
            set
            {
                EventHandler value2 = new EventHandler(this.b_del_Click);
                Button b_del = this._b_del;
                if (b_del != null)
                {
                    b_del.Click -= value2;
                }
                this._b_del = value;
                b_del = this._b_del;
                if (b_del != null)
                {
                    b_del.Click += value2;
                }
            }
        }

        // Token: 0x17000137 RID: 311
        // (get) Token: 0x060003CA RID: 970 RVA: 0x0000427A File Offset: 0x
0000247A
        // (set) Token: 0x060003CB RID: 971 RVA: 0x00004282 File Offset: 0x0
0002482
        internal virtual DataGridView DGV0 { get; [MethodImpl(MethodImplO
ptions.Synchronized)] set; }

        // Token: 0x17000138 RID: 312
        // (get) Token: 0x060003CC RID: 972 RVA: 0x0000428B File Offset: 0x
0000248B
        // (set) Token: 0x060003CD RID: 973 RVA: 0x00004293 File Offset: 0x0
0002493
        internal virtual DataGridViewTextBoxColumn Column2 { get; [MethodI
mpl(MethodImplOptions.Synchronized)] set; }

        // Token: 0x17000139 RID: 313
        // (get) Token: 0x060003CE RID: 974 RVA: 0x0000429C File Offset: 0x
0000249C
        // (set) Token: 0x060003CF RID: 975 RVA: 0x000042A4 File Offset: 0x0
00024A4
        internal virtual TextBox TextIP { get; [MethodImpl(MethodImplOptions
.Synchronized)] set; }
```

```
        // Token: 0x1700013A RID: 314
        // (get) Token: 0x060003D0 RID: 976 RVA: 0x000042AD File Offset: 0x
000024AD
        // (set) Token: 0x060003D1 RID: 977 RVA: 0x0001C428 File Offset: 0x0
001A628
        internal virtual Button OKY
        {
            [CompilerGenerated]
            get
            {
                return this._OKY;
            }
            [CompilerGenerated]
            [MethodImpl(MethodImplOptions.Synchronized)]
            set
            {
                EventHandler value2 = new EventHandler(this.OKY_Click);
                Button oky = this._OKY;
                if (oky != null)
                {
                    oky.Click -= value2;
                }
                this._OKY = value;
                oky = this._OKY;
                if (oky != null)
                {
                    oky.Click += value2;
                }
            }
        }

        // Token: 0x1700013B RID: 315
        // (get) Token: 0x060003D2 RID: 978 RVA: 0x000042B5 File Offset: 0x0
00024B5
        // (set) Token: 0x060003D3 RID: 979 RVA: 0x000042BD File Offset: 0x
000024BD
        internal virtual NumericUpDown po { get; [MethodImpl(MethodImplO
ptions.Synchronized)] set; }

        // Token: 0x1700013C RID: 316
        // (get) Token: 0x060003D4 RID: 980 RVA: 0x000042C6 File Offset: 0x0
00024C6
        // (set) Token: 0x060003D5 RID: 981 RVA: 0x0001C46C File Offset: 0x0
001A66C
        internal virtual Timer TOpacity
        {
            [CompilerGenerated]
            get
```

```
            {
                return this._TOpacity;
            }
            [CompilerGenerated]
            [MethodImpl(MethodImplOptions.Synchronized)]
            set
            {
                EventHandler value2 = new EventHandler(this.TOpacity_Tick);
                Timer topacity = this._TOpacity;
                if (topacity != null)
                {
                    topacity.Tick -= value2;
                }
                this._TOpacity = value;
                topacity = this._TOpacity;
                if (topacity != null)
                {
                    topacity.Tick += value2;
                }
            }
        }

        // Token: 0x060003D6 RID: 982 RVA: 0x000042CE File Offset: 0x00002
4CE
        public EditSocket()
        {
            base.Load += this.EditSocket_Load;
            this.RectInputText0 = new List<Rectangle>();
            this.InitializeComponent();
            this.Font = reso.f;
        }

        // Token: 0x060003D7 RID: 983 RVA: 0x0001C4B0 File Offset: 0x0001A
6B0
        private void SpyStyle()
        {
            this.po.BackColor = SpySettings.DefaultColor_Background;
            this.po.ForeColor = SpySettings.DefaultColor_Foreground;
            checked
            {
                this.RectInputText0.Add(new Rectangle(this.po.Location.X - 1, thi
s.po.Location.Y - 1, this.po.Width + 1, this.po.Height + 1));
                try
                {
                    foreach (DataGridView dataGridView in this.PanelBOX.Controls
.OfType<DataGridView>())
                    {
                        dataGridView.BackgroundColor = SpySettings.DefaultColor_
```

```
Background;
                dataGridView.BackColor = SpySettings.DefaultColor_Backgr
ound;
                dataGridView.ColumnHeadersDefaultCellStyle.BackColor =
SpySettings.DefaultColor_Background;
                dataGridView.DefaultCellStyle.BackColor = SpySettings.Def
aultColor_Background;
                dataGridView.DefaultCellStyle.SelectionForeColor = SpySett
ings.DefaultColor_Background;
                dataGridView.DefaultCellStyle.ForeColor = SpySettings.Defa
ultColor_Foreground;
                dataGridView.DefaultCellStyle.SelectionBackColor = SpySett
ings.DefaultColor_Foreground;
                dataGridView.ColumnHeadersDefaultCellStyle.ForeColor =
SpySettings.DefaultColor_Foreground;
            }
        }
        finally
        {
            IEnumerator<DataGridView> enumerator;
            if (enumerator != null)
            {
                enumerator.Dispose();
            }
        }
        try
        {
            foreach (Label label in this.PanelBOX.Controls.OfType<Label>(
))
            {
                label.ForeColor = SpySettings.DefaultColor_Foreground;
            }
        }
        finally
        {
            IEnumerator<Label> enumerator2;
            if (enumerator2 != null)
            {
                enumerator2.Dispose();
            }
        }
        try
        {
            foreach (Button button in this.PanelBOX.Controls.OfType<Butt
on>())
            {
                button.BackColor = SpySettings.DefaultColor_Foreground;
                button.ForeColor = SpySettings.DefaultColor_Background;
```

```
            }
        }
        finally
        {
            IEnumerator<Button> enumerator3;
            if (enumerator3 != null)
            {
                enumerator3.Dispose();
            }
        }
        try
        {
            foreach (TextBox textBox in this.PanelBOX.Controls.OfType<Te
xtBox>())
            {
                textBox.BackColor = SpySettings.DefaultColor_Background;
                textBox.ForeColor = SpySettings.DefaultColor_Foreground;
                this.RectInputText0.Add(new Rectangle(textBox.Location.X -
1, textBox.Location.Y - 1, textBox.Width + 1, textBox.Height + 1));
            }
        }
        finally
        {
            IEnumerator<TextBox> enumerator4;
            if (enumerator4 != null)
            {
                enumerator4.Dispose();
            }
        }
        try
        {
            foreach (Panel panel in base.Controls.OfType<Panel>())
            {
                panel.BackColor = SpySettings.DefaultColor_Background;
            }
        }
        finally
        {
            IEnumerator<Panel> enumerator5;
            if (enumerator5 != null)
            {
                enumerator5.Dispose();
            }
        }
        this.Refresh();
    }
}
```