МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ»
Кафедра Систем информационной безопасности

«ДОПУЩЕН К ЗАЩИТЕ»
Зав. кафедрой к.п.н., доцент Р. Ш. Бердибаев
_____ «_____» _____2019 г.
(подпись)

ДИПЛОМНЫЙ ПРОЕКТ

На тему: Защита пользовательских данных на уровне операционной системы
Специальность Системы информационной безопасности
Выполнил Кайрбаев Назымбек Эсетович Группа СИБ-15-2
Научный руководитель Аскарова Нурсанат Темирбековна

Консультант:
по экономической части:
к.э.н., профессор Арепбаева Ж.Г.
(ученая степень, звание, Ф.И.О)
_____ «22» мая 2019 г.
(подпись)

по безопасности жизнедеятельности:
э.т.н., ст. преп. Бекбасаров Ш.Ш.
(ученая степень, звание, Ф.И.О)
_____ «22» мая 2019 г.
(подпись)

по применению вычислительной техники:
м.т.н., ст. преподаватель Аскарова Н.Т.
(ученая степень, звание, Ф.И.О)
_____ «24» мая 2019 г.
(подпись)

Нормоконтролер:
м.т.н., ст. преподаватель Аскарова Н.Т.
(ученая степень, звание, Ф.И.О)
_____ «24» мая 2019 г.
(подпись)

Рецензент:
_____
(ученая степень, звание, Ф.И.О)
_____ «_____» _____2019 г.
(подпись)

Алматы 2019

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ»
Институт систем управления и информационных технологий
Кафедра Систем информационной безопасности
Специальность Системы информационной безопасности

ЗАДАНИЕ
на выполнение дипломного проекта

Студенту Кайрбаеву Назымбеку Эсетовичу

Тема проекта Защита пользовательских данных на уровне операционной системы

Утверждена приказом по университету № 124 от « 26 » октября 2018 г.

Срок сдачи законченного проекта «_____» _____2019 г.

Исходные данные к проекту (требуемые параметры результатов исследования (проектирования) и исходные данные объекта): работа подразумевает проектирование системы защиты пользовательских данных на уровне ОС, которое позволяет пользователю улучшить безопасность персональных данных. В качестве инструмента для улучшения безопасности использовались групповые политики, то есть были применены ряд политик в параметрах безопасности. В системе защиты будет использовались и применяться следующие политики: минимальная длина пароля, политика сложного пароля, политика блокировки учетной записи, аудит входа в систему, переименование учетной записи Администратор и так далее. Также в целях улучшения безопасности были использованы следующие встроенные функции: выполнение резервного копирования с помощью службы архивации, шифрование диска.

Перечень вопросов, подлежащих разработке в дипломном проекте, или краткое содержание дипломного проекта: дипломный проект включает в себя 5 глав, разделенных на подглавы, каждая из которых освещает определенную тематику, связанную с проектированием системы защиты.

В первой главе дипломного проекта представлена информация об анализе операционных систем: виды операционных систем, назначение и функции операционных систем, сравнение операционных систем, исследование уязвимостей, защита операционной системы.

Во второй главе дипломного проекта представлена информация об мерах защиты пользовательских данных: внутренние меры защиты и внешние меры защиты.

В третей главе подробно описывается проектирование и конфигурация системы защиты пользовательских данных.

В четвертой главе приводится безопасность жизнедеятельности. Имеются в подглавах расчеты тепловых нагрузок в помещении и расчет теплового баланса.

В пятой главе рассматриваются технико-экономическое обоснование. Расчеты были произведены на: затраты на проектирование системы, затраты на электроэнергию, затраты на оплату труда, затраты на социальный налог и затраты на амортизацию.

Перечень графического материала (с точным указанием обязательных чертежей):

1 топология сети;

2 скрины операционной системы;

3 скрины с примененными групповыми политиками;

4 скрины резервного копирования;

5 скрины с шифрованием.

Основная рекомендуемая литература:

1 Аманжолова К. Б., Алибаева С. А. Экономика предприятии телекоммуникации: Учебное пособие. - Алматы: АИЭС, 2003

2 Голубицкая Е. А., Жигульская Г. М. Экономика связи. – М. Радио и связь, 2000

3 Самоучитель Python URL: https://pythonworld.ru/samouchitel-python

4 Групповые политики URL: https://habr.com/ru/post/262247/

5 Active Directory: https://ru.epicstars.com/botyi-telegram/

6 Нормы микроклимата URL: http://adilet.zan.kz/rus/docs /V050003789

Конструкции по проекту с указанием относящихся к ним разделов проекта

Раздел	Консультант	Сроки	Подпись
Безопасн. жизнедеят.	Бекбасаров Ш.Ш.	05.03-23.05	
Экономика	Аренбаева Н.Г.	04.03-22.05	
Нормоконтроль	Аскарова Ж.Б.	24.05.	
Вычисл. техники	Аскарова Ж.Б.	04.03-24.05	

График
подготовки дипломного проекта

Наименование разделов, перечень разрабатываемых вопросов	Сроки представления научному руководителю	Примечание
Анализ операционных систем	1.02.2019-4.02.2019	
Виды операционных систем	5.02.2019 - 7.02.2019	
Назначение и функции опер. сис.	8.02.2019 - 12.02.2019	
Сравнение операционных систем	13.02.2019 - 15.02.2019	
Меры защиты пользователя	18.02.2019 - 22.02.2019	
Внутренние меры защиты	25.02.2019 - 27.02.2019	
Внешние меры защиты	28.02.2019 - 4.03.2019	
Проектирование и конструирование	5.03.2019 - 7.03.2019	
Постановка задачи	8.03.2019 - 13.03.2019	
Требования к проектированию	14.03.2019 - 18.03.2019	
Объект защита	19.03.2019 - 22.03.2019	
Настройка Active Pirectory	25.03.2019 - 28.03.2019	
Групповые политики WS 2012	29.03.2019 - 3.04.2019	
Восстановление системы	4.04.2019 - 9.04.2019	
Bit Locker	10.04.2019 - 15.04.2019	
Безопасность жизнедеятельности	16.04.2019 - 19.04.2019	
Технико - экономическое обоснование	22.04.2019 - 25.04.2019	

Дата выдачи задания «___» _____ 2019 г.

Заведующий кафедрой _____ (_____)
(Подпись) (Ф.И.О)

Научный руководитель проекта _____ (Макарова Н.Ф.)
(Подпись) (Ф.И.О)

Задание принял к исполнению студент _____ (Кайрбаев М.Э.)
(Подпись) (Ф.И.О)

Аннотация

Дипломный проект посвящен проектированию защиты пользовательских данных на уровне операционной системы. Была спроектирована корпоративная сеть со своим именным доменом организации. Рассмотрены доменные параметры конфигурации групповых политик операционной системы Windows Server 2012. В целях улучшения защиты пользовательских данных был выполнен backup и шифрование файлов.

Также был произведен анализ условий труда при проектировании системы защиты и эксплуатации. В части технико-экономических обосновании были произведены расчеты экономической эффективности проектируемой системы защиты.

Аңдатпа

Дипломдық жоба операциялық жүйе деңгейінде пайдаланушылық деректерді қорғауды жобалауға арналған. Ұйымның атау доменімен корпоративтік желісі жобаланды. Windows Server 2012 операциялық жүйесінің топтық саясат теңшелімінің домен параметрлері қарастырылды. Пайдаланушы деректерін қорғауды жақсарту мақсатында сақтық көшірме және файлдарды шифрлеу орындалды.

Сонымен қатар, қорғау және пайдалану жүйесін жобалау кезінде еңбек жағдайларына талдау жүргізілді. Техникалық-экономикалық негіздемелер бөлігінде жобаланатын қорғау жүйесінің экономикалық тиімділігінің есептеулері жүргізілді.

Annotation

The graduation project is dedicated to designing user data protection at the operating system level. A corporate network was designed with its own organization’s domain name. Considered domain configuration settings group policies of the operating system Windows Server 2012. In order to improve the protection of user data, backup and file encryption was performed.

Also, an analysis of working conditions in the design of protection and operation systems was made. In terms of feasibility studies, calculations were made of the economic efficiency of the designed protection system.

Содержание

Введение

На данный момент информационный контент в общедоступном варианте стал применим в виде компьютерных сетей, которые помогают в ежедневном быте. Компьютерные сети полностью внедрились в повседневную жизнь людей, также вместе с этим явлением развился и другой фактор это – безопасность данных. Как только началось использование и функционирование персональных данных в информационных системах, отчитывая от социальных сетей и заканчивая поликлиникой, существенно обосновался риск и опасность разглашения личной информации.

В процессе развития информационных систем стали реализовываться методы, средства и виды авторизации информационных систем. Массово стали применяться вычислительные техники, вместе с ним появились и уязвимости. Данные могут быть редактированы вне закона или могут вовсе быть похищены и уничтожены. Если учитывать то, что чтобы установить и оборудовать хорошую систему защиты данных потребуется большие материальные и финансовые затраты, нужно не только выставлять пороговые механизмы защиты, а использовать специальные средства, методы и мероприятия с целью предотвращения потери данных.

Целью написания данной моей дипломной работы было изучить виды операционных системы, также вместе с ним и защита систем, выявление видов защиты, меры построения базовой защиты с использованием встроенных мер защиты и посторонними методами. К дополнению, так как на данный момент вопрос о безопасности данных является приоритетным направлением в информационной системе, я показал свое видение защиты пользовательских данных на уровне операционной системы Windows 10.

В нынешнее время информационных технологий вопрос безопасности стоит на важных позициях. В связи с этим считаю тему дипломной работы актуальной. Практические действия направленные на безопасное хранение данных в операционной системе связаны были со встроенными мерами защиты. Выделяю такую актуальную тему как защита пользовательских данных на уровне операционной системы, я использовал в практической части групповые политики операционной системы Windows. С целью улучшения системы безопасности в различных организациях, сотрудники и все люди имеющие непосредственное отношение к организации имеют положительное мнение во внедрении различных систем защит. Учитывая фактор риска кражи, удаления, повреждения пользовательских данных, система защиты имеет возможность улучшения защиты данных. В начале внедрения системы защиты с помощью групповых политик, нужно учитывать желания каждого пользователя во внутренней сети организации, потому как в некоторых случаях систем защиты, пользователю придется смириться с разными деталями в процессе работы. Групповые политики являются важными деталями в пользовательской системе, так как с помощью них пользователь может самостоятельно включить политики необходимые для него.

1 Анализ операционных системы

В данном дипломном проекте я изучил и ознакомился с видами и мерами защиты операционных систем, такие операционные системы как:

- Windows;
- Linux;
- Mac OS.

В частности были затронуты такие виды защиты операционных систем: внутренние меры защиты операционных систем и внешние меры. К внешним мерам отнесем такие меры как: антивирусы и различные программные обеспечения для полномерной и контролирующей защиты системы.

Внутренние меры защиты операционной системы к этому термину можно отнести вещи и возможности системы, которые были основаны при создании и внедрении различных операционных систем для эксплуатации различных целей. То есть возможностями, которых может воспользоваться любой использующий систему. Встроенные меры защиты являются вполне серьезными мерами защиты для безопасности персонального компьютера, вследствие чего пользователь может безопасно и полномерно функционировать возможностями своей системы.

Внешние меры защиты операционных системы к этому термину можно отнести вещи, которые мы устанавливаем добровольно в целях полномерной работы операционной системы и безопасности данных, с которыми мы ежедневно работаем. Если рассматривать антивирусы, то антивирусы относятся к внешним программным обеспечениям для защиты системы. То есть пользователь устанавливает антивирус в целях предотвращения кражи или же уничтожения данных. Антивирусы имеют множество функции направленные на защиту и мониторинга системы.

1.1 Виды операционных систем

Существует множество видов операционных систем, но я выделю основные три, которые сейчас овладели информационным рынком и которые больше всего используются в качестве установки системы на пользовательский компьютер.

1.1.1 Microsoft Windows

Всемирно известная и одна из самых компетентным компании в информационном рынке Microsoft, выпустила свою первую операционную систему в середине 1980-х годов. После этого релиза было выпущено и создано много версии и видов операционных систем Windows, но самыми востребованными на рынке оказались Windows 10, Windows XP, Windows 7, Windows Vista и Windows8. Если мы устанавливаем операционную систему Windows, нужно выбрать какую версию мы хотим и также какой выпуск мы предпочтем для установки, виды выпусков:

- Home Premium;

- Professional;
- Ultimate.

В настоящее время Windows является одной из популярнейших операционных систем, не только потому, что он удобен в использовании и большого выбора функционала, но и за возможности высокого уровня интеграции. Windows привыкли использовать в целях использования исключительно для персонального компьютера, но также есть возможность использовать его на серверных версиях вычислительной техники. Windows сам по себе очень прост в использовании, чем и захватил информационный рынок. Благодаря простым версиям Windows, стало максимально легко управлять персональным компьютером. Большим преимуществом Windows стало то, что он имеет простой графический интерфейс, состоящий из значков в окнах, в которых имеется описание к каждой кнопке. То, что в Windows появилось много возможностей стало одновременно открытием и удобством в его использовании, к примеру, появления одновременной работы и использовании с несколькими программами во много раз увеличила эффективность работы системы. Важным фактором в популяризации Windows, стало то, что появилась возможность легкого и удобного написания программ, что послужило большому количеству программных обеспечении, работающим над управлением операционной системы Windows.

К тому, что Windows особенный могу отнести множество вещей: то, что он многозадачный, то есть процессор может переключаться между программными обеспечениями; имеется свой один программный интерфейс, что позволяет создавать данные в одних окнах и программах и перемещать их в другие; единый пользовательский интерфейс, что означает интерфейс приложении стандартизирован, то есть, освоив одну программу легче освоить и другие; единый программно-аппаратный интерфейс. Важным преимуществом системы является то, что система сама обеспечивает совместимость разнообразного оборудования и программ. Производители оборудования добиваются только работы с Windows, после чего система берет на себя заботы по обеспечению работы устройств. Аналогично производители программ могут не переживать о работе с неизвестным им оборудованием. Подключение устройств, происходит автоматически, система распознает то, что установлено на компьютере, и настраивает на работу с новым оборудованием.

Одной из популярнейших систем стала версия Windows 7, операционная система семейства Windows NT, следующая за Windows Vista. Сама операционная система появилась на свет и вышла в продажу 22 октября 2009 года, меньше чем через три года после выпуска Windows Vista. По данным из статистики 2012 года для Windows 7 среди используемых в мире операционных систем для доступа в Интернет составила около 55%, вследствие чего заняла 1 место во всем мире по эксплуатации и внедрению систем в компьютеры. Новые изменения в этой версии системы послужили пользой для многочисленных пользователей. В Windows 7 встроено было 120

фоновых рисунков, которые были уникальны для каждой страны и языковой версии. Также стало заметно появление 50 новых шрифтов, а шрифты, которые раньше использовались в системе, были доработаны в целях корректного отображения всех символов. Стоит отметить, что Windows 7 стала первой версией, которая включает больше шрифтов для отображения нелатинских символов, чем для отображения латинских. Также в дополнение к новшеству системы можно отнести тесную интеграцию с производителями драйверов. Большинство драйверов определяются автоматически, при этом в 90% случаев сохраняется обратная совместимость с драйверами для Windows Vista. В системе Windows 7 была улучшена совместимость со старыми приложениями, некоторые из которых нельзя было запустить на Windows Vista. DirectX 11-ой версии впервые была выпущена вместе с Windows 7, были добавлены следующие улучшения: была добавлена поддержка новых вычислительных шейдеров, возможность многопоточного рендеринга, улучшена тесселяция, появились новые алгоритмы компрессии текстур и др. Новшества в операционной системе Windows 7 произошли в направлении безопасности. Сюда можно отнести то, что в системе была реализована более гибкая настройка User Account Control, также внесены изменения в технологию шифрования BitLocker и добавлены функции шифрования съемных носителей BitLocker to go.

1.1.2 Linux

Операционная система Linux, является одной из передовых систем в рынке и держит свою марку по сей день. У Linux множество преимуществ, которым позавидуют другие операционные системы. Система является на данный момент одной из известнейших и наиболее часто используемой операционной системой с открытым исходным кодом.

Linux был создан в 1991 году Линусом Торвальдсом, тогдашним студентом Университета Хельсинки. Торвальдс создал Linux как бесплатную и открытую альтернативу Minix, другому клону Unix, который преимущественно использовался в академических условиях. Первоначально он намеревался назвать его «Freax», но администратор сервера Торвальдс использовал для распространения оригинального кода, названного его каталогом «Linux», после сочетания имени Торвальдса и слова Unix, после чего имя застряло.

Linux является программным обеспечением, которое находится под всем остальным программным обеспечением на компьютере, в связи с этим получает запросы от этих программ и передает эти запросы аппаратному программному обеспечению. Также система в целом является ядром и набором программных обеспечении, инструментов и сервисов чтобы обеспечить все необходимые компоненты для полнофункциональной работы операционной системы.

Во многих отношениях Linux похож на другие операционные системы, с которыми мы встречались ранее. Как и другие операционные системы Linux

имеет свой графический интерфейс, а типы программного обеспечения, которые мы привыкли использовать в других операционных системах схожи. Во многих случаях создатель программного обеспечения мог сделать версию для Linux той же программы, которую мы использовали в других системах. Стоит отметить, что Linux также отличается от других операционных систем во многих важных отношениях. Во-первых, и, возможно, самое главное, Linux – это программное обеспечение с открытым исходным кодом. Код, используемый для создания Linux, является бесплатным и общедоступным для просмотра, редактирования для пользователей которые имеют навыки для внесении изменении в код. Большим преимуществом системы является то, что компании и частные лица выбирают именно эту систему для своих серверов, потому что это безопасно и за возможность получения поддержки от большого сообщества пользователей.

Linux состоит, в основном, из трех важных и неизменимых компонентов: ядро, системная библиотека и системные утилиты.

Ядро – является основной частью Linux. Он отвечает за все основные виды деятельности этой операционной системы. Он состоит из различных модулей и напрямую взаимодействует с базовыми оборудованиями. Ядро в целом представляет собой необходимую абстракцию для сокрытия сведений об оборудовании низкого уровня в системах или прикладных программ.

Системная библиотека – это специальные функции или программы, с помощью которых прикладные программы или системные утилиты получают доступ к функциям ядра. Эти библиотеки реализуют большинство функции операционной системы и не требуют прав доступа к коду модуля ядра.

Системные утилиты отвечают за выполнение специализированных задач индивидуального уровня.

1.1.3 Mac OS

Mac OS в оригинале эта операционная система именуется, как Macintosh Operating System. Всемирно известная технологическая компания Apple разработала эту систему для своих клиентов. Впервые она была представлена в 1984 году, операционная система была на основе графического интерфейса, и имела несколько различных версии.

Операционная система Mac OS считается и является пионером операционных систем на основе графического интерфейса, поскольку она была запущена, когда MS-DOS был отраслевым стандартом. Система является полностью работоспособной и соответствует всем требуемым стандартам. Mac OS является системой, которая предоставляет функциональные возможности и сервисы, аналогичные системам OS Windows и Linux.

Система Mac OS предназначена для работы на компьютерах Apple, и по умолчанию не поддерживает архитектуру x86. Маркетинг Apple по выпуску системы Mac OS, был сосредоточен на интуитивной простоте использования операционной системы. В отличие от практически всех других современных ПК, Mac OS была изначально основана на графическом изображении.

Пользователю не приходилось вводить команды и пути к каталогам в текстовых подсказках, была возможность пользователю перемещать указателем мыши, чтобы визуально перемещать по Finder – серии виртуальных папок и файлов, которые были в виде значков. В 1980-х Apple заключила соглашение, позволяющее Microsoft использовать некоторые аспекты интерфейса Mac в ранних версиях Windows. Тем не менее, за исключением краткого периода в 1990-х годах, Mac OS никогда не лицензировалась для использования с компьютерами других производителей, кроме Apple.

В более поздних выпусках Mac OS появились такие функции, как общий доступ к файлам через Интернет, просмотр сети и учетные записи нескольких пользователей. В 1996 году Apple приобрела конкурирующую компанию NeXT Computers, которая была основана Стивеном Джобсом после его ухода из Apple, а в 2001 году компания выпустила Mac OS X – крупный редизайн, основанный как на системе NextStep, так и на последней версии OS Apple. OS X работала на ядре UNIX и предлагала технические усовершенствования, такие как защита памяти и вытесняющая многозадачность, наряду с более универсальным Finder, элегантным интерфейсов под названием Aqua и удобной графической панелью Docx для частого запуска используемых приложений. Обновление OS X добавили такие функции, как автоматическое резервное копирование и менеджер “Dashboard” для небольших удобных приложений, называемых виджетами.

1.2 Назначение и функции операционных систем

Операционная система имеет набор программ, которые находятся между прикладным программным обеспечением и компьютерным оборудованием. Концептуально программное обеспечение операционной системы является посредником между аппаратным и прикладным программным обеспечением. Термин системное программное обеспечение иногда используется взаимозаменяемо с операционной системой, но системное программное обеспечение означает все программы, связанные с координацией компьютерных операции. Системное программное обеспечение включает в себя операционную систему, но также включает программное обеспечение BIOS, драйверы и служебные программы.

Операционная система имеет три основные функции: управлять ресурсами компьютера, такими как центральный процессор, память, дисководы и принтеры; устанавливать интерфейс пользователя; выполнять и предоставлять сервисы для прикладного программного обеспечения. Большая часть работы операционной системы скрыта от пользователя, многие необходимые задачи выполняются скрытно. Если мы разберем функцию управления ресурсами, то она направлена на то, чтобы пользователь не знал деталей. Все операции вводы и вывода, хотя и запускаются прикладной программой, фактически выполняются операционной системой.

К важным функциям операционной системы можно отнести и видимые функции, то есть то что замечает каждый пользователь и использует возможность данной функций. В области безопасности операционная система использует защиты паролем для защиты пользовательских данных и другие подобные методы, это предотвращает несанкционированный доступ к программам и данным пользователя. Контроль производительности системы, функция которая отслеживает общее состояние системы, чтобы повысить производительность, также записывает время ответа между запросами на обслуживание и ответом системы. Целью и назначением данной возможности операционной системы является то, чтобы получить полное представление о работоспособности системы. Бухгалтерский учет работы, система отслеживает время и ресурсы, используемые различными задачами и пользователями, эта информация может использоваться для отслеживания использования ресурсов для конкретного пользователя или группы пользователей. Средство обнаружения ошибок, система постоянно контролируется, чтобы обнаружить ошибки и избежать сбоя в работе компьютерной системы. Координация между другим программным обеспечением и пользователями, операционные системы также координируют и назначают интерпретаторы, компиляторы, ассемблеры и другое программное обеспечение для различных пользователей компьютерных систем. Управление памятью, операционная система управляет основной памятью или основной памятью. Основная память состоит из большого массива байтов или слов, где каждому байту или слову присваивается определенный адрес. Основная память - это быстрое хранилище, к которому может обращаться непосредственно центральный процессор. Для выполнения программы она должна быть сначала загружена в основную память. Операционная система выполняет следующие действия для управления памятью: он отслеживает первичную память, то есть какие байты памяти используются какой пользовательской программой. Адреса памяти, которые уже были выделены, и адреса памяти, которые еще не использовались. В мультипрограммировании ОС решает порядок, в котором процессу предоставляется доступ к памяти, и как долго. Он выделяет память для процесса, когда процесс запрашивает ее, и освобождает память, когда процесс завершается или выполняет операцию ввода-вывода. Управление процессором , в многопрограммной среде ОС определяет порядок, в котором процессы имеют доступ к процессору, и сколько времени обработки у каждого процесса. Эта функция ОС называется планированием процессов. Операционная система выполняет следующие действия для управления процессором. Отслеживает статус процессов. Программа, которая выполняет эту задачу, называется контроллером трафика. Распределяет процессор, который является процессором, процессу. Отключает процессор, когда процесс больше не требуется. Управление устройством, операционная система управляет связью устройства через соответствующие драйверы. Он выполняет следующие действия для управления устройством. Отслеживает

все устройства, подключенные к системе, обозначает программу, отвечающую за каждое устройство, известное как контроллер ввода / вывода. Решает, какой процесс получает доступ к определенному устройству и как долго. Выделяет устройства эффективным и действенным способом. Отключение устройств, когда они больше не нужны. Управление файлами, файловая система организована в каталоги для эффективной или простой навигации и использования. Эти каталоги могут содержать другие каталоги и другие файлы. Операционная система выполняет следующие действия по управлению файлами. Он отслеживает, где хранится информация, настройки доступа пользователя и состояние каждого файла и многое другое. Эти средства все вместе известны как файловая система.

Существует множество функции которые выполняет операционная система, но основная задача ее состоит в том, чтобы обеспечить интерфейс между пользователем и оборудованием. Операционная система, также известная как средство диспетчера устройств, управляет всеми ресурсами, подключенные к системе, известны как ресурсы компьютера. К примеру, система определяет в какое время ЦП будет выполнять операцию и в какое время память будет использоваться программами.

Одна из функции операционной системы состоит в том, чтобы контролировать все операции хранения, то есть, как данные или файлы будут храниться на компьютерах и как файлы будут доступны пользователям. Все возможные операции, которые несут ответственность за хранение и доступ к файлам, определяется операционной системой. Также система позволяет нам создавать файлы, каталоги и читать, записывать данные файлы, а также копировать содержимое файлов и каталогов из одного места в другое.

Функции, которые относятся к управлениям хранения: управление процессами, управление памятью, расширенная машина, многозадачность.

Управление процессами, означает, что все процессы, которые предоставляют пользователям, или процессы, которые являются собственными процессами системы, управляются операционной системой. Система создаст приоритет для пользователя, а также запустит или остановит выполнение процесса и создаст дочерний процесс после разделения больших процессов на малые процессы.

Управление памятью, операционная система управляет памятью компьютера. Системные средства предоставляют память для процесса, а также освобождают память от процесса. Управление памятью определяет, что если процесс завершится, то это освободит память от процесса.

Расширенная машина, это функция означает, что операционная система также предоставляет нам общий доступ к файлам между несколькими пользователями, которые имеют графические среды.

Система может выполнять множество функции, поэтому ее можно назвать многозадачной. В этой функции есть возможность увеличить логическую память компьютера с помощью физической памяти компьютерной системы.

Назначение операционных систем можно разделить на множество категорий и вещей. Понятие назначения операционной системы связано с целями и концепцией систем. Суть системы в предоставлении пользователю и функционирующему операционной системой, состоит в основном с том чтобы система динамически распределяла ресурсы вычислительной техники а также имела такие способности и навыки как управление ресурсами системы в соответствии с требованиями задач и процессов. Ресурсом операционной системы может быть объект, в способности и возможности которого входит разграничение системы между электронно-вычислительной машиной и вычислительными процессами. Электронно-вычислительные машины можно разделить в два вида, это аппаратные ресурсы и программные ресурсы. Одному из видов, а именно к аппаратным можно отнести такие вещи, как процессорное время, оперативно запоминающее устройство и периферийные устройства. Ко второму типу, а именно программным относятся несколько другие вещи, это являются программные средства целью которых может носить характер управления вычислительными процессами и данными. Назначением операционной системы является в первую очередь распределение ресурсов в соответствии с теми запросами пользователя, которые непосредственно взаимодействует с системой. Как правило, ресурс функционирует в качестве разделения, когда все вычислительные процессы занимают его в промежутке какого-то интервала времени. Вкратце суть разделения времени состоит в следующем. Каждому программному обеспечению, которые имеют свое место в оперативной памяти и стоит в режиме готов к функционированию, распределяется для выполнения определенный интервал времени, состоящий в соответствии с приоритетом пользователя. В случае того, если программное обеспечение не будет выполнена в границах этого интервала, ее функционирование обязательно прекращается и программа откатывается в конец очереди. Из начала очереди убирается та программа, которая функционирует в периоде соответствующего интервала мультиплексирования, после чего программа поступает в конец очереди, в соответствии с циклическим алгоритмом. В режиме разделения существует одна разновидность, которой является фоновый режим. Фоновый режим распределения можно объяснить в следующей формулировке, в процессе работы программы у которой приоритет ниже работает на фоне программы у которого приоритет выше.

Технологический термин ресурс которое относится к вычислительной технике следует понимать в качестве функционального элемента вычислительной системы, который также выделен процессу на определенный период времени. Если рассматривать вариант того, что физические ресурсы и реальные устройства электронно-вычислительной системы, с использованием нынешних передовых операционных систем могут создаваться и использовать виртуальные ресурсы, являющиеся моделями физических.

1.3 Сравнение операционных систем

Под понятие сравнение можно подразумевать описание важных и выделяющих компонентов, тех или иных операционных систем. В целом каждая операционная система имеет ярко-выраженные различия между собой. Различие, как правило насквозь видны пользователям и обращать внимание на различие систем непосредственно является важный аспектом в изучении видов операционных систем. Рассматривание каждой востребованной операционной системы, подразумевает под собой качественное и долгосрочное использование систем, вследствие чего выполняются выводы из анализа данных.

В сравнении буду использовать две операционные системы, это Windows и Mac OS.

Преимуществом и основными различиями в Mac OS является то, что эта операционная система на основе BSD Unix с графическим интерфейсом. Многие пользователи этой системы утверждают что система более удобна чем Windows. В операционной системе предусмотрены учетные записи на основе разрешений и улучшений средства управления доступом для ограничения распространения вредоносных программ. Программное обеспечение защищает системную папку от действий редактирования, если пользователь не имеет административных привилегий. Простота использования часто упоминается в качестве основной причины для использования в образовательных учреждениях и в бизнесе.

Что касается Windows, то она широко распространена в бизнес-средах и отличается архитектурой, в зависимости от того, какая версия установлена и версии лучше всего исследовать на информационном сайте продукта. Из-за популярности операционной системы Windows, вредоносных программ достаточно много и антивирусная программа часто является тем минимум, который пользователь должен использовать для защиты своих вычислительных ресурсов и данных.

Безопасность Mac OS и Windows.

В Mac OS было разработано значительно меньше вирусов, так как операционная система работает на небольшом количестве компьютеров , поэтому хакерам не кажется полезным создавать вирус. Меньшее количество вирусов для операционной системы, позволяет Apple оставаться на вершине самых безопасных систем, также исправление уязвимостей производится с помощью обновлений программного обеспечения. Поскольку нет необходимости в антивирусном программном обеспечении , это означает, что Mac по-прежнему может иметь оптимизированную производительность без риска для безопасности. Одним из важных компонентов этой системы безопасность, что в итоге является основным пунктом продажи операционной системы. Преимуществом является то, что нет сторонних вирусов, так как все меньше людей используют Mac OS. Недостатком является скорее всего то,

что операционная система не подвержена влиянию почти такого же количества проблем, как Windows.

В Windows большое количество вредоносных программ и вирусов, что ставит под угрозу безопасность системы. Причиной этого, является то, что существуют сотни тысяч вирусов для окон из-за большого количества пользователей, что сделало его большей целью для хакеров. Это является отрицательным качеством в системе Windows. В силу того, чтобы система являлась более безопасной и имела возможность полноценной работы, Windows для пользователей рекомендует сторонние антивирусные программные обеспечения. Встроенное антивирусное программное обеспечение не так сильно, как у другого типа антивирусного программного обеспечения, например Kaspersky. Потребность в антивирусном пакете также влияет на производительность системы, поэтому Mac может показаться быстрее. Как итог, чем больше людей используют Microsoft, тем больше вирусов.

Интерфейс Mac OS и Windows.

Операционная система Mac представила панель запуска, которая отображает все значки приложения. Панель запуска использует тот же интерфейс, что и iPad и iPhone, где пользователь может перейти к следующему экрану и перетащить значки в другой значок, чтобы создать папку. Это намного проще для навигации и использования, чем предыдущие интерфейсы. Большим же недостатком может являться то, что все сторонние приложения включают полноэкранный режим, который используется в Mac OS для небольших однооконных приложений, таких как iChat или Twitter, поэтому потребуется место на рабочем столе и чтобы это устранить пользователю придется перемещать все открытые значки, чтобы освободить место для полноэкранного режима.

В отличие от операционной системы Mac OS, Windows в действительности не изменил свой интерфейс. В более новых версиях операционных систем Windows, можно увидеть новшества такого вида, что можно увидеть страницу в уменьшенном виде, наведя указатель мыши на папку или значок, который находится на нижней панели задач, без нажатия на значок.

Встроенные программные обеспечения в системе Windows и Mac OS.

Если рассматривать систему компании Apple, а именно распространенную Mac OS, то можно заметить что встроенных программных обеспечении достаточно. Большим плюсом является то, что программы являются нужными для пользователя, то есть у пользователя есть возможность использовать программы в своих целях. Этими вещами можно заметить, что Apple старается сделать максимальные продукты для своих ценных пользователей. Встроенными программами являются: почта, iTunes, браузер Safari, мультимедийная программа iMovie. Такие программы как: Microsoft Office, Safari, Garage band, Photoshop уже непосредственно входят в систему, это и привлекает большое количество клиентов. Недостатком

является то, что Mac является дорогим компьютером. Функции Mac OS представлены по-разному, так как окна Windows представляют каждую программу в виде значка, независимо от того, как Mac OS представляют свои программы на объекте, называемом “док-станцией”. Это вид, где приложения находятся вместе и имеют легкий доступ.

Встроенными программными обеспечениями Windows, являются такие как: Internet Explorer, калькулятор, игры.

1.4 Исследование уязвимостей операционных систем

На сегодняшний день техническое слово уязвимость является одним из распространенных. В операционных системах можно по-разному предполагать уязвимости, так как проблем в работе операционных систем большое количество. Вопросы связанные напрямую с исследованием уязвимостей стоит в приоритете у разработчиков и у тех, кого интересует развитие систем. В целом операционные системы представляют собой сложные части программного обеспечения. Среда использования создает проблемы для систем, заставляя их обнаруживать ранее неизвестные дефекты. Некоторые их этих дефектов связаны с требованиями безопасности, которые называются уязвимостями.

Основные виды уязвимостей это:

- DoS (отказ в обслуживании);
- обход чего-либо (например, пароля для входа в систему);
- исполнение кода(возможность злоумышленником выполнить какую-то команду на устройстве жертвы);
- повреждение памяти;
- доступ к информации;
- увеличение привилегий переполнение(буфера).

1.4.1 DoS

Первая уязвимость: операционной системы Windows 10, это atmdf.dll в библиотеке Adobe Type Manager позволяет удаленно организовать DoS посредством созданного OpenType шрифта.

Вторая уязвимость: HTTP.sys позволяет устроить DoS через созданные запросы HTTP 2.0.

Таблица 1.1 - Уязвимости категории «DoS» в Windows 10

Уязвимость (№)	Код по CVE	Дата (дд/мм/гг)	Уровень воздействия на:			Сложность доступа	Аутентификация	Полученный доступ	Доп. виды уязвимости	Версии продукта
			Конфиденциальность	Целостность	Доступность					
№1	2015-2506	08/09/2015	Полный	Полный	Полный	Средняя	Не требуется	H/A		x64; x86
№2	2016-0150	12/04/2016	Отсутствует	Отсутствует	Полный	Низкая	Не требуется	H/A		1511
№3	2016-3369	14/09/2016	Отсутствует	Отсутствует	Полный	Низкая	Не требуется	H/A	Переполнение	1511

1.4.2 Обход чего-либо

Первая уязвимость: RDP позволял взломщикам обойти ограничения доступа и установить сессию для аккаунтов без пароля модифицированный RDP клиент.

Вторая уязвимость: Task Scheduler позволял локальному пользователю обойти ограничения системных файлов и удалить любой из них.

Таблица 1.2 - Уязвимостей категории «Обход чего-либо» в Windows 10

Уязвимость (№)	Код по CVE	Дата (дд/мм/гг)	Уровень воздействия на:			Сложность доступа	Аутентификация	Полученный доступ	Доп. виды уязвимости	Версии продукта
			Конфиденциальность	Целостность	Доступность					
№1	2016-0019	2016-01-13	Полный	Полный	Полный	Средняя	Не требуется	H/A		Gold (x86; x64); 1511 (x86; x64)
№2	2015-2525	08/09/2015	Полный	Полный	Полный	Низкая	Не требуется	H/A		
№3	2016-0151	12/04/2016	Полный	Полный	Полный	Низкая	Не требуется	H/A	Получение привилегий	1511

1.4.3 Исполнение кода

Первая уязвимость: операционная система позволяла злоумышленникам получать контроль над системой, когда Windows Search не удавалось обработать объекты в памяти.

Вторая уязвимость: операционная система позволяла взломщику удаленно исполнить команду на машине жертвы посредством того, как Windows Search обрабатывал объекты памяти.

Таблица 1.3 - Уязвимостей категории «Исполнение кода» в Windows 10.

Уязвимость (№)	Код по CVE	Дата (дд/мм/гг)	Уровень воздействия на:			Сложность доступа	Аутентификация	Полученный доступ	Доп. виды уязвимости	Версии продукта
			Конфиденциальность	Целостность	Доступность					
№1	2017-8543	14/06/2017	Полный	Полный	Полный	Низкая	Не требуется	H/A		1511; 1607; 1703
№2	2017-8589	11/07/2017	Полный	Полный	Полный	Низкая	Не требуется	H/A		1511; 1607; 1703
№3	2017-11771	13/10/2017	Полный	Полный	Полный	Низкая	Не требуется	H/A		1511; 1607; 1703

1.4.4 Повреждение памяти

Первая уязвимость: The Imaging Component позволял злоумышленнику повредить память через созданный им документ.

Вторая уязвимость: Animation Manager позволял исполнить код за счет созданного веб-сайта.

Таблица 1.4 - Уязвимостей категории «Повреждение памяти» в Windows

Уязвимость (№)	Код по CVE	Дата (дд/мм/гг)	Уровень воздействия на:			Сложность доступа	Аутентификация	Полученный доступ	Доп. виды уязвимости	Версии продукта
			Конфиденциальность	Целостность	Доступность					
№1	2016-0195	10/05/2016	Полный	Полный	Полный	Низкая	Не требуется	H/A	Исполнение кода, переполнение	1511
№2	2016-7205	10/11/2016	Полный	Полный	Полный	Низкая	Не требуется	H/A	Исполнение кода, переполнение	1511; 1607
№3	2016-7217	10/11/2016	Полный	Полный	Полный	Низкая	Не требуется	H/A	Исполнение кода, переполнение	1511; 1607

1.4.5 Доступ к информации

Первая уязвимость: драйверы в режиме ядра могли дать аутентифицированному злоумышленнику возможность исполнить созданное им приложение для получения информации или даже DoS.

Вторая уязвимость: GDI позволял обойти механизм защиты ASLR через неустановленный вектор.

Таблица 1.5 - Уязвимостей категории «Доступ к информации» в Windows

Уязвимость (№)	Код по CVE	Дата (дд/мм/гг)	Уровень воздействия на:			Сложность доступа	Аутентификация	Полученный доступ	Доп. виды уязвимости	Версии продукта
			Конфиденциальность	Целостность	Доступность					
№1	2017-0077	12/05/2017	Полный	Полный	Полный	Средняя	Не требуется	H/A	DoS	1511; 1607; 1703
№2	2016-3209	13/10/2016	Частичный	Отсутствует	Отсутствует	Низкая	Не требуется	H/A	Обход ограничений	1511; 1607
№3	2016-3312	09/08/2016	Частичный	Отсутствует	Отсутствует	Низкая	Не требуется	H/A		1511

1.4.6 Увеличение привилегий.

Первая уязвимость: драйверы в режиме ядра давали пользователю возможность получить привилегии через созданное им приложение.

Вторя уязвимость: графические компоненты ядра позволяли локальному пользователю получить привилегии через созданное им приложение.

Таблица 1.6 - Уязвимостей категории «Увеличение привилегий» в Windows

Уязвимость (№)	Код по CVE	Дата (дд/мм/гг)	Уровень воздействия на:			Сложность доступа	Аутентификация	Полученный доступ	Доп. виды уязвимости	Версии продукта
			Конфиденциальность	Целостность	Доступность					
№1	2016-3266	13/10/2016	Полный	Полный	Полный	Низкая	Не требуется	H/A		1511; 1607
№2	2016-3270	13/10/2016	Полный	Полный	Полный	Низкая	Не требуется	H/A		1511; 1607
№3	2016-0026	10/11/2016	Полный	Полный	Полный	Средняя	Не требуется	H/A	Переполнение	1511; 1607

1.5 Защита операционной системы

На данное время это понятие широко распространено в информационном мире, так как операционная система является важнейшей частью информационных технологий, поэтому отрасль защиты операционных систем стоит в приоритете у разработчиков. Понятие безопасность относится к обеспечению системы защиты ресурсов компьютера, таких как центральный процессов, память, диск, программное обеспечение, а также данные и информация, которые хранятся в компьютерной системе. Также к защите операционных систем можно подразумевать все средства и механизмы защиты данных, работающих в операционной системе. Безопасность операционной системы – это обеспечение целостности, доступности и конфиденциальности системы. Безопасность в компьютерной системе можно разделить на различные уровни, такие как поддержание физической безопасности системы, безопасность информации, которую содержит система, и безопасность сети в которой она работает. Во всех этих областях

операционная система играет жизненно важную роль в обеспечении безопасности. В общем, защита операционной системы влечет за собой защиту всех данных, приложений и от атак на операционную систему. Угрозы могут возникать умышленно или из-за ошибок со стороны людей, вредоносных программ или в связи с существующими уязвимостями. Существует множество методов защиты той или иной операционной системы, но цель одна – это обеспечение максимально безопасной работы системы для пользователя. Угрозы, которые возникают в процессе функционирования системы, делятся по приоритетам. Это означает то, что существует критические состояние системы и удовлетворительные. Операционная система со своими существующими внутренними мерами защиты осуществляет действия против угроз на систему. Меры, которые выстаивает система при обнаружении угрозы, является вполне достаточными чтобы прекратить существование нежелательных угроз.

К защите операционной системы можно отнести использование сложных паролей. Самый распространенный метод защиты операционной системы, это пароль и он должен быть сложным. Метод создания сложного пароля является вполне защищаемым и эффективным, за счет того что злоумышленнику не помогут программы, которые подбирают автоматически пароли. Пароли, состоящие из специальных символов, прочерков и пробелов, содержащих прописные буквы наряду со строчными буквами и цифрами, гораздо труднее угадать, чем имя матери или дату рождения пользователя. Также следует помнить, что при увеличении длины пароля всего на один символ, увеличивается и степень числа возможных комбинаций для подбора. В целом, пароль длинной менее 8 символом объективно считается легким для подбора. 10, 12 или 16 символов – уже гораздо лучше. Однако не стоит придумывать такие пароли, которые трудно будет запомнить или набрать.

Также к системе защиты можно отнести шифрование информации. Метод шифрования подходит для более опытных пользователей, так как этот процесс выстраивания системы защиты относится к сложнейшим методам. В этой системе защиты нужно учитывать точную информацию, по которому будут шифроваться данные, то есть пользователь должен упираться на цели и обстоятельства, при которых осуществляется защита. Данный метод может шифровать отдельные файлы так и целые разделы дисков.

Одним из методов защиты операционной системы можно также отнести резервное копирование данных. Это правило, по которому осуществляется защита любого направления в информационной системе. Резервным копированием данных может быть простой перенос данных на жесткие диски или же автоматическое копирование на сервер. На серверах, в которых хранятся резервные копии, должны быть настроены системы матрицы RAID, способные автоматически восстановить утерянную информацию. Матрица RAID, работает по такому принципу, как дублирование данных на несколько жестких дисков.

2 Меры защиты пользовательских данных на уровне операционной системы Windows

2.1 Внутренние меры защиты

Подразумевают под собой возможности защиты пользовательских данных с помощью встроенных программных обеспечении. Внутренними мерами защиты могут являться межсетевой экран, защитник Windows, парольная защита, локальные групповые политики, разграничение доступов к файлам и т.д.

Брандмауэр - это система, разработанная для предотвращения несанкционированного доступа к частной сети или из нее. Можно реализовать брандмауэр в аппаратной или программной форме, или в комбинации того и другого. Брандмауэры предотвращают доступ неавторизованных пользователей Интернета к частным сетям, подключенным к Интернету, особенно к интрасетям. Все сообщения, входящие или выходящие из интрасети, должны проходить через брандмауэр, который проверяет каждое сообщение и блокирует те, которые не соответствуют указанным критериям безопасности. Брандмауэр может обеспечить безопасность, которая сделает вас менее уязвимыми, а также защитить ваши данные от взлома или взятия ваших компьютеров в заложники.

Межсетевой экран имеет такую функцию, как фильтрация пакетов. В функции фильтрации пакетов, система проверяет каждый пакет, входящий или выходящий из сети и принимает или отклоняет его на основе пользовательских правил. Фильтрация пакетов довольно эффективна и прозрачна для пользователей, но настроить ее сложно.

Межсетевые экраны настраиваются при каждом подключении к Интернету, поэтому весь поток данных тщательно контролируется. Межсетевые экраны также могут быть настроены в соответствии с «правилами». Эти правила являются просто правилами безопасности, которые могут быть установлены пользователем или сетевыми администраторами, чтобы разрешить трафик на их веб-серверы, FTP-серверы, серверы Telnet, что дает владельцам и администраторам компьютеров огромный контроль над трафиком, который входит и выходит из их системы или сети.

Правила будут определять, кто может подключаться к Интернету, какие типы соединений можно устанавливать, какие и какие файлы можно передавать на выход. В основном весь входящий и исходящий трафик можно отслеживать и контролировать, что обеспечивает установщику брандмауэра высокий уровень безопасности и защиты.

Межсетевые экраны используют 3 типа механизмов фильтрации. Первое, это Фильтрация пакетов или чистота пакетов. Поток данных состоит из пакетов информации, и брандмауэры анализируют эти пакеты, чтобы выявить оскорбительные или нежелательные пакеты в зависимости от того, что вы определили как нежелательные пакеты. Второе, это привилегии. Брандмауэры в этом случае принимают на себя роль получателя и, в свою

очередь, отправляют его на узел, который запросил информацию, и наоборот. Третье, это проверка. В этом случае межсетевые экраны вместо просеивания всей информации в пакетах помечают ключевые функции во всех исходящих запросах и проверяют одинаковые характеристики сопоставления в притоке, чтобы решить, является ли это релевантной информацией, которая поступает.

Существует два типа межсетевого экрана: программные и аппаратные.

Программные брандмауэры. Операционные системы нового поколения поставляются со встроенными брандмауэрами, или вы можете купить программное обеспечение брандмауэра для компьютера, который подключается к Интернету или выступает в качестве шлюза к вашей домашней сети.

Аппаратные брандмауэры. Аппаратные брандмауэры обычно представляют собой маршрутизаторы со встроенной картой Ethernet и концентратором. Ваш компьютер или компьютеры в вашей сети подключаются к этому маршрутизатору и выходят в Интернет.

Групповая политика – это инструмент, доступный пользователю операционной системы Windows. Групповая политика позволяет централизованно управлять настройками компьютера , также имеет простую функцию как, распространение программного обеспечения. Групповые политики являются важным компонентом операционной системы, так как в нем расположены оснастки, с помощью которых появляется возможность оптимального администрирования своего персонального компьютера. Групповые политики позволяют настраивать параметры для определенного набора пользователей. Эффективное функционирование операционной системы невозможно без четкого разграничения доступа к ресурсам. Важным инструмент, позволяющий настраивать параметры безопасности работы пользователя в сети в операционных системах Windows, являются политики безопасности.

Групповая политика имеет следующие преимущества:

- позволяет централизованно и децентрализовано управлять параметрами политик;
- обладает гибкостью и масштабируемостью. Может быть применена в широком наборе конфигураций системы, предназначенных как для малого бизнеса, так и для больших корпораций;
- предоставляет интегрированный инструмент управления политикой с простым и хорошо понятным интерфейсом;
- обладает высокой степенью надежности и безопасности.

Несмотря на сложность построения организаций, локальные системные администраторы должны задавать, управлять и обслуживать настройки пользователей и персональных компьютеров, которые находятся в различных подразделениях, потому что в каждом отделе могут существовать свои ограничения, потребности в функционировании специализированного программного обеспечения и другое. Групповые политики предлагают достаточно обширный выбор возможностей, уменьшающих цену управления

компьютерными системами, предоставляя собой компонент операционной системы Windows, который имеет такие функции, как управление изменениями и конфигурацией пользователей и персональных компьютеров в центральной точке администрирования. Сама модуль групповой политики включает в себя инфраструктуру основанной на архитектуре «клиент - сервер», предоставляющий собой основу для обработки общих функциональных параметров административных шаблонов, а также определенных компонентов, называемых расширениями клиентской стороны. Расширения клиентской стороны интерпретирует параметры в объекте групповой политики и вносят соответствующие изменения в конфигурацию компьютера и пользователя. Такие расширения относятся ко всем основным категориям параметров политики. Другими словами, одно расширение клиентской стороны предназначено для установки программного обеспечения, другое применяет изменения безопасности, третье - обеспечивает автоматическую настройку компьютеров, подключенных к проводной сети и так далее.

Защитник Windows – встроенная антивирусная программа операционной системы Windows. Играет важную роль в безопасности системы, так как имеет функцию защиты от различного рода атак. Является базовой мерой защиты, то есть имеет ограниченные возможности в роли защитника от вредоносных программ. Служит для предотвращения появлений, помещения на карантин или удаление шпионских вредоносных модулей в операционной системе. Защитник выполняет основные действия связанные с безопасностью системы, такие как:

- отслеживание списка программ, которые автоматически запускаются при старте ОС;
- отслеживания установок ;
- слежки за компонентами и безопасностью, что связаны с Internet Explorer;
- наблюдение за обновлением компонентов Windows;
- мониторинг автозапуска программ и всех действии, которые они выполняют.

2.2 Внешние меры защиты

Внешние меры защиты пользовательских данных на уровне операционной системы. К мерам данного типа относятся антивирусы.

Антивирусная программа – это специально разработанные программные обеспечения разных производств для защиты от вирусов. Целью антивирусных программных обеспечении являются обезопасить компьютеры. Антивирусы играют важную роль в функционировании операционных систем. Программные обеспечения против вирусов могут обнаруживать компьютерные вирусы и восстанавливать зараженные файлы. На данный момент антивирусное программное обеспечение разрабатывается в основном для Windows, что вызвало большим количеством вредоносных программ

именно под эту платформу. Также разрабатываются и для операционных систем Linux и Mac OS. Это вызвано тем, что появилось ряд распространений вредоносных программ под эти платформы.

Классифицировать антивирусные продукты можно сразу по нескольким признакам, таким как: используемые технологии антивирусной защиты, функционал продуктов, целевые платформы.

По используемым технологиям антивирусной защиты:

- классические антивирусные продукты;
- продукты проактивной антивирусной защиты;
- комбинированные продукты.

По функционалу продуктов:

- антивирусные продукты (продукты обеспечивающие только антивирусную защиту);
- комбинированные продукты (продукты, обеспечивающие не только защиту от вредоносных программ, но и фильтрацию спама, шифрование, резервное копирование данных и другие функции).

По целевым платформам:

- антивирусные продукты для ОС семейства Windows;
- антивирусные продукты для защиты рабочих станций;
- антивирусные продукты для защиты файловых и терминальных серверов; антивирусные продукты для защиты почтовых и Интернет-шлюзов;
- антивирусные продукты для защиты серверов виртуализации.

Для использования антивирусов необходимы постоянные обновления так называемых баз антивирусов. Они представляют собой информацию о вирусах – как их найти и обезвредить. Поскольку вирусы пишут часто, то необходим постоянный мониторинг активности вирусов в сети. Для этого существуют специальные сети, которые собирают соответствующую информацию .

Для того чтобы антивирус функционировал, нужны постоянные обновления так называемых баз антивирусов. В свою очередь они представляют собой данные о вирусах – как их найти и обезвредить. Учитывая факт того, что вирусы пишутся в большом количестве, то соответственно нужно постоянно следить за активностью вирусов в сети. Специально для этого существуют специальные сети, которые собирают соответствующую информацию. После сбора этой информации производится анализ вредоносности вируса, анализируется его код, поведение, и после этого устанавливаются способы борьбы с ним. Чаще всего вирусы запускаются вместе с операционной системой. В таком случае можно просто удалить строки запуска вируса из реестра, и на этом в простом случае процесс может закончиться. Более сложные вирусы используют возможность заражения файлов. Например, известны случаи, как некие даже антивирусные программы, будучи зараженными, сами становились причиной заражения других чистых программ и файлов.

3 Проектирование и конфигурация защиты пользовательских данных на уровне операционной системы

3.1 Постановка задачи

Проектируя систему защиты пользовательских данных, важно поставить правильно перед собой следующие задачи:

- ознакомиться с технологиями защиты пользовательских данных;
- выявить уязвимости операционной системы;
- изучить внутренние возможности операционной системы для защиты;
- изучить внешние возможности операционной системы для защиты;
- сформулировать требования по безопасности;
- реализовать защиту пользовательских данных.

3.2 Требования к проектированию защиты пользовательских данных

Проектируемая система защиты пользовательских данных должна обеспечить защиту пользователя в системе, система которой будет установлена на виртуальной сети. Также должна обеспечить конфиденциальность, целостность и доступность.

Система защиты должна выполнять следующие функции:

- обеспечить безопасность конфиденциальных пользовательских данных на уровне операционной системы;
- обеспечить защиту несанкционированного доступа;
- защитить систему от атак из Интернета;
- мониторинг операционной системы.

Как правило большинство организации при обеспечении безопасности информационных систем затраты на безопасность не могут превышать экономические потери, т.е. ущерб от реализации возможных угроз безопасности. В связи с этим, я использовал бесплатные возможности для реализации практической части дипломной работы.

В качестве рекомендаций по дальнейшей оптимизации системы, я предлагаю рассмотреть приобретение UTM-решения – универсальный шлюз безопасности, объединяющий в себя функции межсетевого экрана, антивируса, системы обнаружения и предотвращения вторжений, системы глубокой проверки пакетов.

3.3 Объект защиты

Объектом защиты является операционная система, разворачиваемая на виртуальной машине Vmware Workstation Pro, установленная на моем персональном компьютере. Система защиты развернута на групповых политиках операционной системы Windows Server 2012 в доменном редакторе групповых политик. Разделы по которым можно разделить групповые политики таковы: политики учетных записей; локальные политики; брандмауэр Windows в режиме повышенной безопасности; политика

открытого ключа; политика диспетчера списка сетей; политика ограниченного использования программ; политика управления приложениями.

Раздел политики учетных записей управляет политиками паролей и политиками блокировки учетных записей. Политики учетных записей служат важным инструментом в установлении системной безопасности пользователя.

Раздел локальных политик управляет политиками аудита, назначением прав пользователю и параметрами безопасности. В локальных политиках достаточно широкий выбор политик для того, чтобы система работала как в режиме мониторинга, так и в режиме безопасности.

Раздел политики управления приложениями включает в себя функцию AppLocker. С помощью компонента AppLocker можно указать, какие пользователи и группы в организации могут запускать определенные приложения.

3.4 Настройка Active Directory

Сеть располагается на территории виртуальной машины «VMware workstation» и включает в себя две установленные операционные системы:

- Windows 10;
- Windows server 2012.

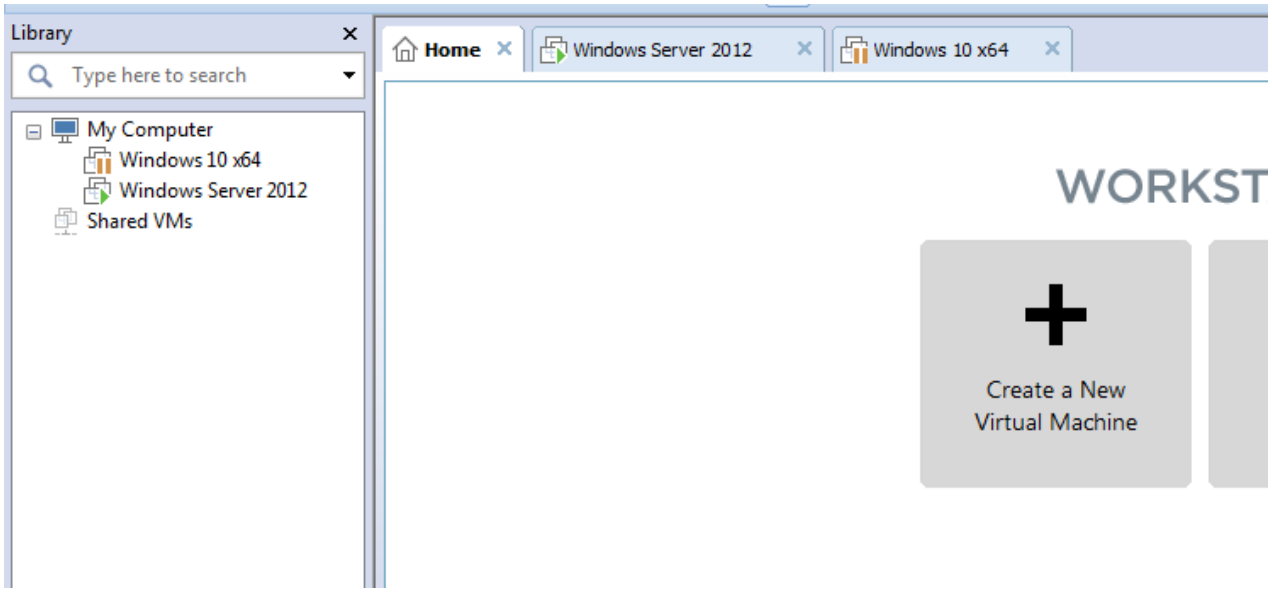


Рисунок 3.1 – Установленные операционные системы

3.4.1 Разворачивание корпоративной сети

В установленной операционной системе Windows Server 2012, был установлен корпоративный домен. В системе нужны базовые установки ролей и компонентов, одна из важных это служба домена. Active Directory, служит для хранения и организации объектов в сети в иерархическую защищенную логическую структуру. Существует ряд подкаталогов основного каталога, они служат вспомогательными инструментами для администратора.

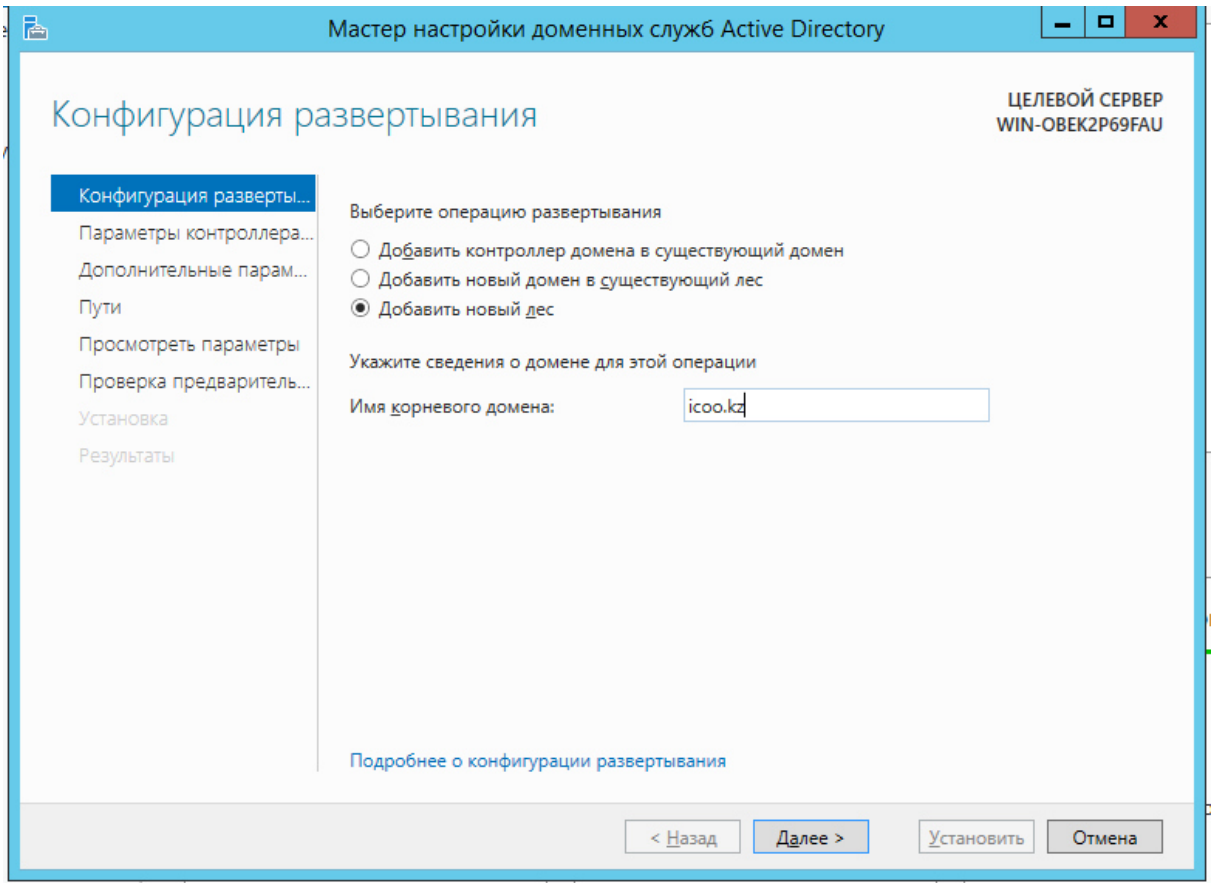


Рисунок 3.2 – Установка домена icoo.kz

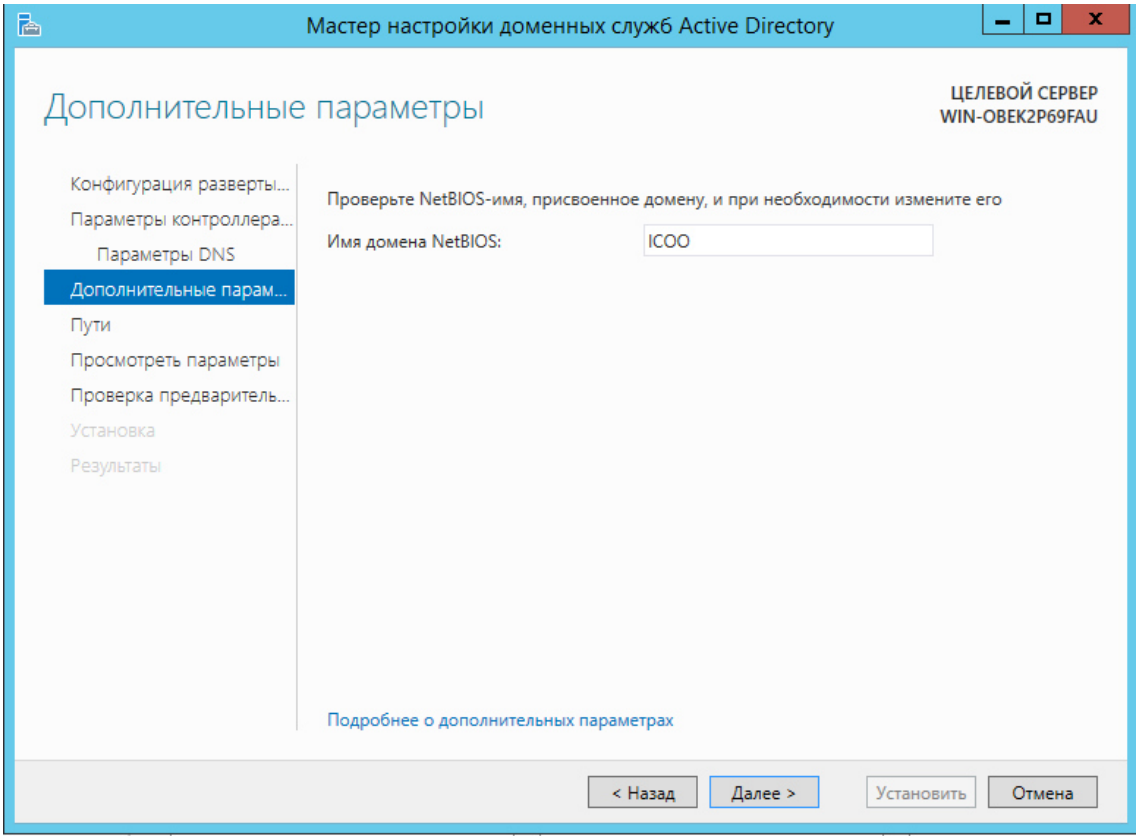


Рисунок 3.3 – Имя домена NetBIOS: ICOO

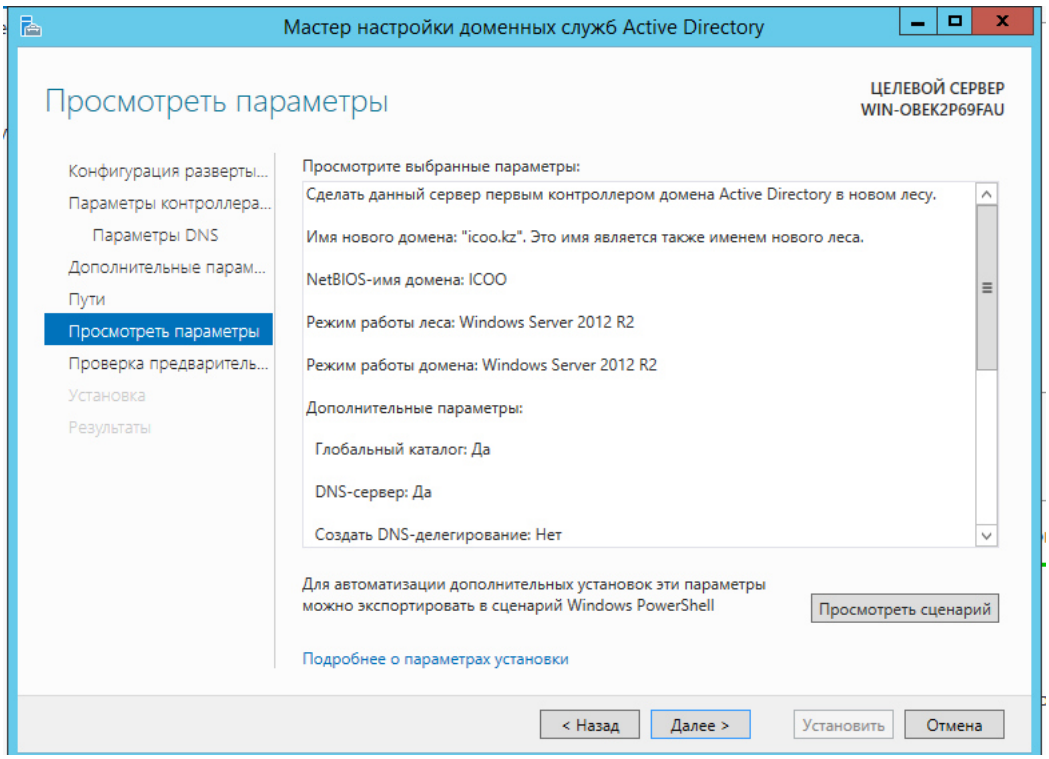


Рисунок 3.4 – Завершение установки корпоративного домена

3.4.2 Контроллер домена

Контроллер домена является сервером, который отвечает за вопросы аутентификации и проверяет пользователей в компьютерных сетях. В добавлении к контроллеру домена можно сказать, что это ящик, в котором находятся ключи к Active Directory. Основная функция контроллера домена состоит в том, что когда пользователи входили в свой домен, контроллер домена проверял их имя пользователя, пароль и другие учетные данные, чтобы разрешить или запретить доступ для этого пользователя.

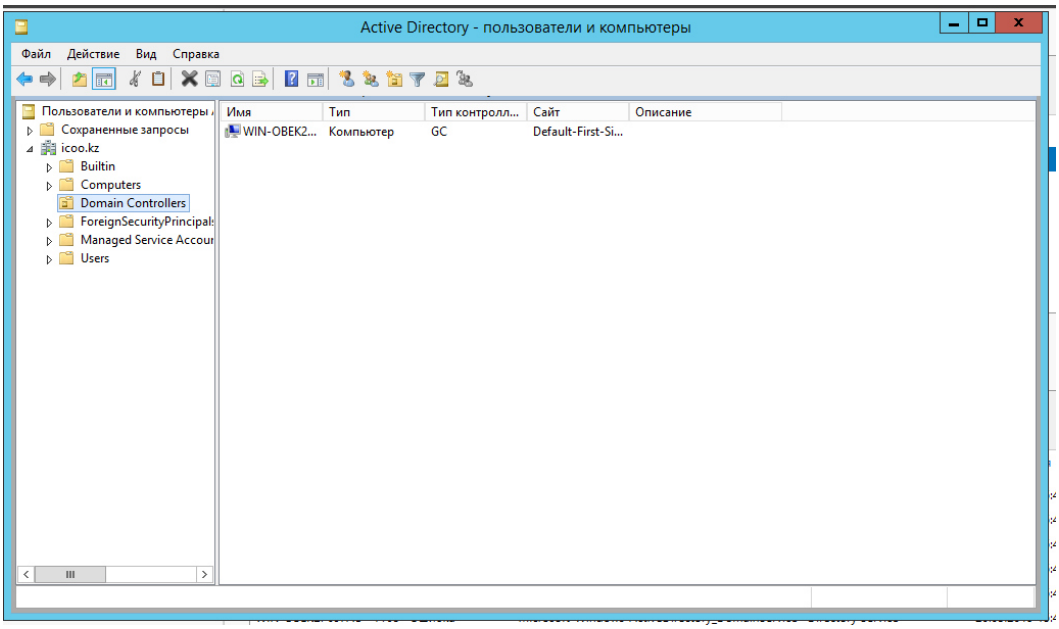


Рисунок 3.5 – Контроллер домена является WIN-OBEK2P69FAU

3.4.3 Подразделения организации

В организации имеются базовые подразделения, которые в совокупности составляют основную часть организации. Подразделения являются неотъемлемой частью всех компании. Так как в корпоративной сети должна быть структура всего, подразделения один из инструментов в структуре. В домене, были созданы четыре подразделения это: бухгалтерия, IT-отдел, разработка, продажа. В каждом подразделении имеются свои группы. Группы делятся по сфере деятельности каждого сотрудника организации. Группы созданные в бухгалтерии: заработная плата, налоги, банковская система. Группы созданные в IT-отделе: кибербезопасность, helpdesk, системные администраторы. Группы созданные в разработке: программы на телефоны, сайты, программы на ПК. Группы созданные в продаже: программы, сайт, оборудование.

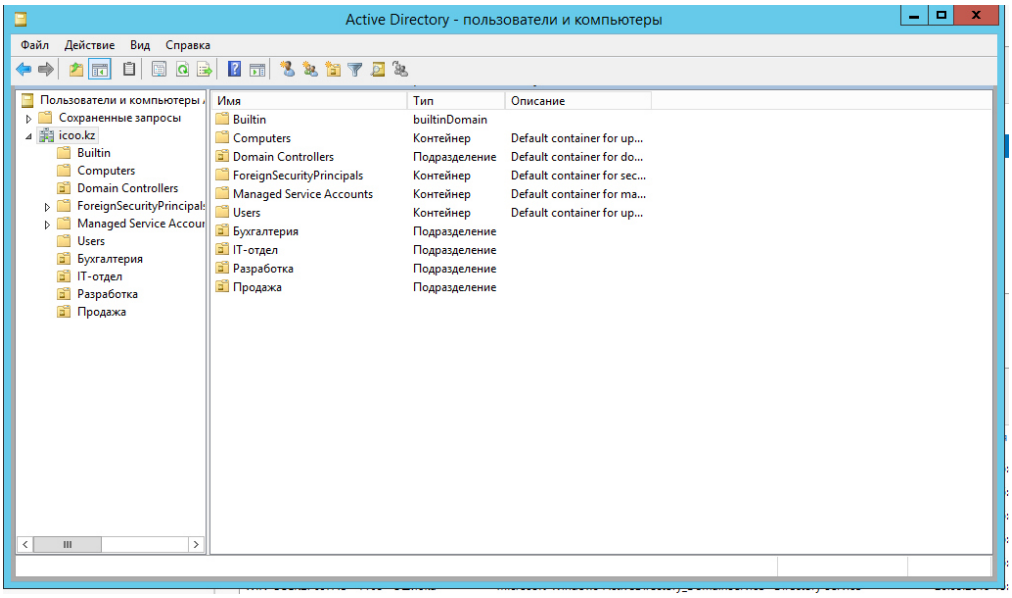


Рисунок 3.6 – Подразделения

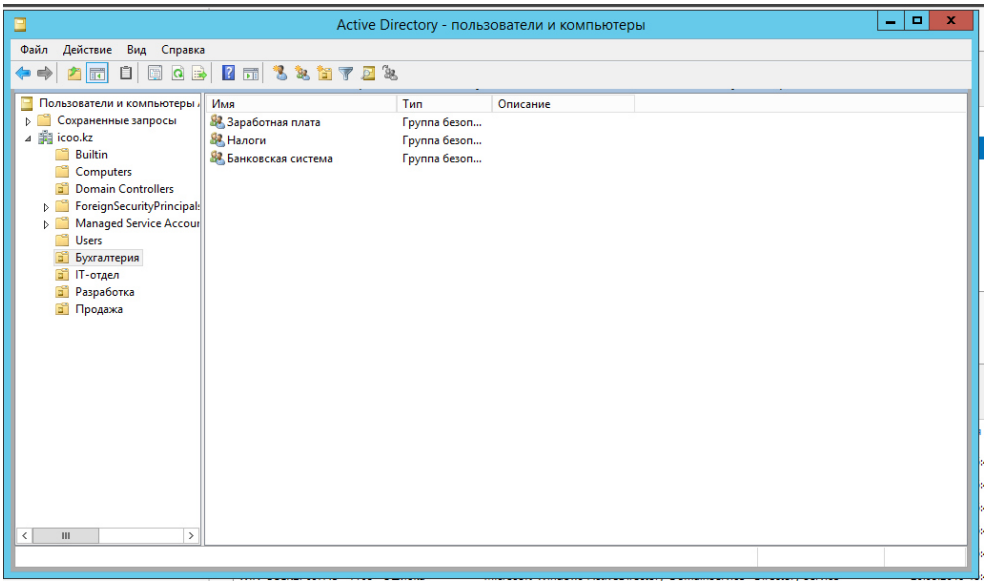


Рисунок 3.7 – Группы в бухгалтерии

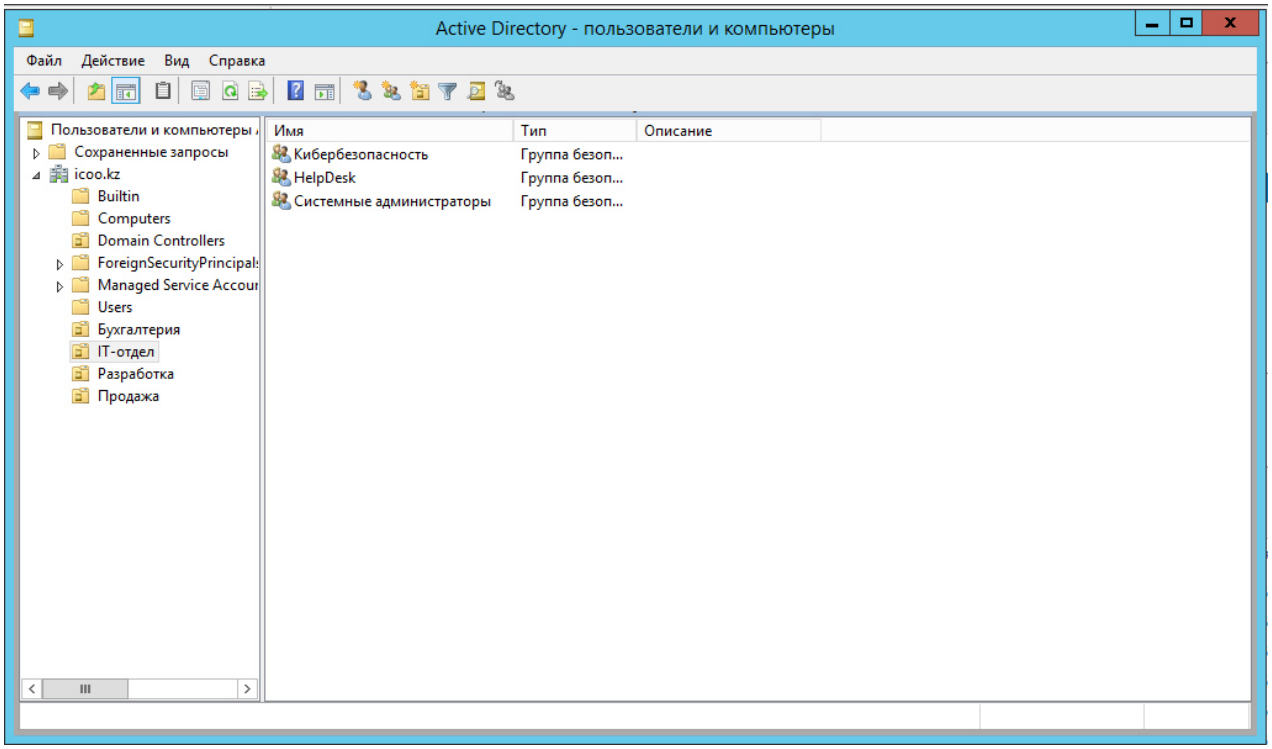


Рисунок 3.8 – Группы в IT-отделе

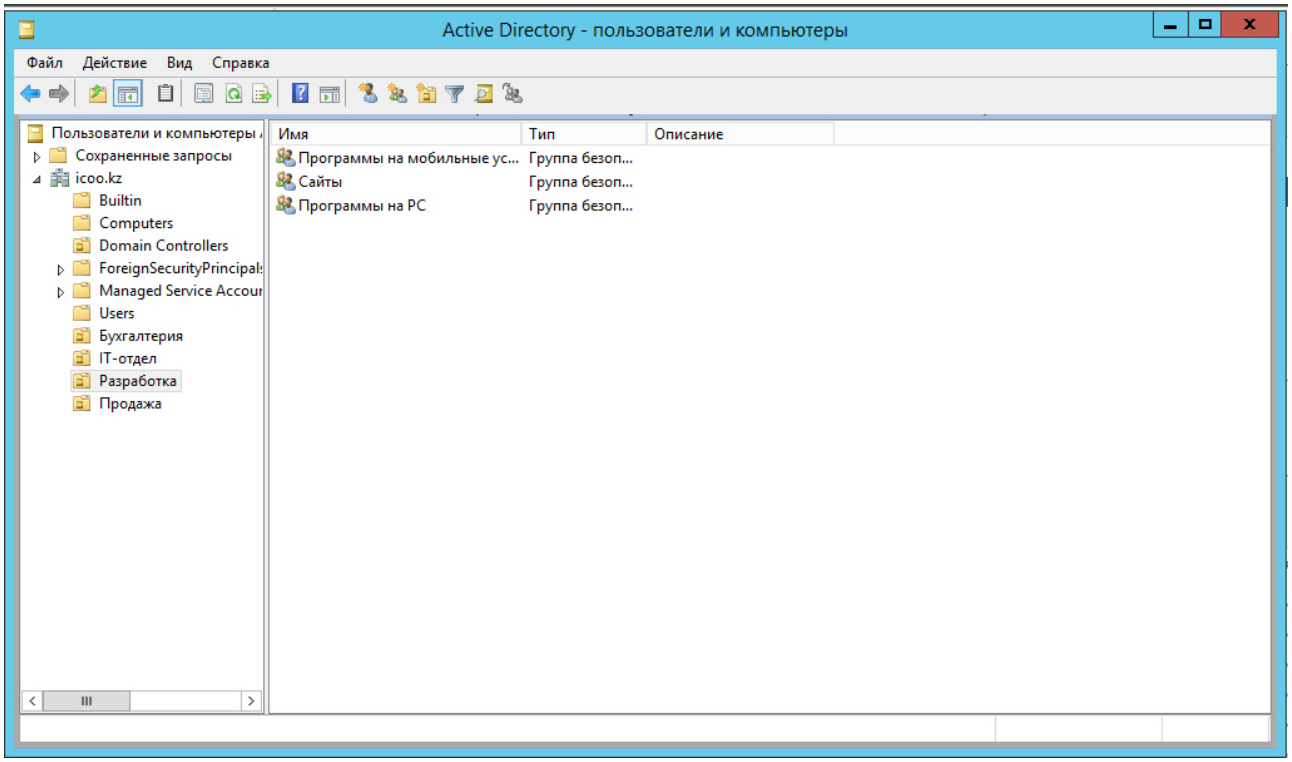


Рисунок 3.9 – Группы в разработке

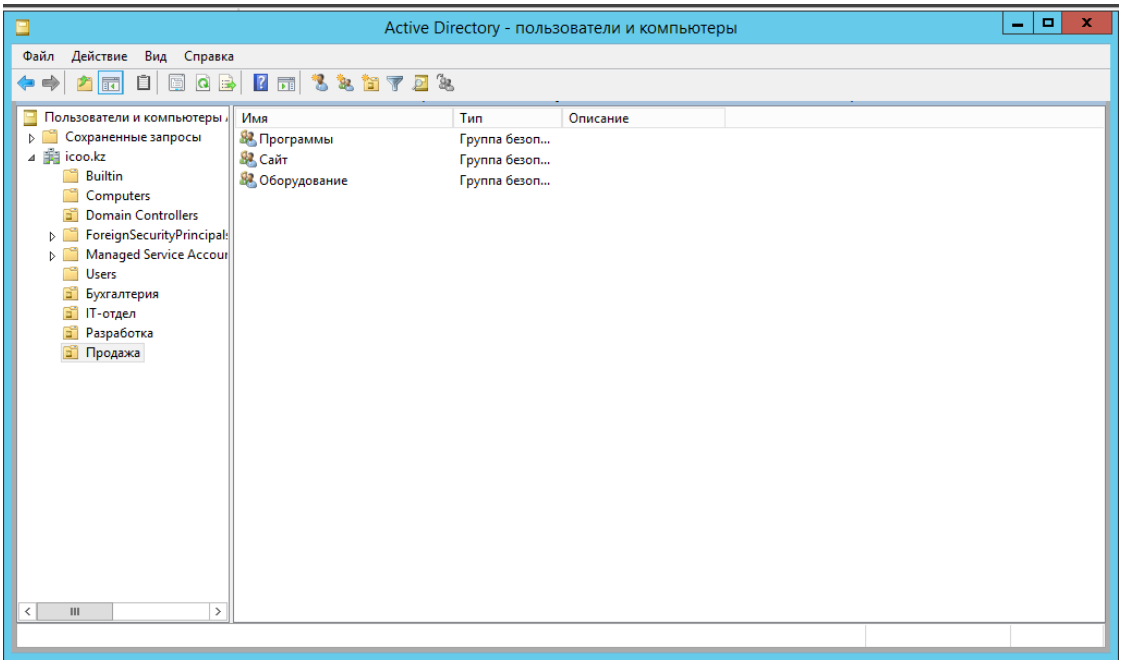
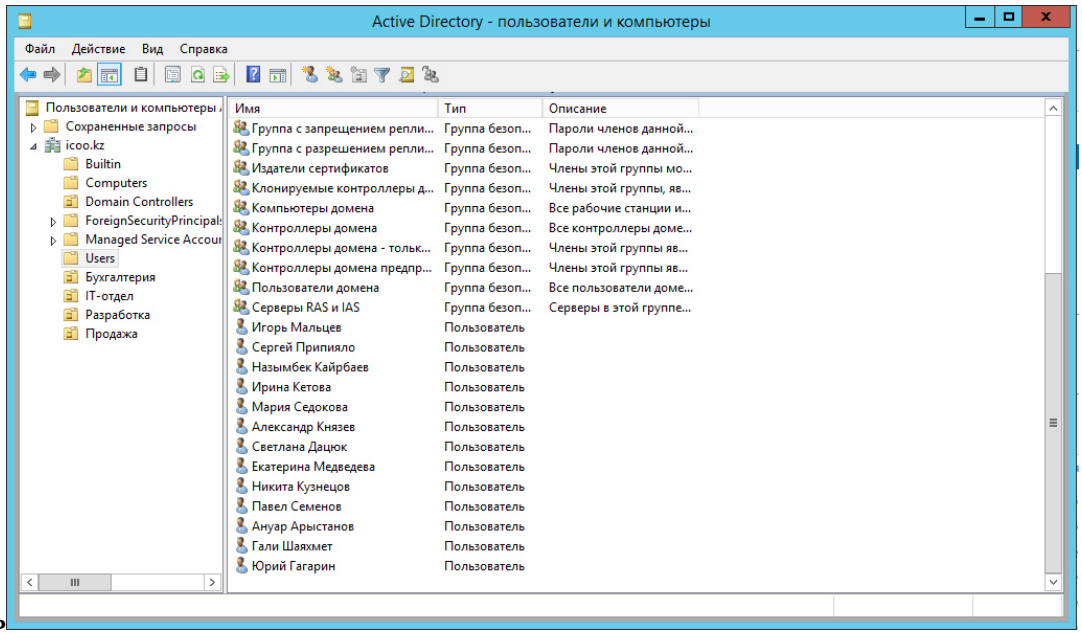


Рисунок 3.10 – Группы в продаже

3.4.4 Пользователи домена

Пользователи создаются с оснастке Active Directory пользователи и компьютеры. Пользователь при создании является часть системы домена. Создаются пользователи исключительно администраторами домена. При создании пользователя указываются данные человека. К числу данных относят имя, фамилия человека. В процессе создания также необходимо установить логин учетной записи для пользователя, так как с помощью него пользователь будет логиниться. В созданном пользователе, есть такие возможности, как: добавления прав пользователю, телефона, почты, указание периода времени использования учетной записи и так далее.



Ъ

Рисунок 3.11 – Пользователи домена

3.4.5 DNS

DNS является системой доменных имен, которая позволяет по доменному имени узнать IP хоста и наоборот. Так как, у каждого компьютера или сетевого устройства есть свой IP адрес, и для того, чтобы обратиться к тому или иному компьютеру или устройству соответственно нужно знать этот IP адрес. В моей оснастке выводится имя компьютера контроллера домена, который и является основной зоной для DNS. Домен, который находится в контроллере домена icoo.kz, имеет зону с IP адресом: 192.168.10. После добавления зоны, выводятся все компьютеры, которые включены в домен. В данном случае вывелся компьютер под именем DESKTOP-G1D2L62H, со своим IP адресом: 192.168.10.130.

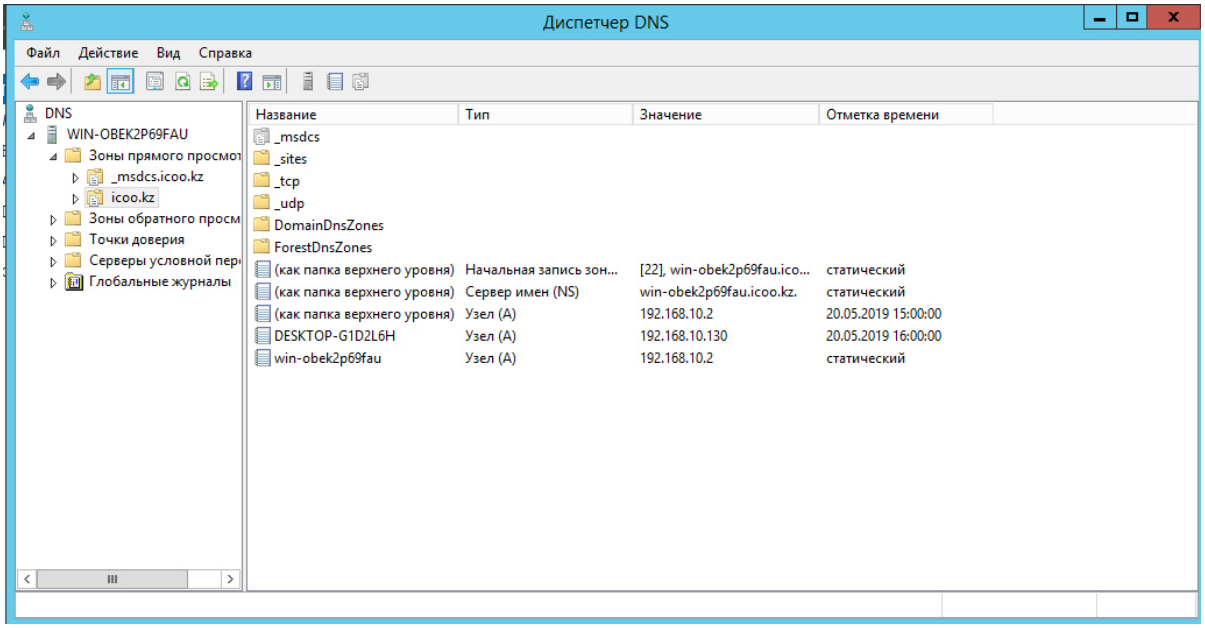


Рисунок 3.12 - DNS

3.4.6 DHCP

DHCP является протоколом, отвечающим за динамическую настройку узла сети с использованием модели OSI. DHCP дает возможность автоматически настроить IPv4 и исключить из процесса управления параметрами сети человеческий фактор. В данном случае компьютер, который был подключен к домену получил IP: 192.168.10.130.

Служба DHCP-сервера - последняя реализация современной автоматизированной сетевой адресации. Она может выполнять все те же функции, что и служба BOOTP, но может также предоставить дополнительную информацию клиентам, которые запрашивают IP-адрес.

Сервер DHCP выдает клиенту IP-адрес с помощью трехшаговой процедуры.

1. Клиент DHCP загружается и рассылает DHCP-запрос на IP-адрес всем узлам в локальной сети.

2. DHCP-сервер в локальной сети получает запрос и готовится к отправке IP-адреса этому клиенту в виде DHCP-аренды IP-адреса.

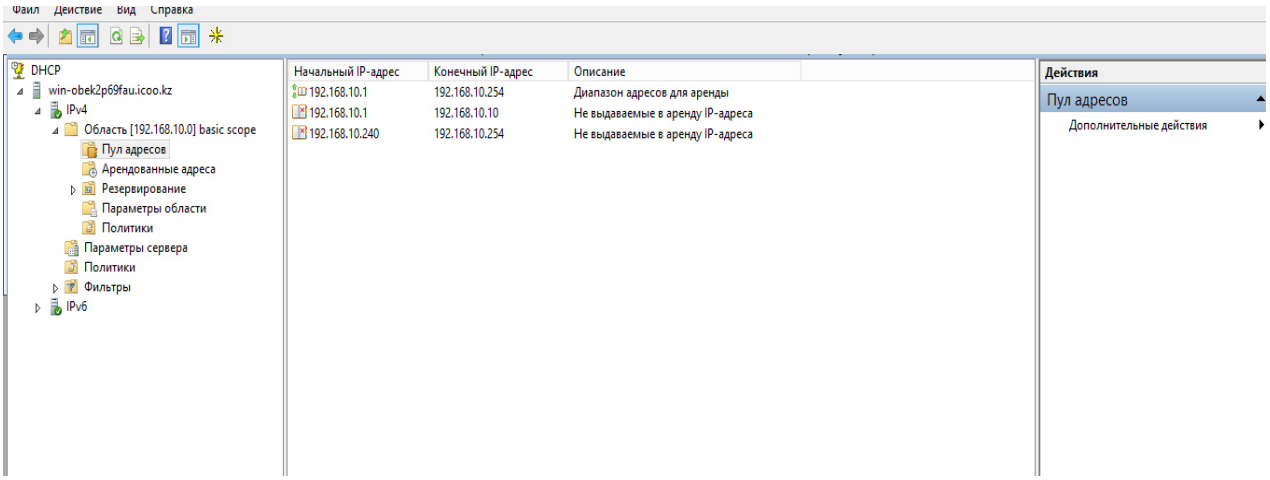


Рисунок 3.13 – DHCP

3.4.7 Добавление компьютера в домена

Добавление компьютера является легким процессом. Целью является то, что компьютер после добавления является частью домена и управление может переходить администратору домена. Для добавления необходимо знать IP-адрес DNS-сервера, в данном случае был: 192.168.10.2. Также в процессе регистрации компьютера необходим администратор с паролем. После чего он добавляется в домен.

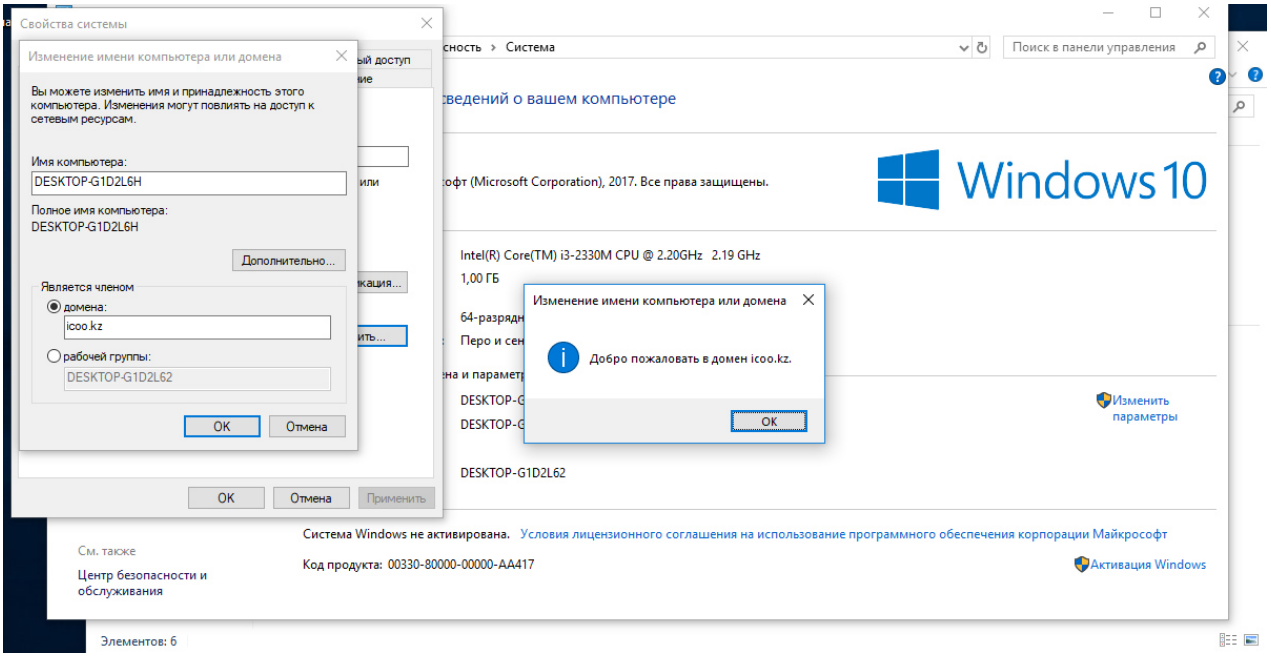


Рисунок 3.14 – Успешное добавление компьютера в icoo.kz

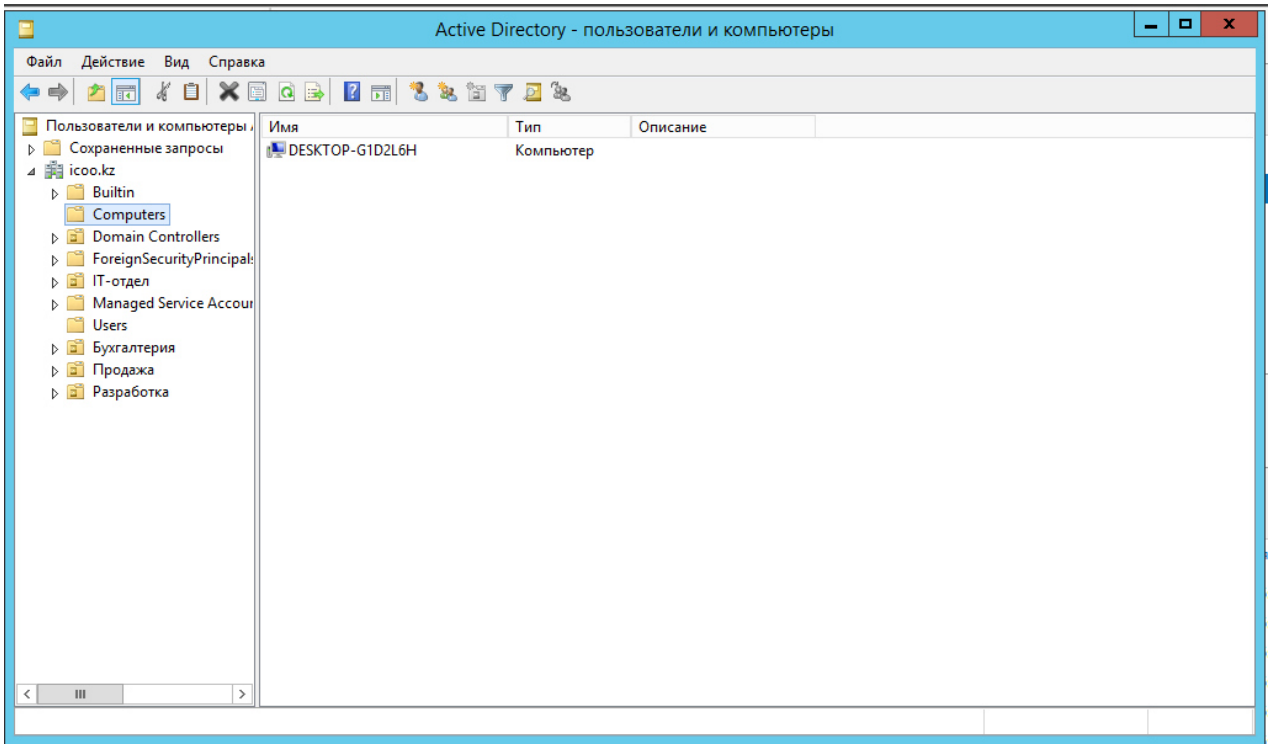


Рисунок 3.15 – Контроллер домена

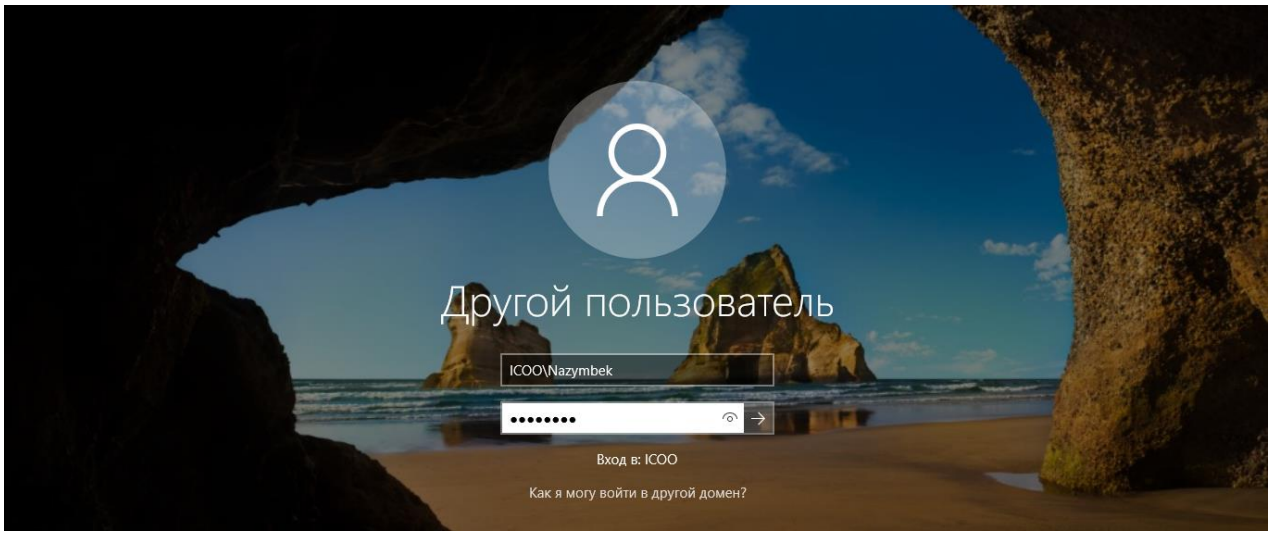


Рисунок 3.16 – Авторизация

3.5 Групповые политики Windows Server 2012

Групповые политики - технология, обеспечивающая механизм, используя который администраторы локальных компьютеров и доменных служб Active Directory могут централизованно развертывать и управлять настройками пользователей и компьютеров в организации. Инфраструктура групповой политики основана на архитектуре «клиент-сервер» с компонентами клиента и сервера и включает в себя модуль групповой политики, представляющий собой основу для обработки общих функциональных параметров административных шаблонов, а также определенных компонентов, называемых расширениями клиентской стороны.

Типы параметров групповой политики: управляемые параметры политики; неуправляемые параметры политики. Управляемые параметры политики влияют на тип изменения конфигурации при применении параметра объекта групповой политики. Неуправляемые параметры политики также вносят изменения в реестр, но, в отличие от управляемых параметров политики, при помощи этого типа настроек, после развертывания таких политик, вы позволяете пользователям изменять их настройки.

В корпоративной сети, а именно в домене icoo.kz, была установлена оснастка групповых политик. В управлении групповых политик имеются подразделения организации, к которым будут применяться настройки параметром политик. По умолчанию существует серверные встроенные политики. Прежде чем настраивать политики создается объект групповой политики, который будет относится ко всем подразделениям организации. Был создан объект под названием: групповые политики для icoo.kz.

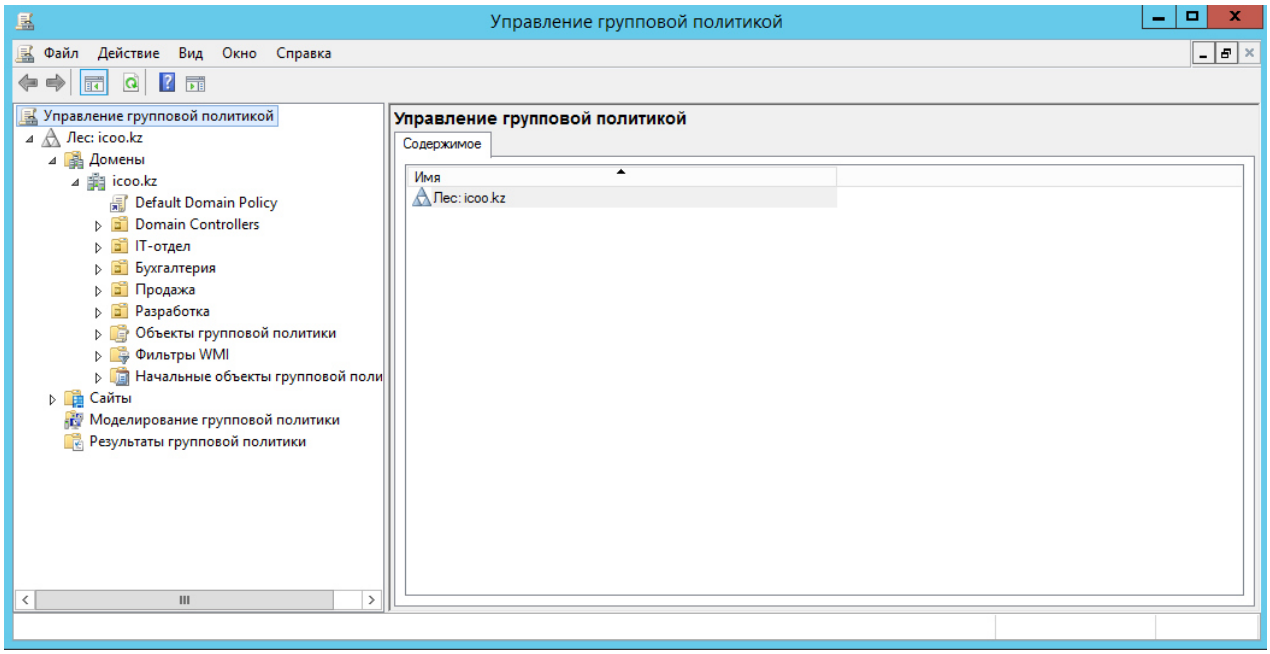


Рисунок 3.17 – Оснастка групповых политик

Объект групповой политики (Group Policy Object, GPO) состоит из двух физически раздельных составляющих: контейнера групповой политики (Group Policy Container, GPC) и шаблона групповой политики (Group Policy Template, GPT). Эти два компонента содержат в себе всю информацию о параметрах рабочей среды, которая включается в состав объекта групповой политики. Продуманное применение объектов GPO к объектам каталога Active Directory позволяет создавать эффективную и легко управляемую компьютерную рабочую среду на базе ОС Windows. Политики применяются сверху вниз по иерархии каталога Active Directory .

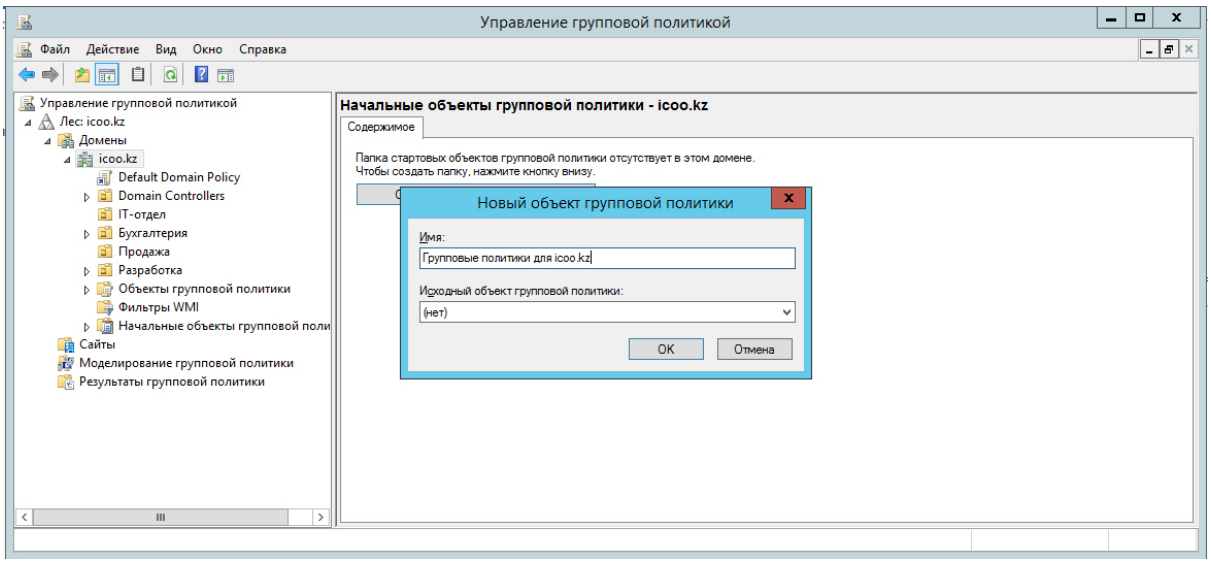


Рисунок 3.18 – Создание объекта

Политика учетных записей включает в себя политику паролей и политику блокировки учетных записей.

В политике паролей были рассмотрены такие политики как: минимальная длина пароля, пароль должен соответствовать сложностям.

В политике блокировки учетных записей были рассмотрены такие политики как: пороговое значение блокировки, продолжительность блокировки учетных записей.

3.5.1 Минимальная длина пароля

Минимальная длина пароля это политика, которая определяет минимальное количество знаков, которое должно содержаться в пароле пользователя.

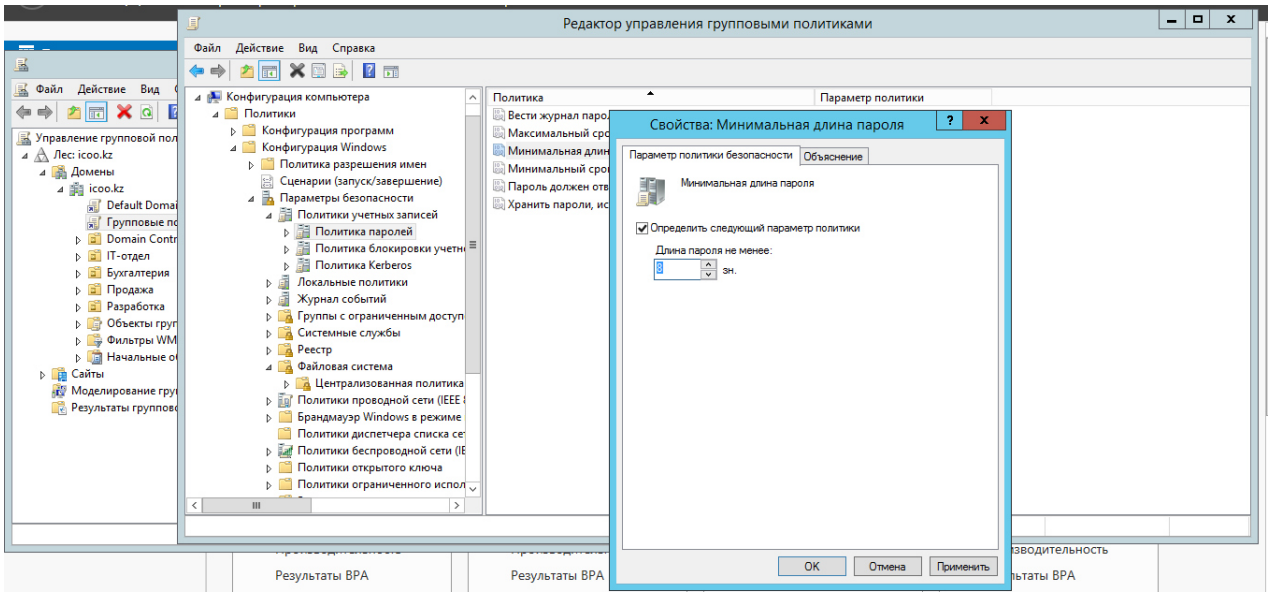


Рисунок 3.19 – Выставляется минимальная длина пароля 8

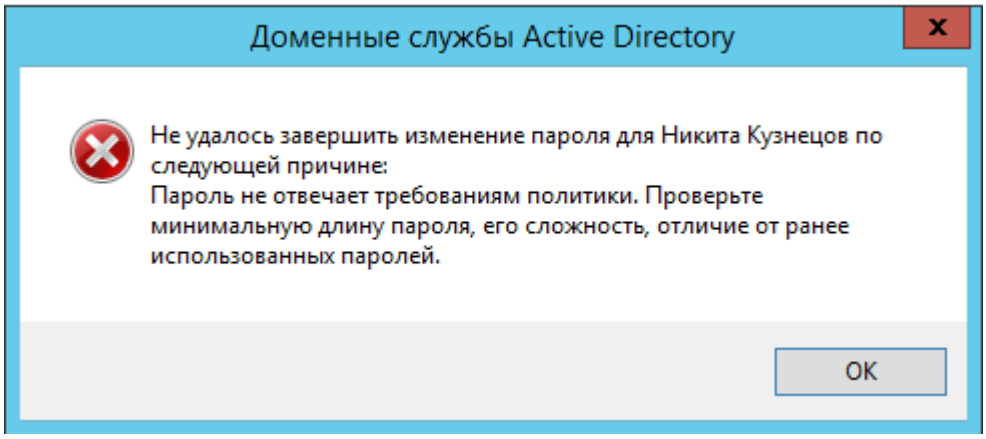


Рисунок 3.20 – Ошибка в запросе на установление пароля меньше 8

3.5.2 Политика сложного пароля

Политика пароля, которое должно отвечать требованиям сложности. Эта политика относится к параметрам безопасности, которая определяет должен ли пароль отвечать требованиям сложности. Если эта политика включена, пароли должны удовлетворять следующим минимальным требованиям.

- Не содержать имени учетной записи пользователя или частей полного имени пользователя длиной более двух рядом стоящих знаков;
- иметь длину не менее шести знаков;
- содержать знаки трех или четырех перечисленных ниже категорий: латинские заглавные буквы, латинские строчные буквы, цифры, отличающиеся от букв и цифр.

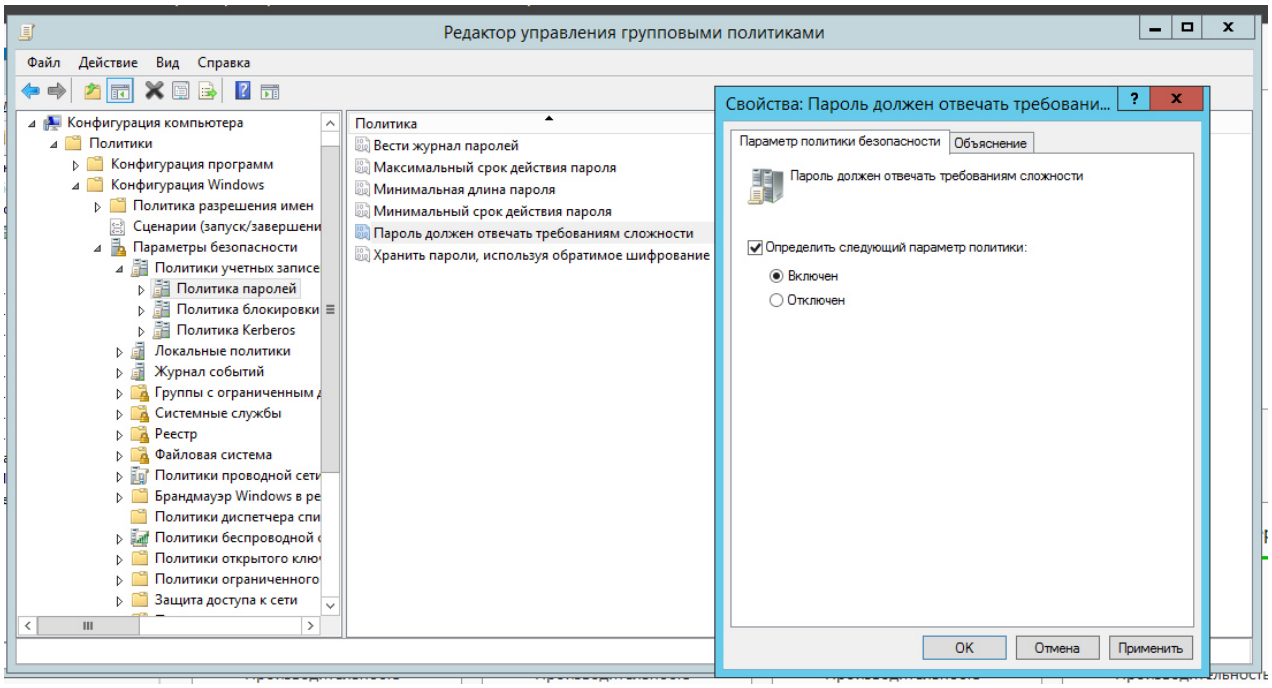


Рисунок 3.21 – Применения сложного пароля

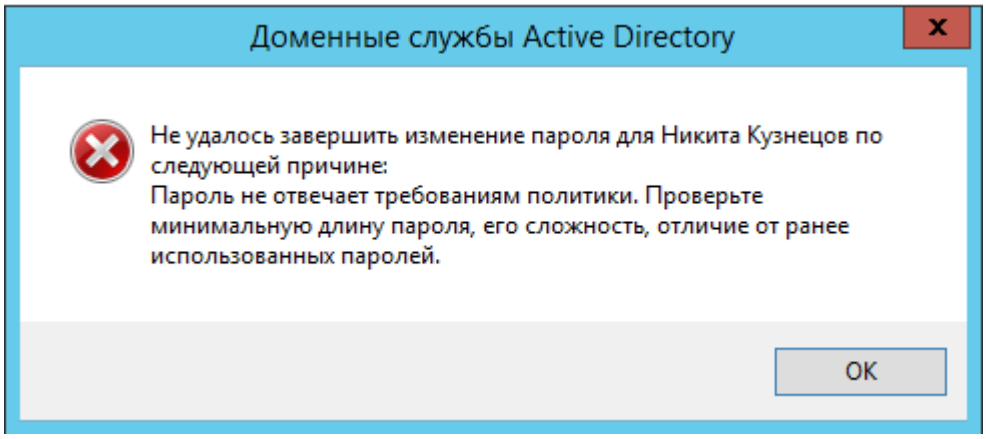


Рисунок 3.22 – Ошибка в запросе на установление легкого пароля

3.5.3 Политика блокировки учетной записи

Политика блокировки учетной записи при неправильном вводе пароля. Этот параметр безопасности определят количество неудачных попыток входа в систему, приводящее к блокировке учетной записи пользователя. Заблокированная учетная запись не может использоваться до тех пор, пока не будет сброшена администратором, либо пока не истечет период блокировки учетной записи. Количество неудачных попыток входа в систему может составлять от 0 до 999. Если установить это значение равным 0, то учетная запись никогда не будет разблокирована. Неудачные попытки ввода паролей на рабочих станциях или серверах-членах домена, заблокированных с помощью клавиш CTRL+ALT+DELETE или с помощью защищенных паролем заставок, считаются неудачными попытками входа в систему.

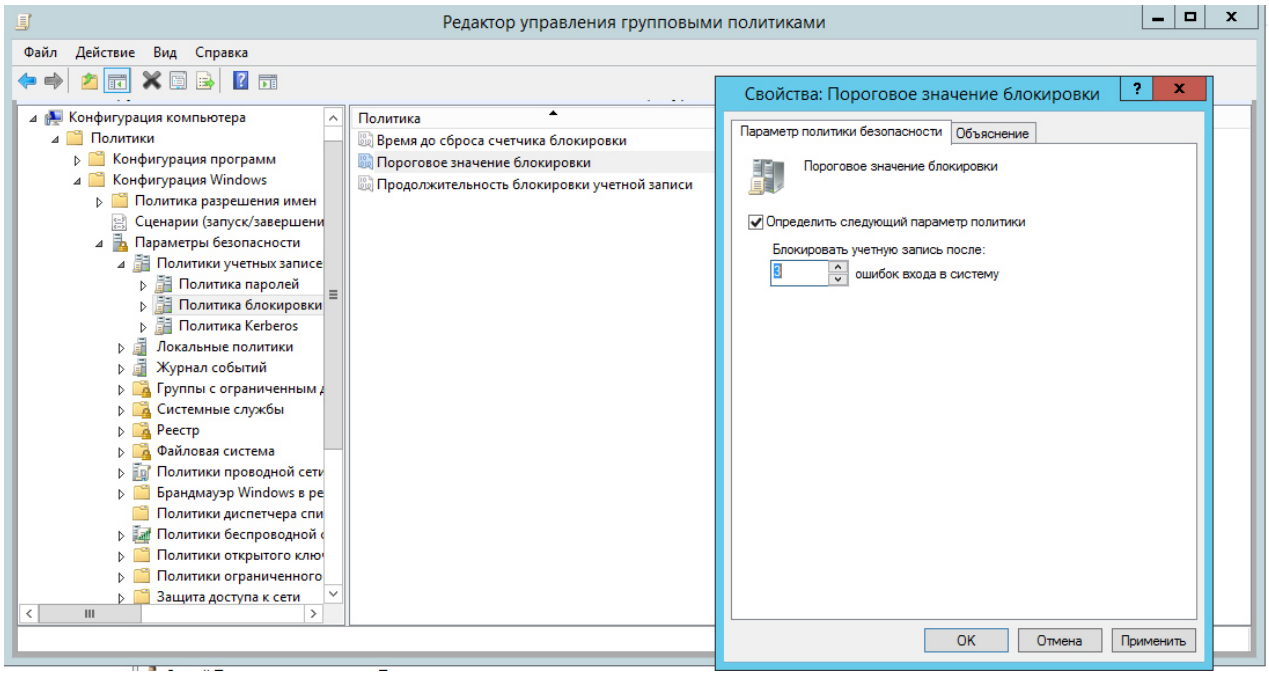


Рисунок 3.23 – Блокирование учетной записи после 3 ошибок

3.5.4 Политика продолжительности блокировки учетной записи

Политика продолжительности блокировки учетной записи. Этот параметр безопасности определяет количество минут, в течении которых учетная запись остается заблокированной до ее автоматической разблокировки. Допустимые значения от: 0 до 99999 минут. Если продолжительность блокировки учетной записи равна 0, то учетная запись будет заблокирована до тех пор, пока администратор не разблокирует ее. Если определено пороговое значение блокировки учетной записи, то длительность блокировки учетной записи должна быть больше или равна времени сброса.

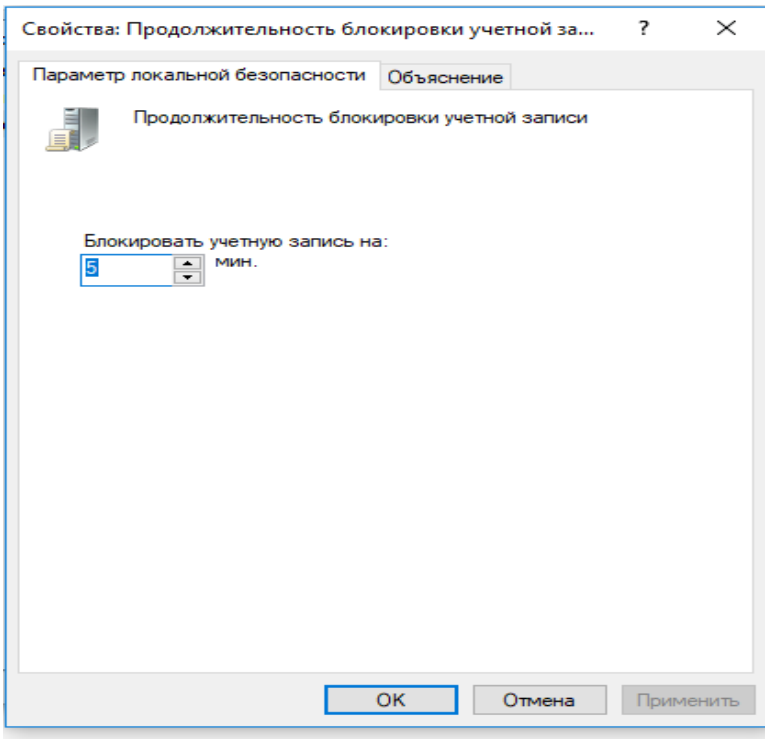


Рисунок 3.24 – Время блокировки учетной записи при заблокированном состоянии

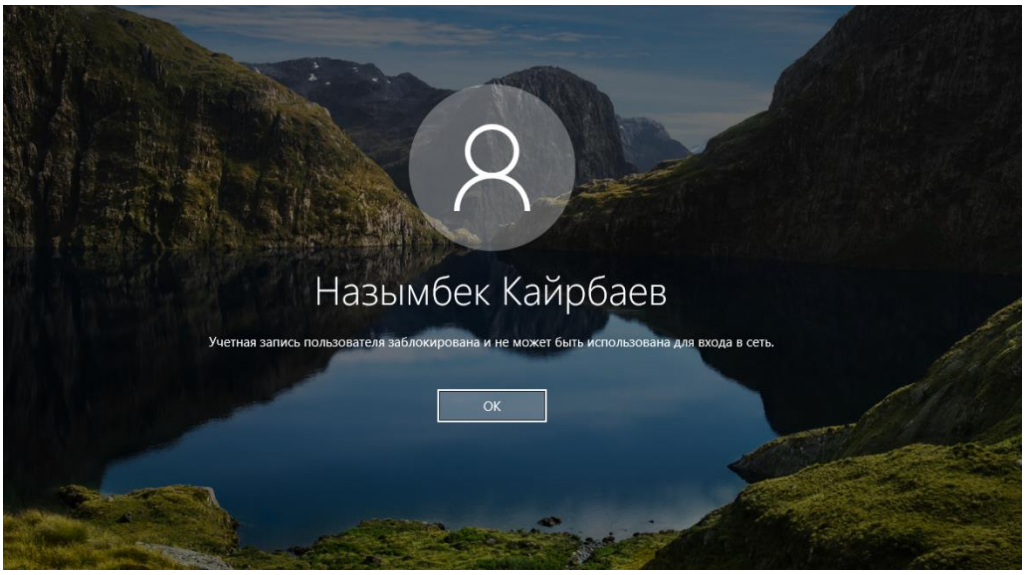


Рисунок 3.25 – Заблокированный пользователь

3.5.5 Политика аудита

Политика аудита входа в систему. Этот параметр безопасности определяет, будет ли операционная система выполнять аудит каждой попытки входа пользователя в систему или выхода из нее на данном компьютере. События входа из системы создаются каждый раз, когда завершается сеанс вошедший в систему учетной записи пользователя. Если этот параметр политики задан, то администратор может указать, какие события подвергаются аудиту: только об успешном выполнении, только об ошибках, те и другие.

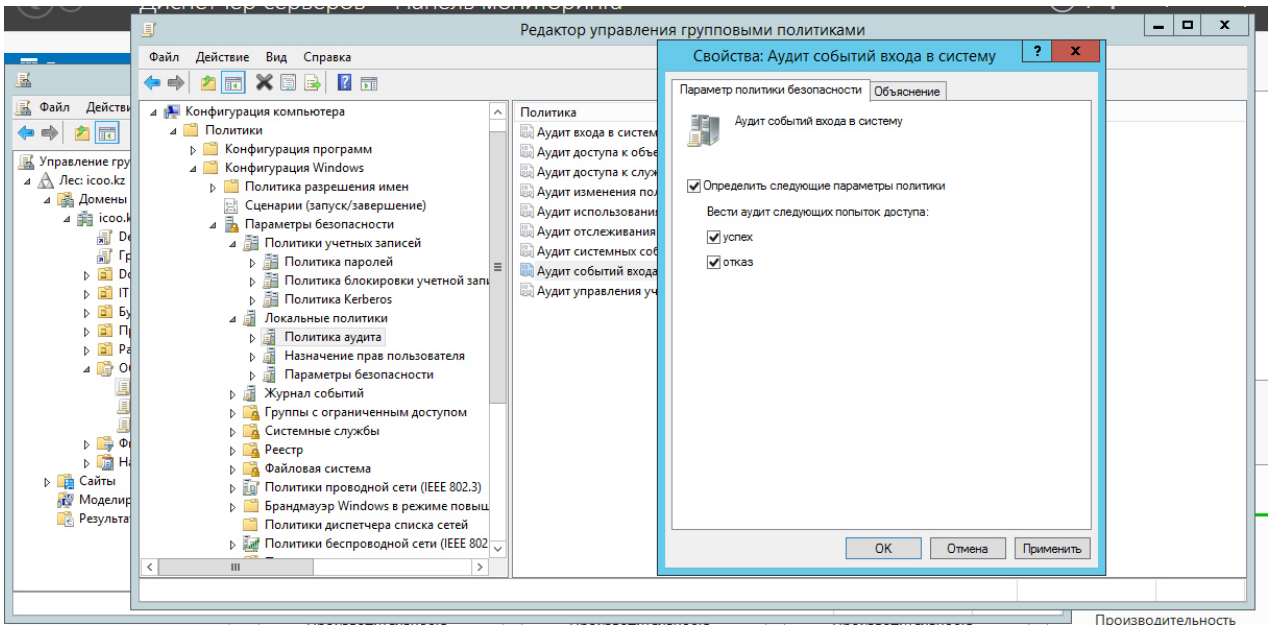


Рисунок 3.26 – Применение политики

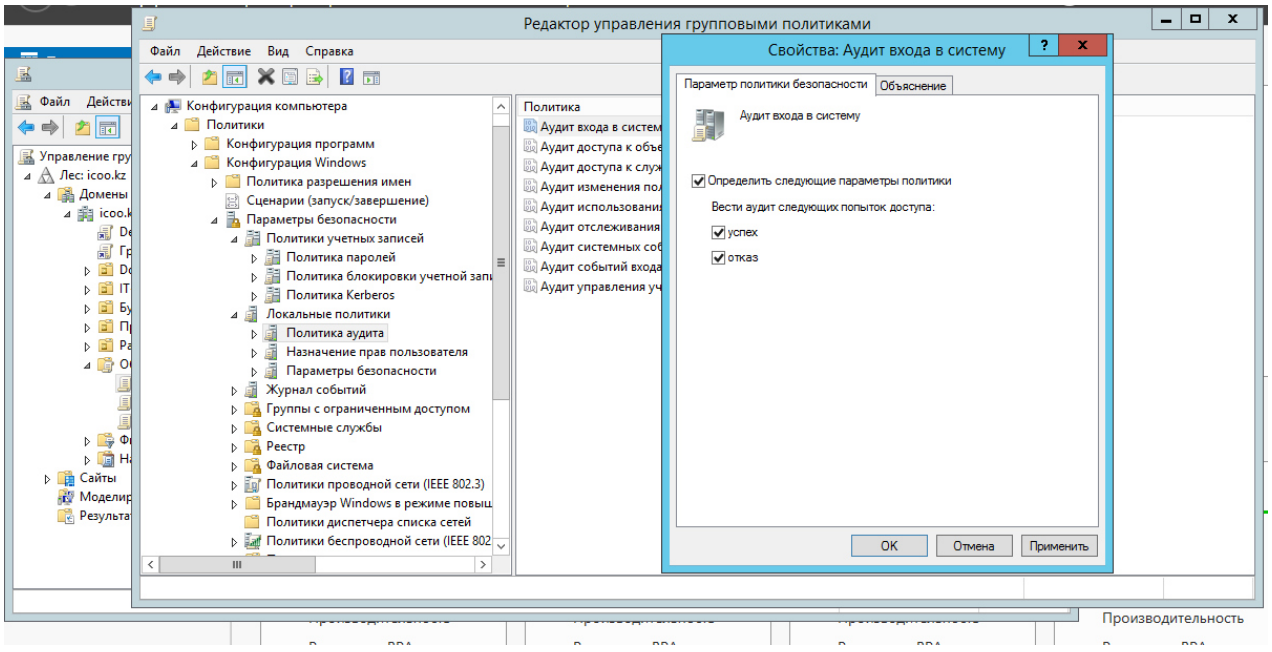


Рисунок 3.27 – Применение политики

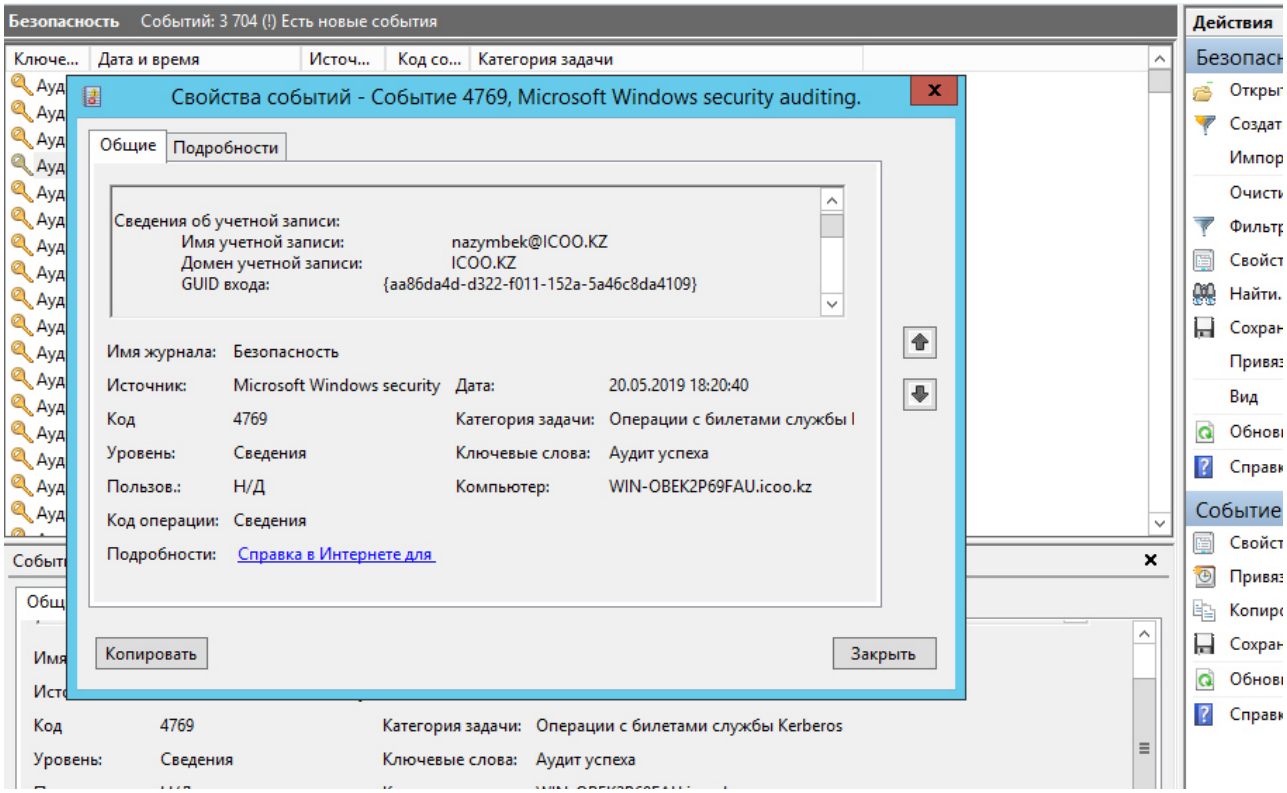


Рисунок 3.28 – Журнал входа и выхода из системы

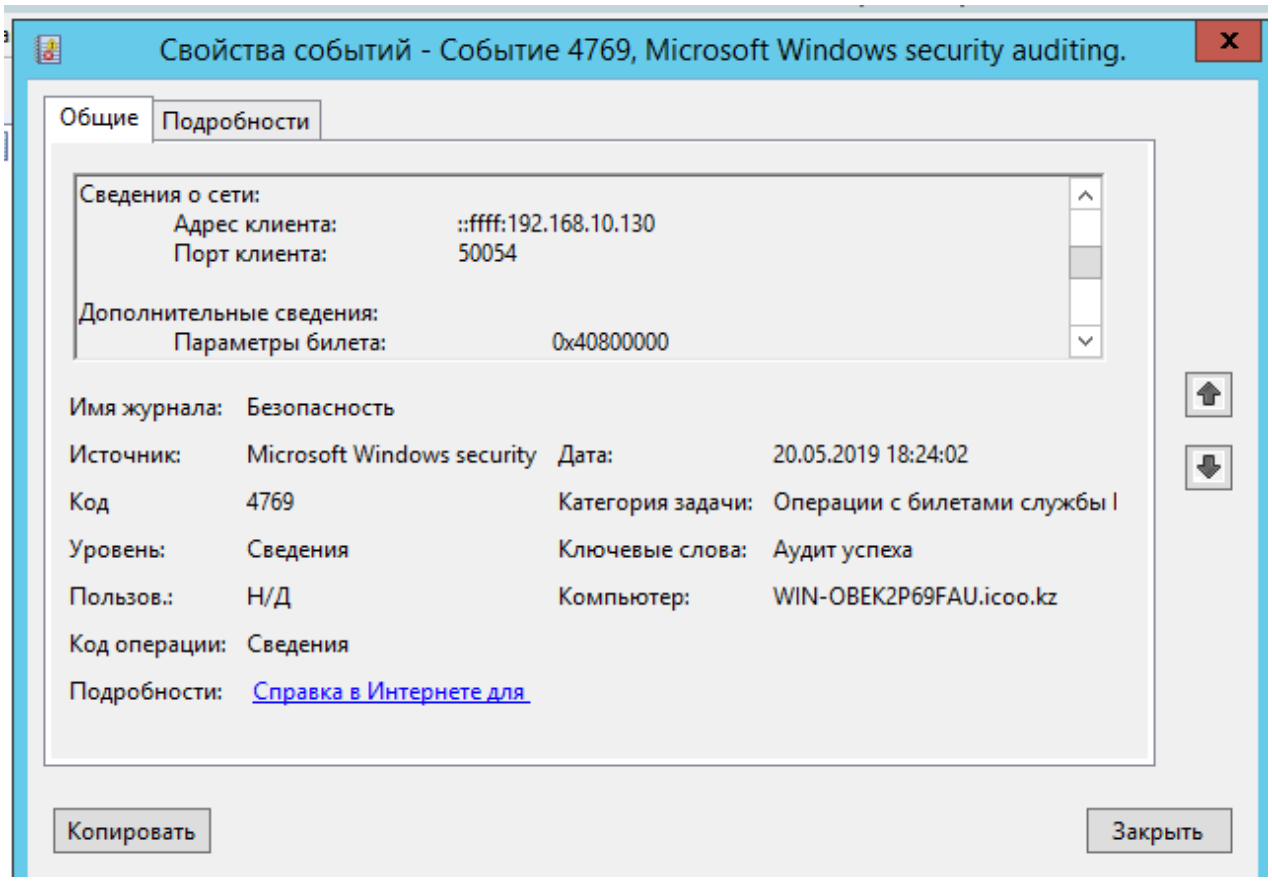


Рисунок 3.29 – Адрес клиента

3.5.6 Политика запрещения локального входа

Политика, запрещающая локальный вход в систему. Этот параметр безопасности определяет, каким пользователям будет отказано во входе в систему. Этот параметр политики заменяет параметр «Разрешить локальный вход в систему», если к учетной записи применяются обе политики.

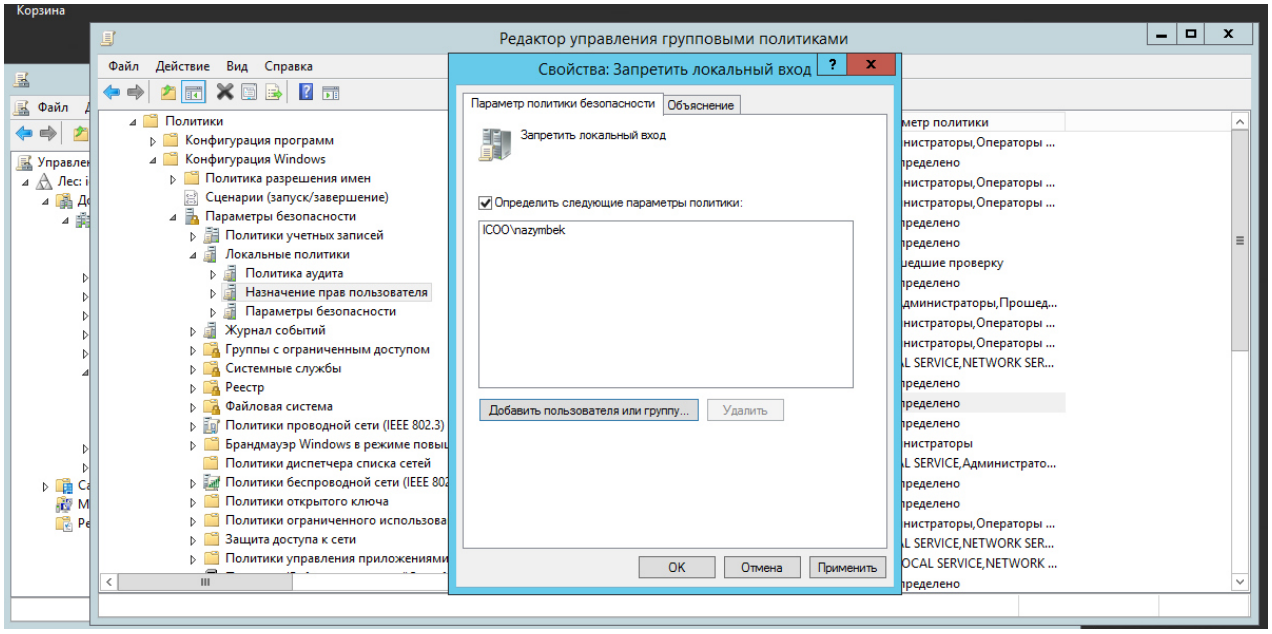


Рисунок 3.30 – Запрет на локальный вход пользователю «nazymbek»

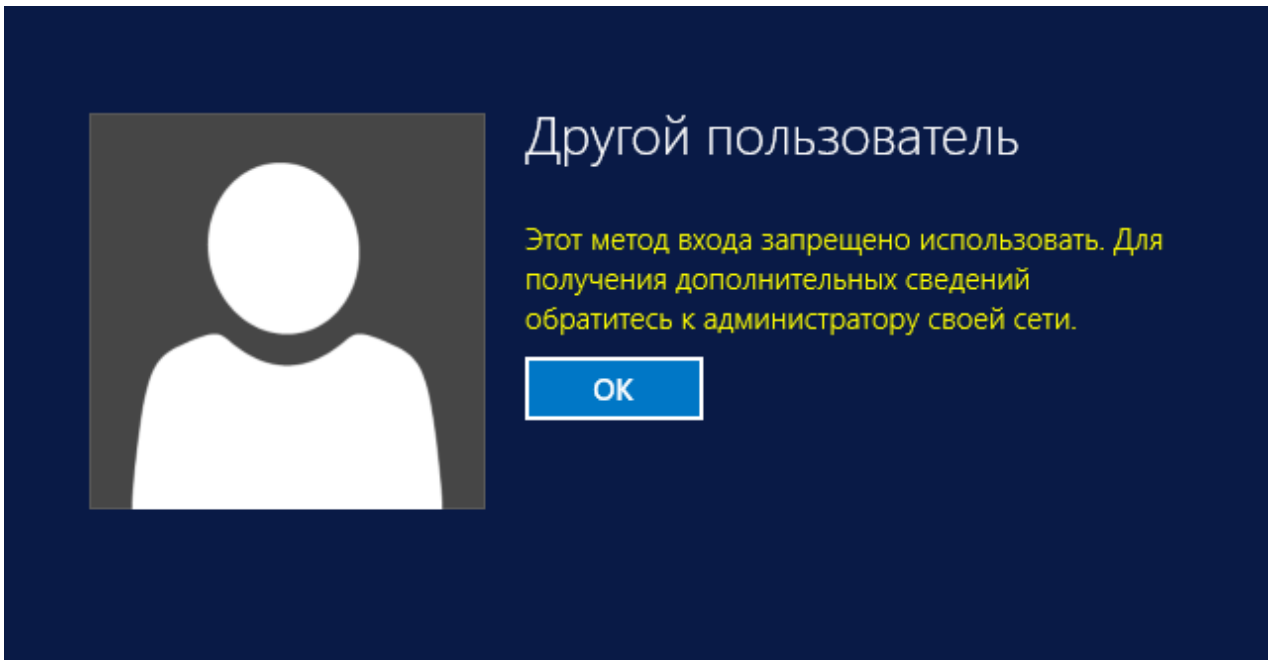


Рисунок 3.31 – Результат входа в систему пользователю «nazymbek»

3.5.8 Политика переименования учетной записи Администратор

Политика переименования учетной записи Администратор. Этот параметр безопасности определяет, будет ли связано другое имя учетной записи с идентификатором безопасности учетной записи «Администратор». Переименование учетной записи «Администратор» несколько затрудняет

угадывание посторонними лицами комбинации имени и пароля этого привилегированного пользователя.

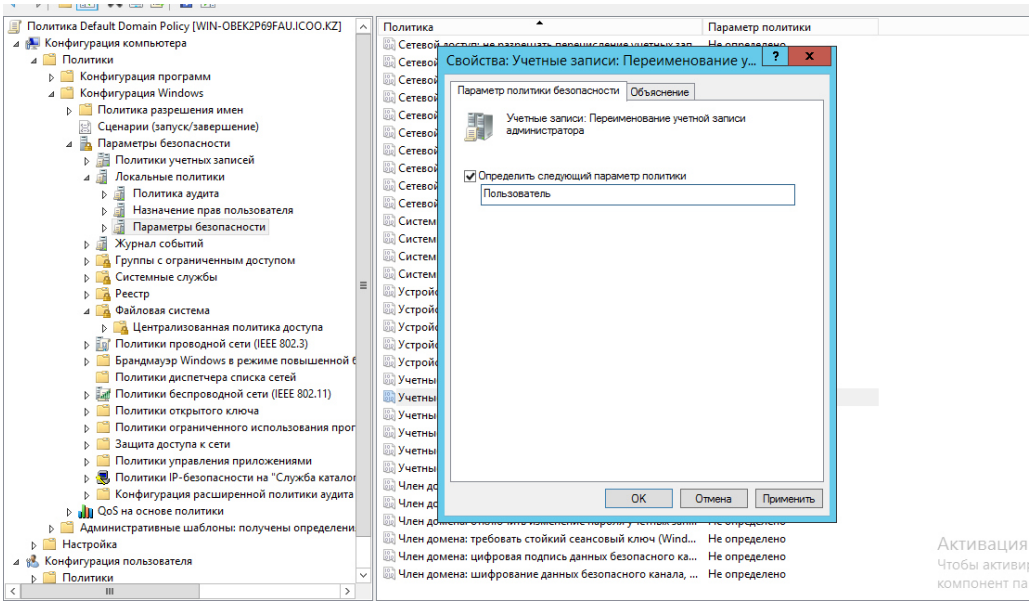


Рисунок 3.32 – Переименование учетной записи «Администратор» на «Пользователь»

3.6 Backup системы

В целях улучшения безопасности пользовательских данных был сделан Backup системного диска с помощью системы архивации данных Windows Server 2012. Оснастка архивации данных представляет собой обычное окно Windows, в котором есть собственный панель управления. Консоль позволяет выполнять две основные функции: настройка однократной или периодической архивации, восстановление данных. Резервное копирование данной консоли поддерживает выполнение автоматического резервного копирования по определенному расписанию.

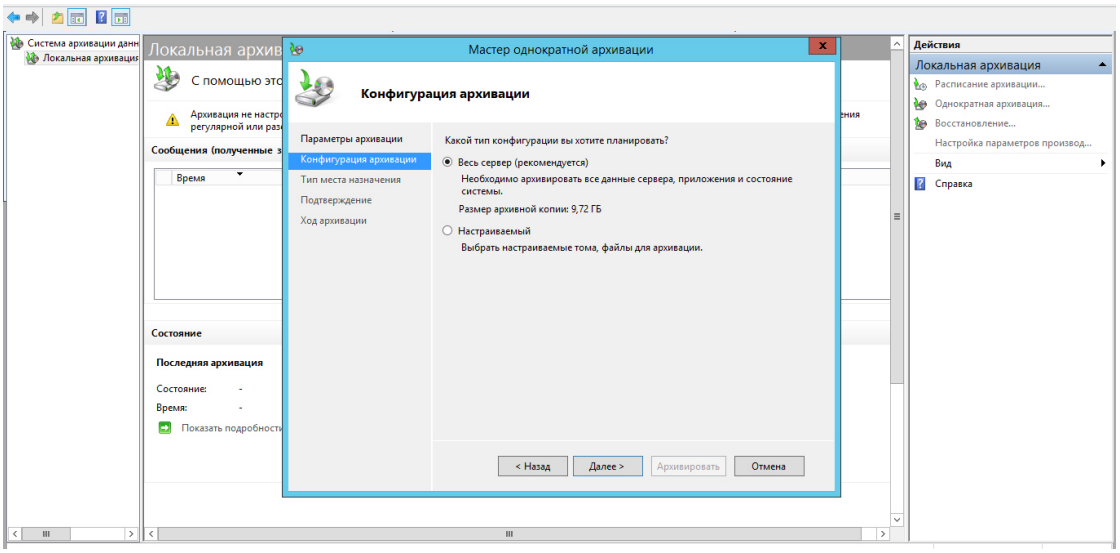


Рисунок 3.33 – Резервное копирование сервера

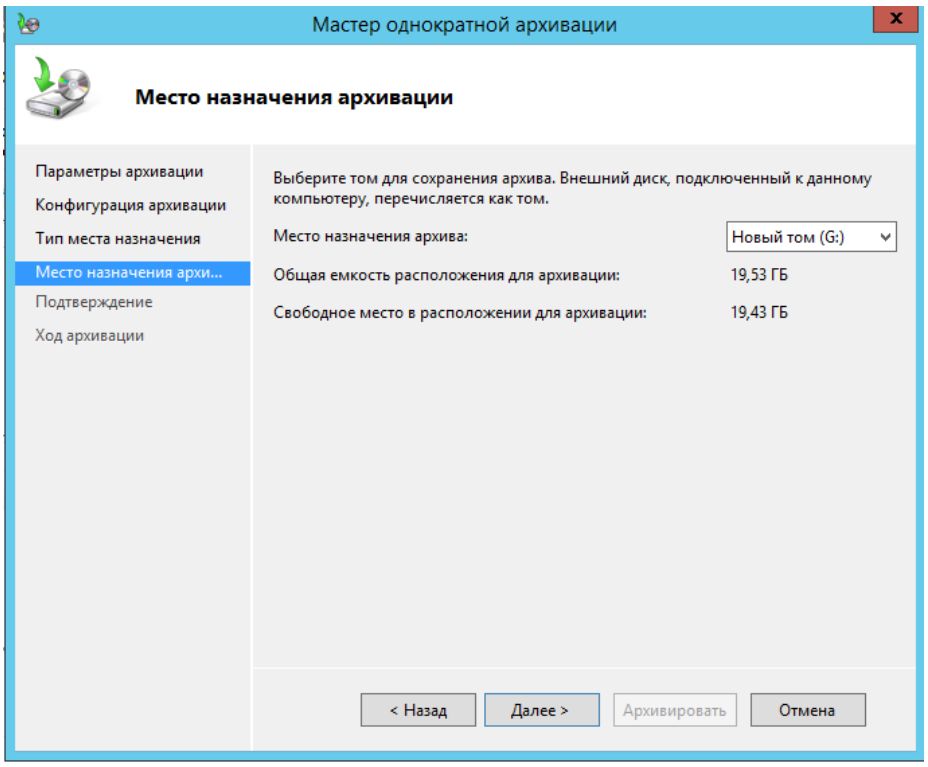


Рисунок 3.34 – Место назначение архивации

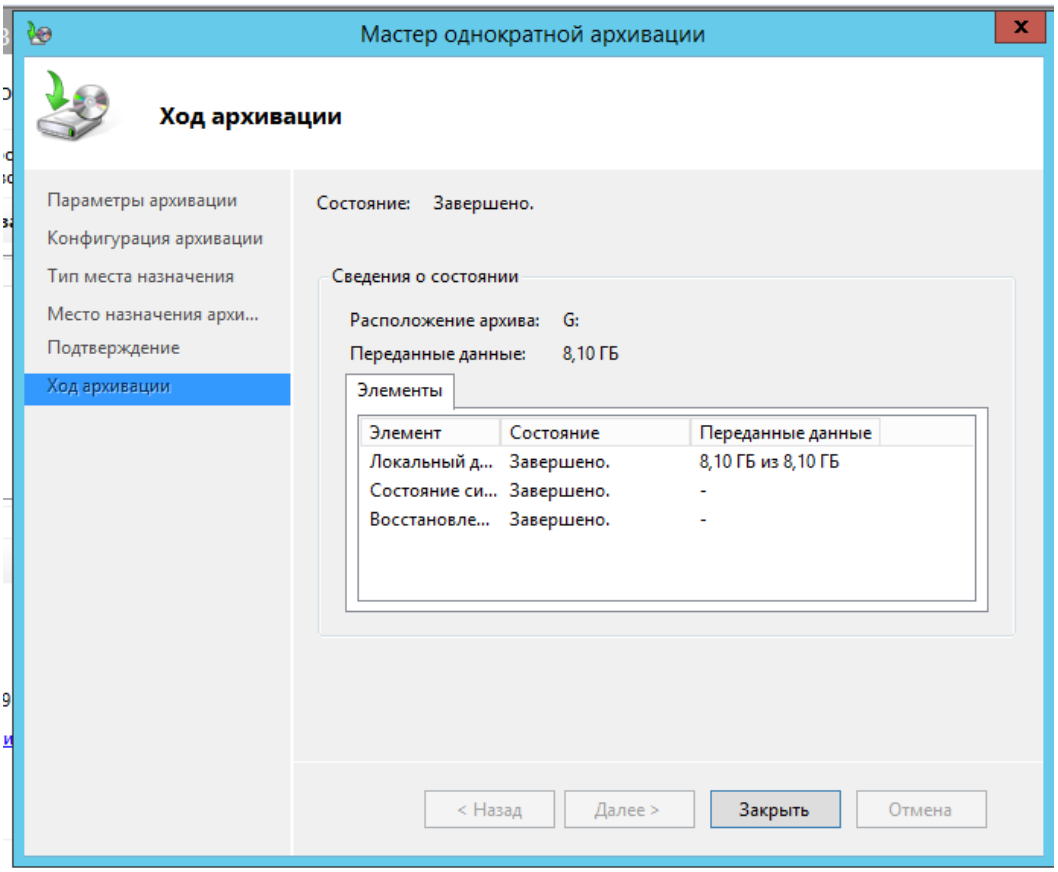


Рисунок 3.35 – Завершение резервного копирования

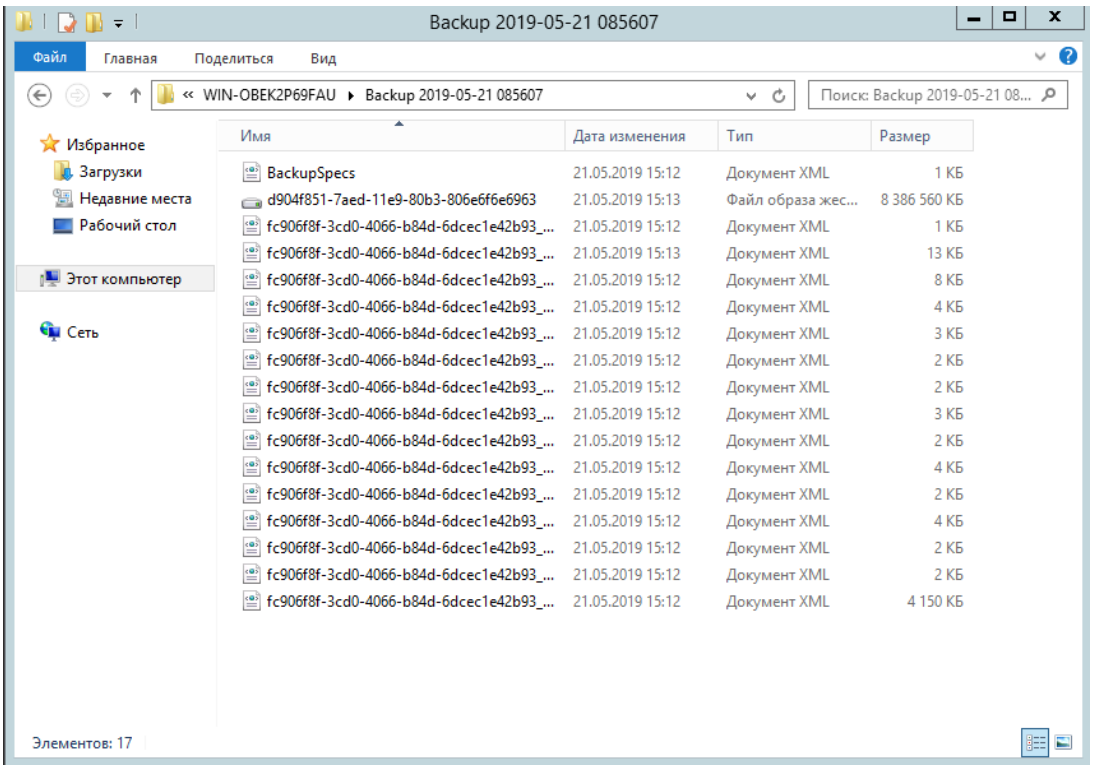


Рисунок 3.36 – Резервные файлы

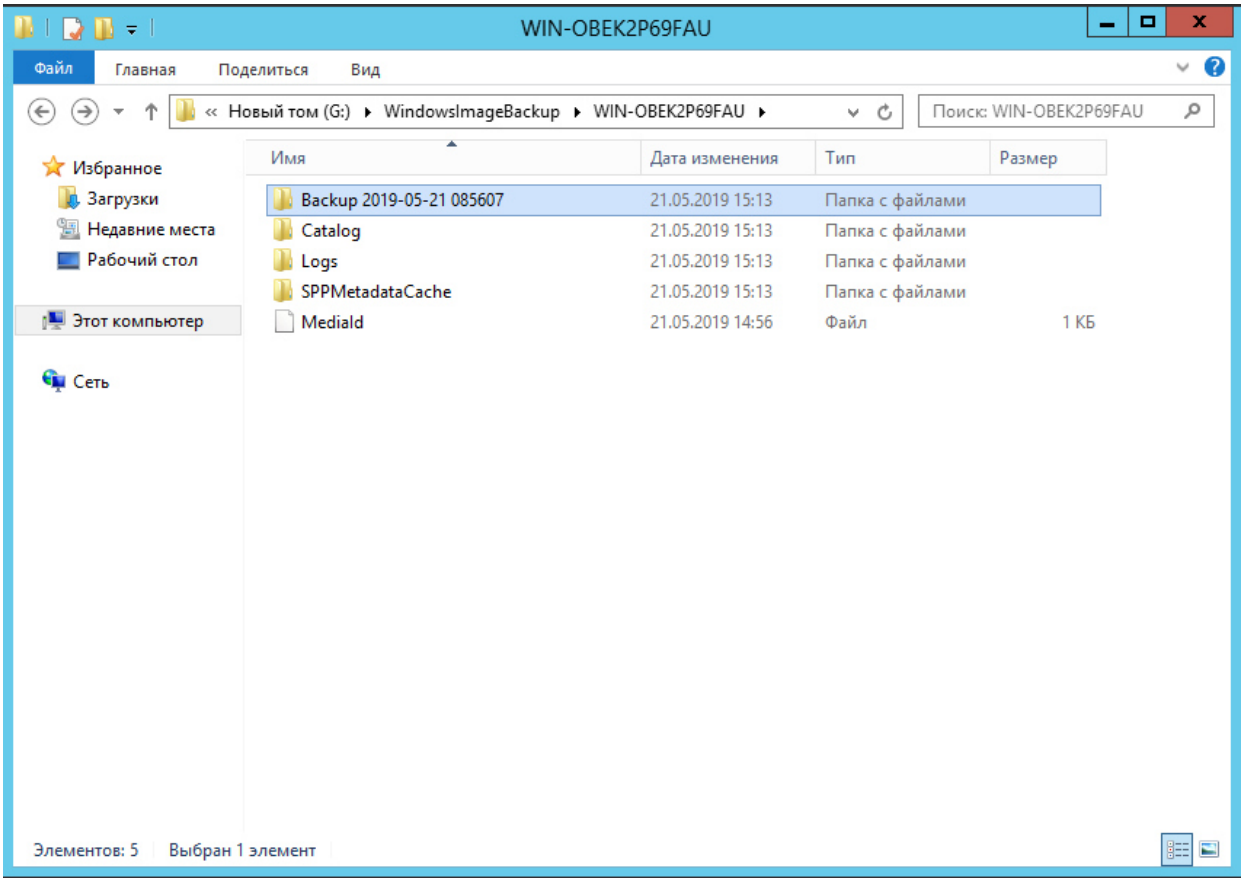


Рисунок 3.37 – Папка с резервными файлами

3.7 BitLocker

BitLocker является встроенным программным обеспечением операционной системы Windows Server 2012. BitLocker это технология шифрования содержимого дисков компьютера, разработанная компанией Microsoft. С помощью данной технологии, появилась возможность шифровать жесткие диски. Алгоритм, который использует BitLocker называется Advanced Encryption Standard. В моей практической работе было выполнено шифрование с помощью ключа, который одновременно является и паролем.

Рисунок 3.38 – Структура шифрования

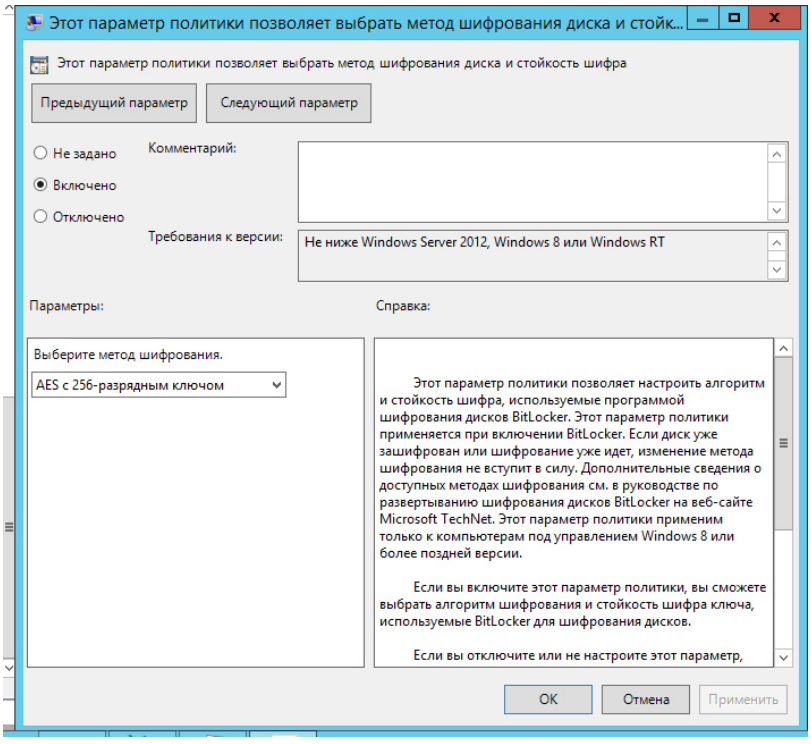


Рисунок 3.39 – Шифрование с AES 256-разрядный ключ

Следующая политика, которая была применена это параметр разрешения использования ПИН-кода при запуске компьютера.

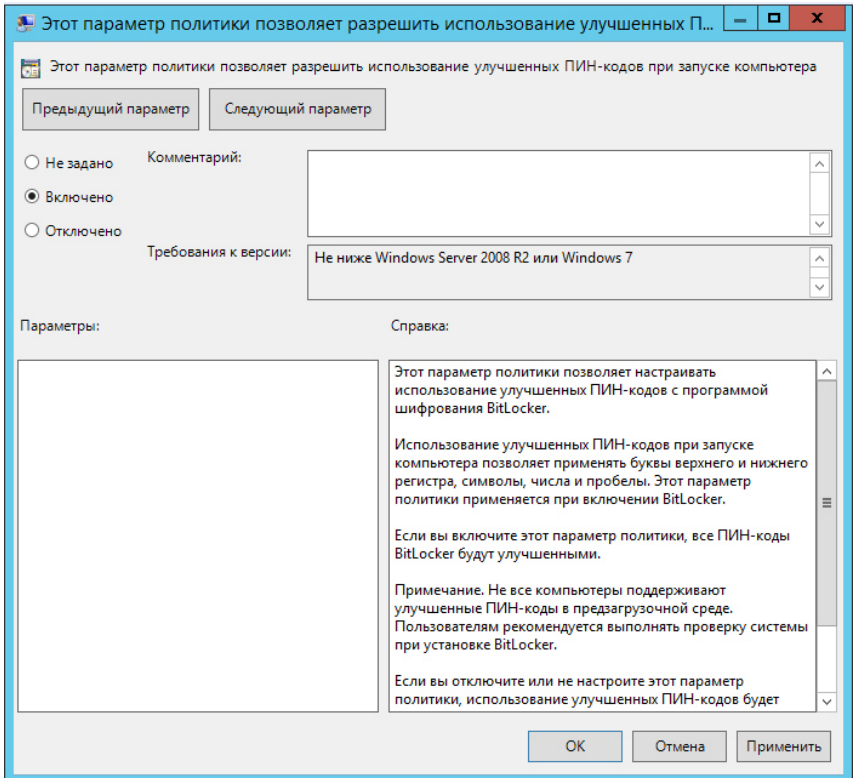


Рисунок 3.40 – ПИН-код при запуске

В процессе работы с BitLocker необходимо выбрать системный том, который будет шифроваться. Также в дополнение базовых настроек шифрования, необходимо создать надежный пароль, в котором используется строчные и прописные буквы, а также цифры, другие знаки и пробелы.

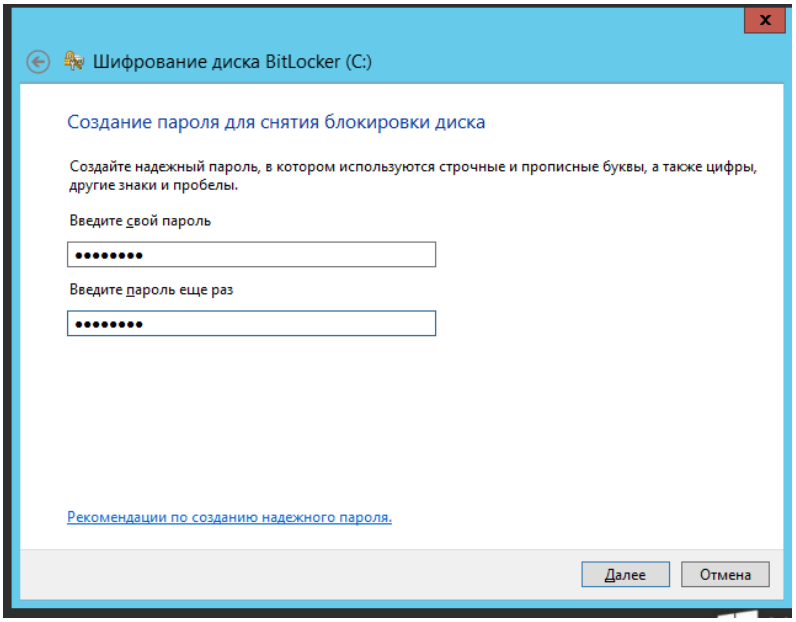


Рисунок 3.41 – Создание пароля

Также при настраивании шифрования, нужно выбрать какую часть диска требуется зашифровать.

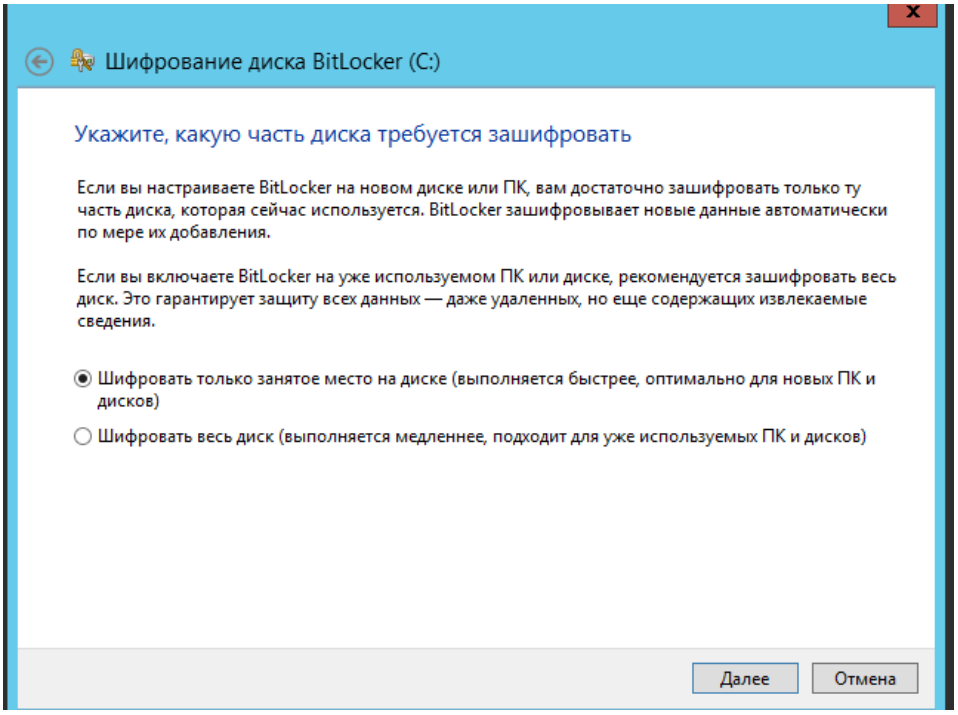


Рисунок 3.42 – Выбор части диска шифрования

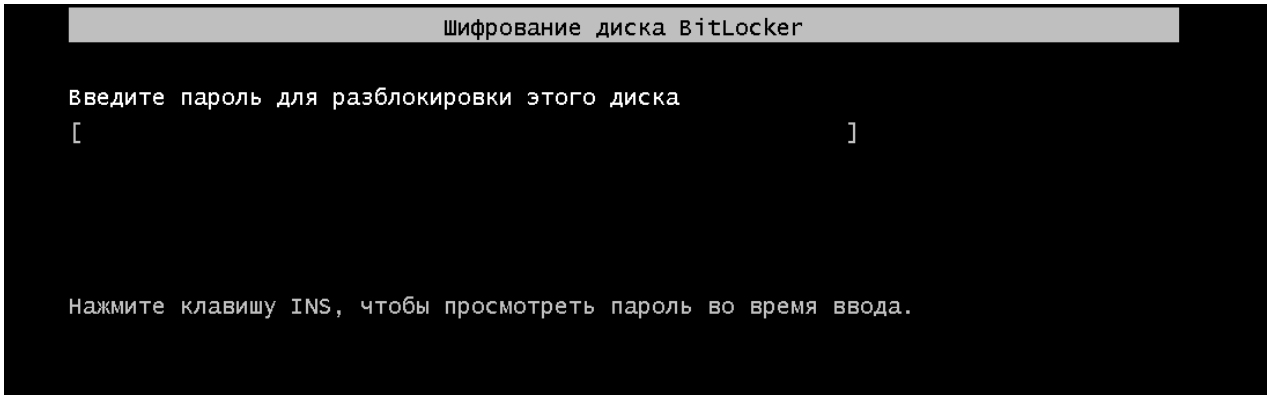


Рисунок 3.43 – Авторизация для шифрования

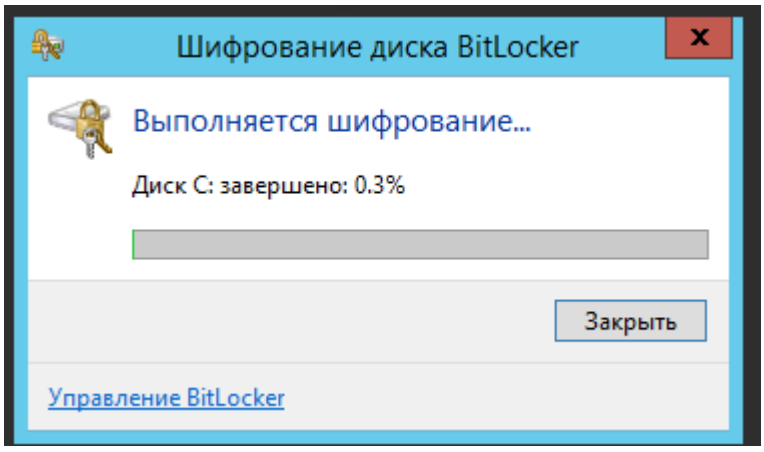


Рисунок 3.44 – Выполнения шифрования

```
C:\Users\Администратор>manage-bde -status
Шифрование дисков BitLocker: версия средства настройки: 6.3.9600
(C) Корпорация Майкрософт (Microsoft Corporation), 2013. Все права защищены.

Тома диска, которые можно защитить с помощью
шифрования диска BitLocker:
Том C: []
[Том с операционной системой]

    Размер:                          40,12 ГБ
    Версия BitLocker:                2.0
    Состояние преобразования:        Выполняется шифрование
    Зашифровано (процентов):         20,7%
    Метод шифрования:                AES 256
    Состояние защиты:                Защита отключена
    Состояние блокировки:            Разблокировка
    Поле идентификации:              Неизвестный
    Предохранители ключа:
        Пароль
        Числовой пароль

Том G: [Новый том]
[Том данных]

    Размер:                          19,53 ГБ
    Версия BitLocker:                2.0
    Состояние преобразования:        Шифрование приостановлено
    Зашифровано (процентов):         7,2%
    Метод шифрования:                AES 256
    Состояние защиты:                Защита отключена
    Состояние блокировки:            Разблокировка
    Поле идентификации:              Неизвестный
    Автоматическая разблокировка:    Отключен
    Предохранители ключа:
        Пароль
        Числовой пароль


C:\Users\Администратор>_
```

Рисунок 3.45 – Статус процесса шифрования

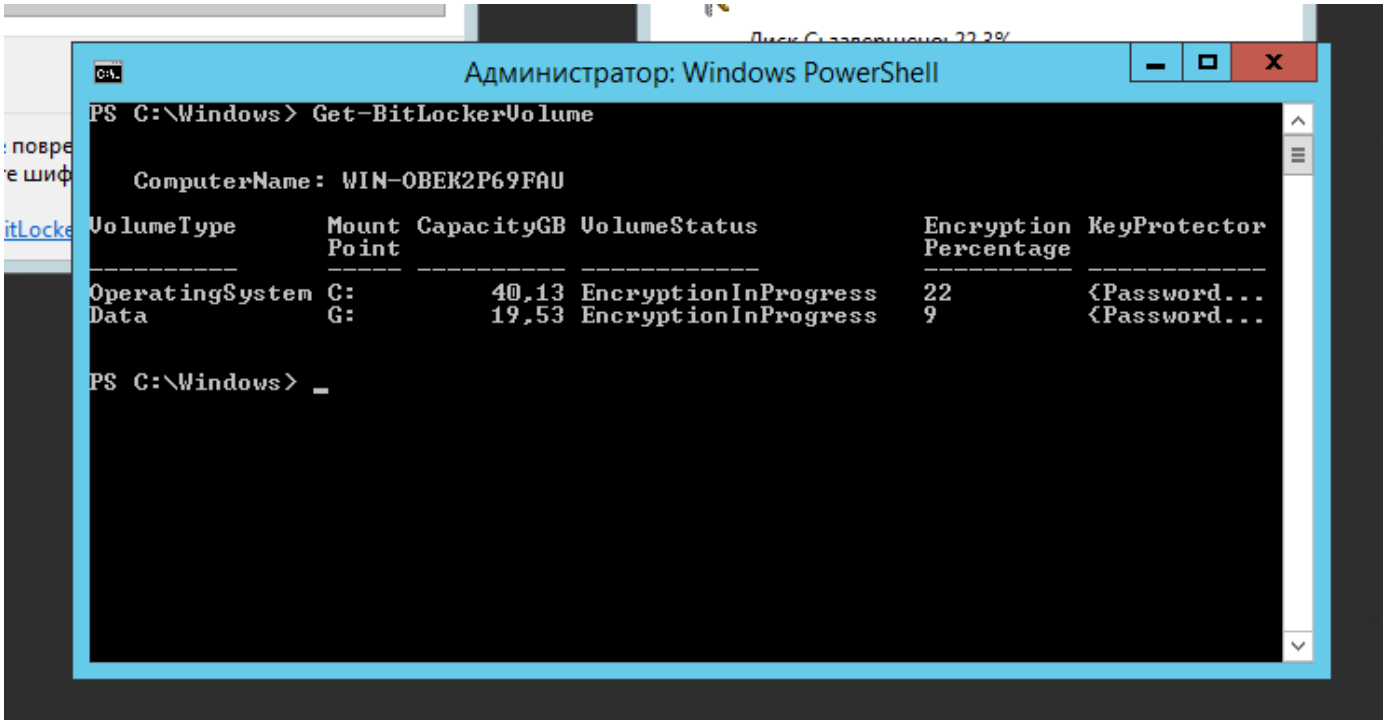


Рисунок 3.46 – Данные о шифровании

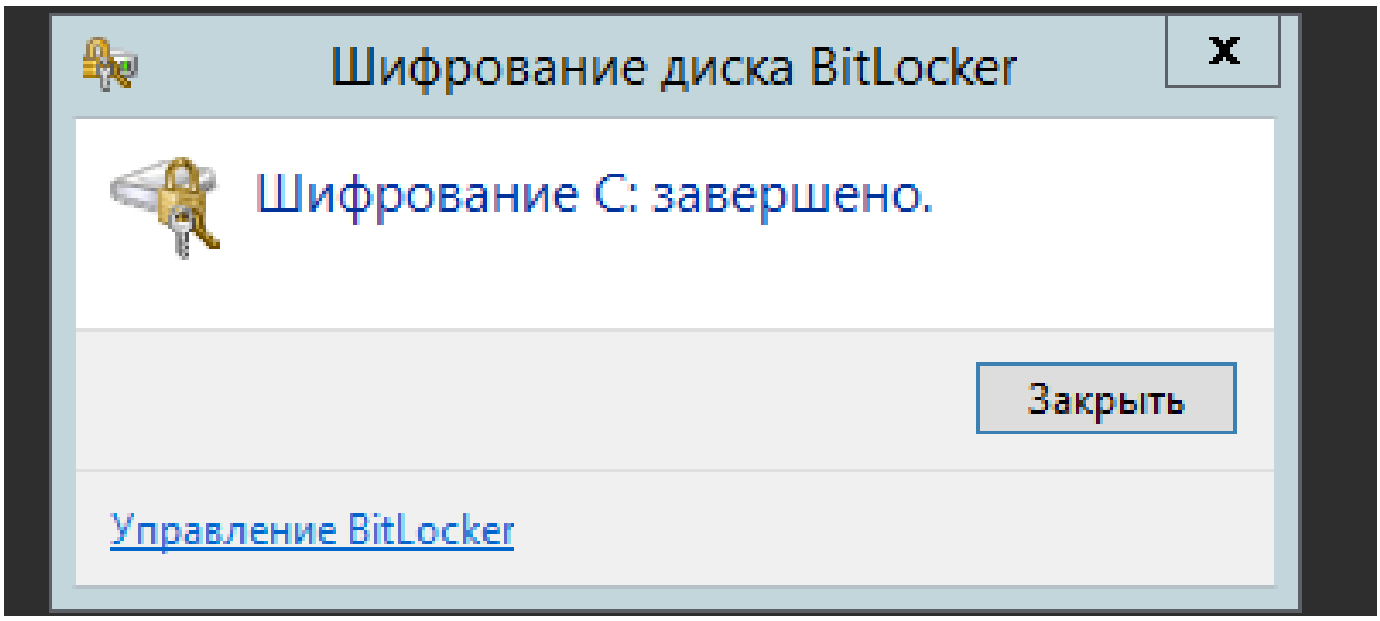


Рисунок 3.47 – Завершение шифрования

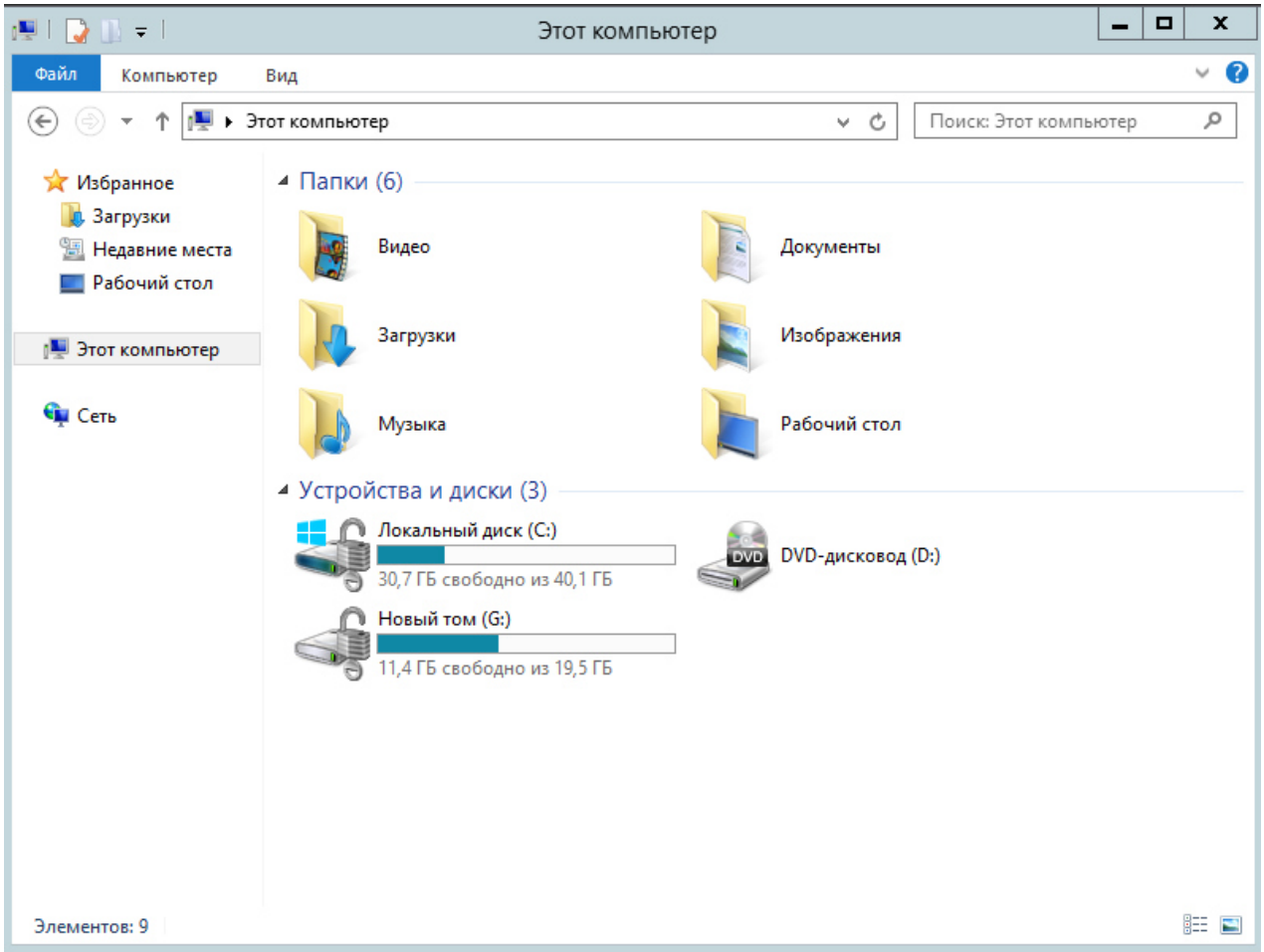


Рисунок 3.48 – Итог зашифрованных дисков

3.8 PowerShell Backup

PowerShell – это встроенный инструмент, который представляет собой оболочку командной строки и включает гибкое использование управления компьютером. Командная строка PowerShell позволяет управлять службами, хранилищами файлами, процессами и серверами. С помощью этого инструмента можно создавать и выполнять собственные сценарии. Оболочка PowerShell имеет сходство с командной строкой, а именно в наличии собственных наборов команд. Синтаксис языка, определения командлетов и их параметров в этой программе отличается от привычного, хотя утилита способна распознавать многие команды CMD.

В процессе изучения комплексных мер защит операционных систем, была выделена утилита как резервное копирование с помощью PowerShell. К созданию резервной копии необходимо было проанализировать структуру выполнения данного процесса. В соответствии с тем, что резервное копирование является важной частью защиты пользовательских данных был написан собственный сценарий. Сценарий был направлен на то, чтобы выполнять резервную копию по расписанию.

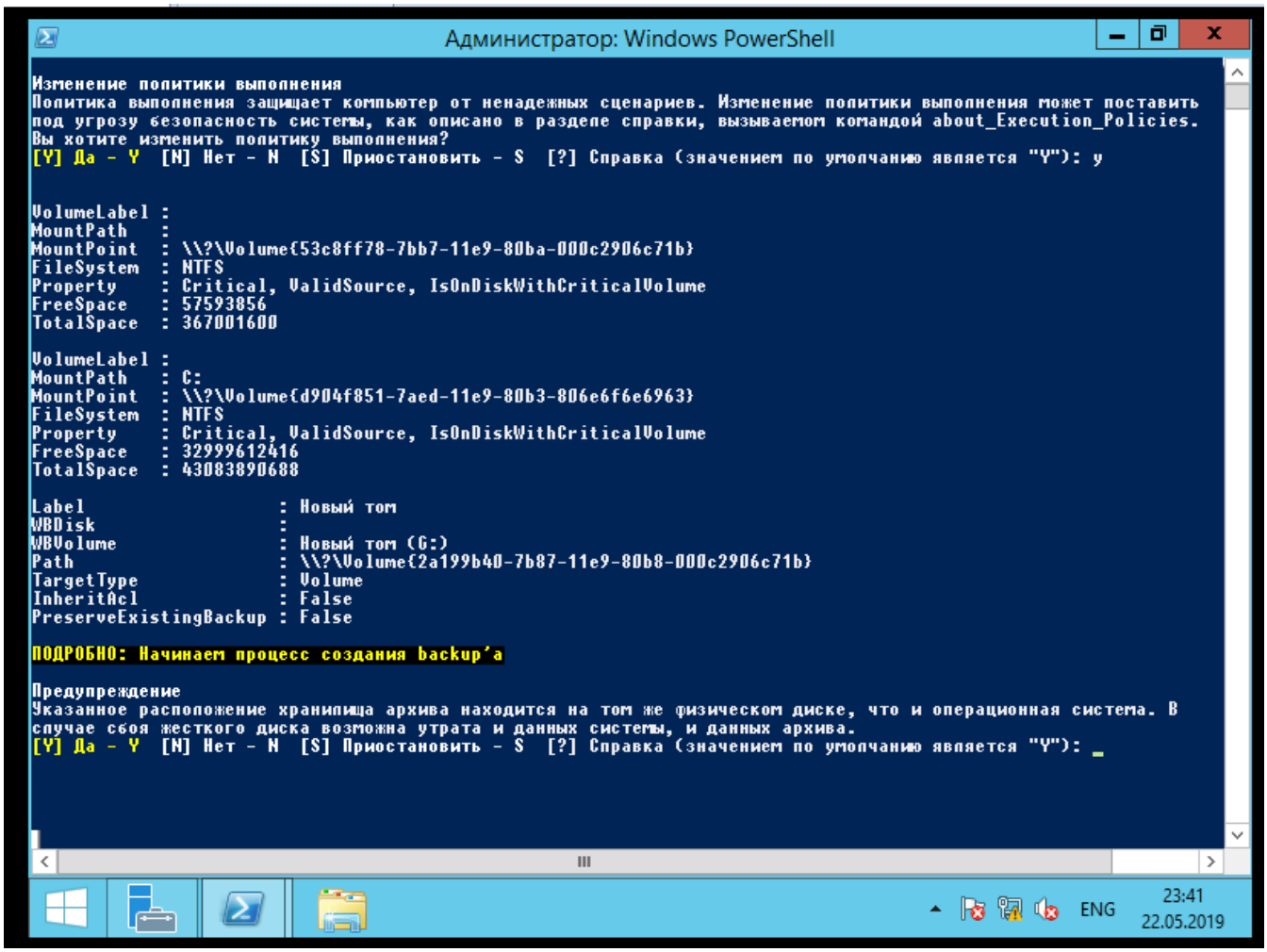


Рисунок 3.49 – Выполнение скрипта

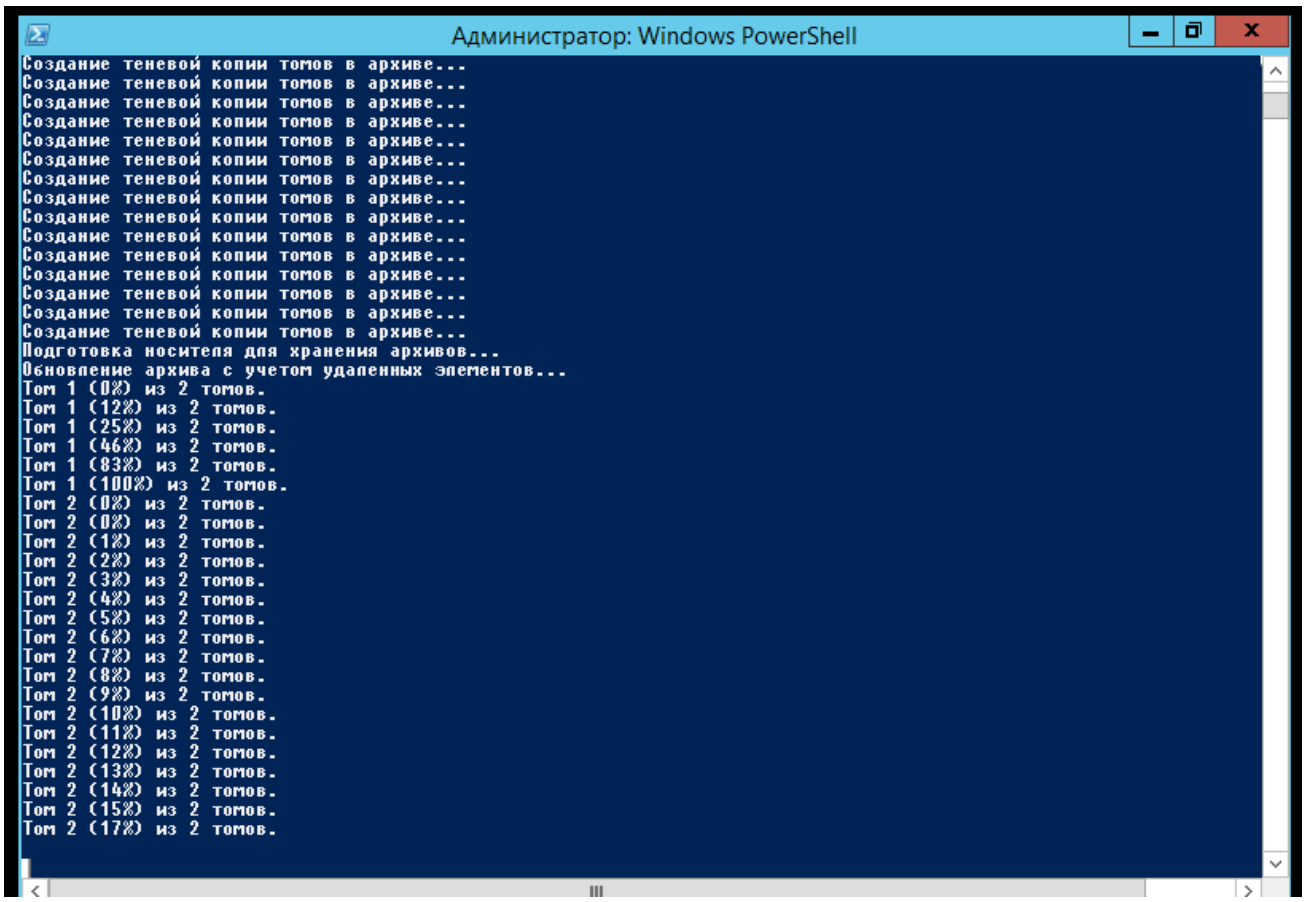


Рисунок 3.50 – Процесс резервирования файлов

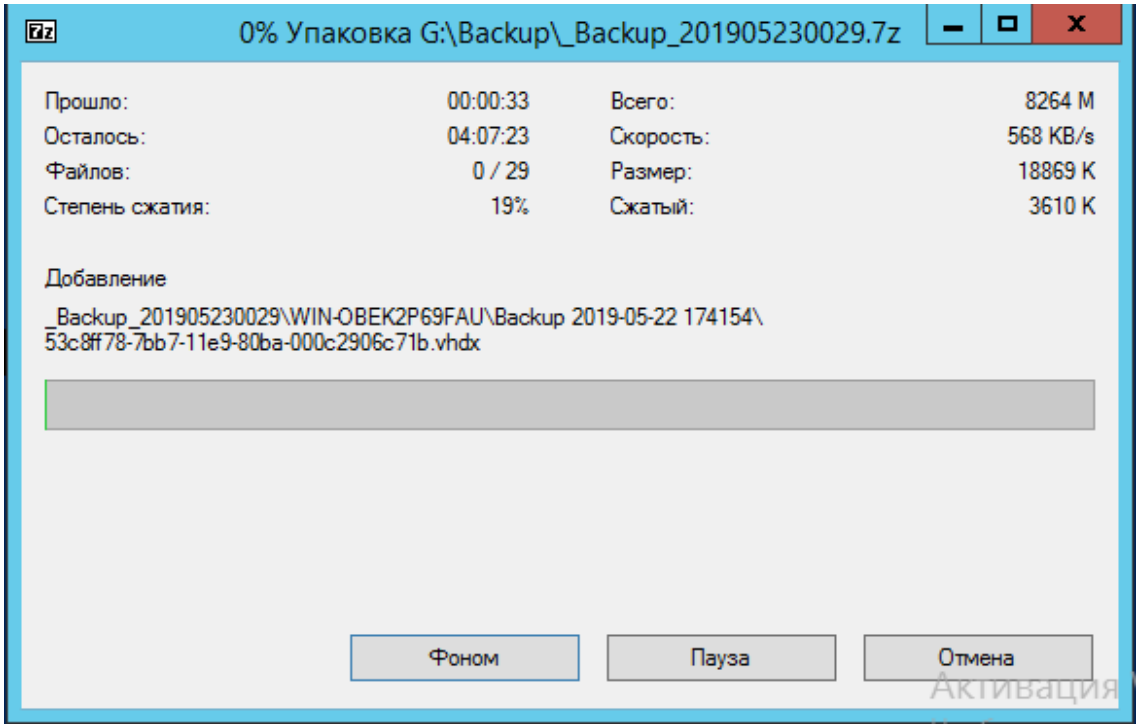


Рисунок 3.51 – Архивирование резервных файлов

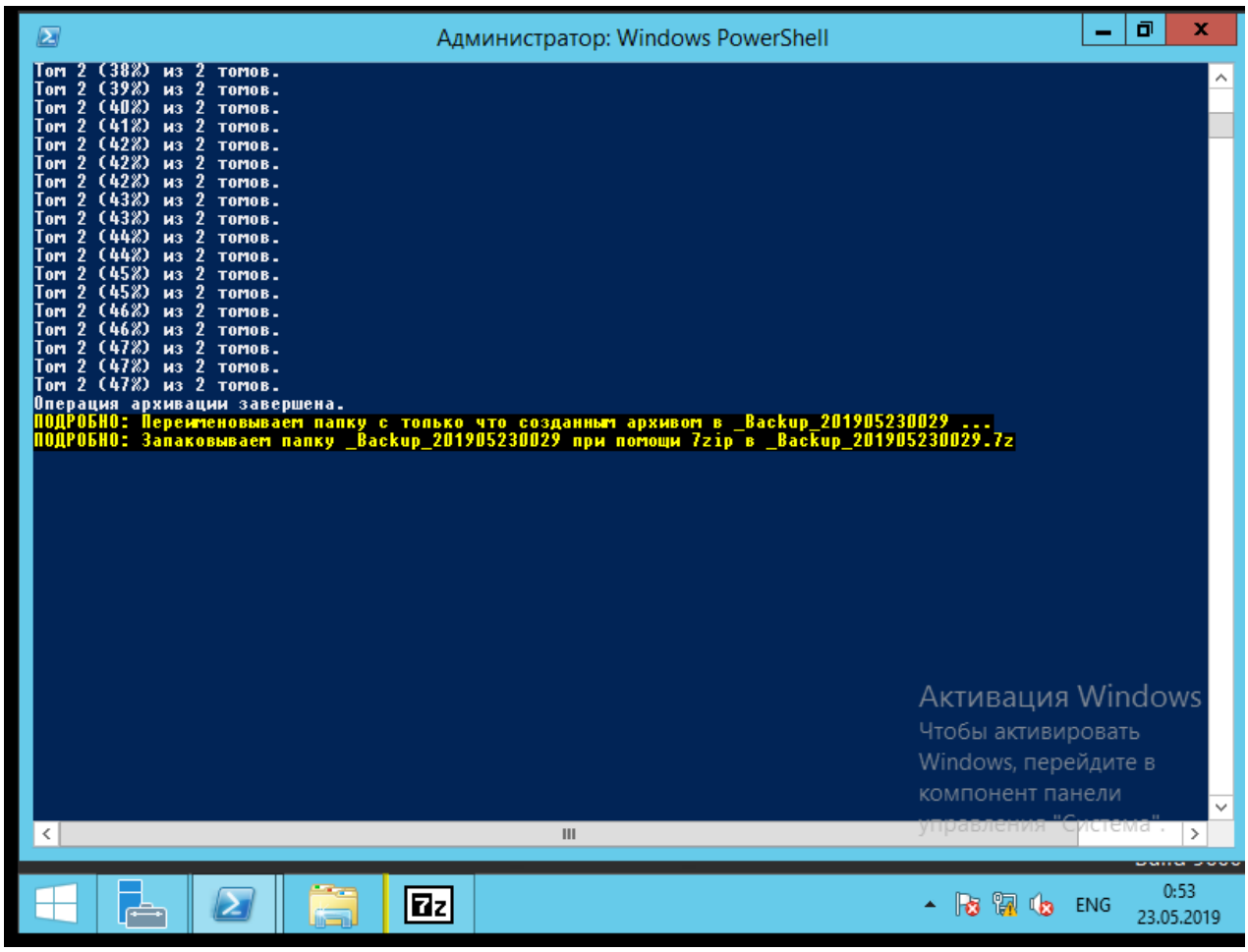


Рисунок 3.52 – Запаковывание папки Backup

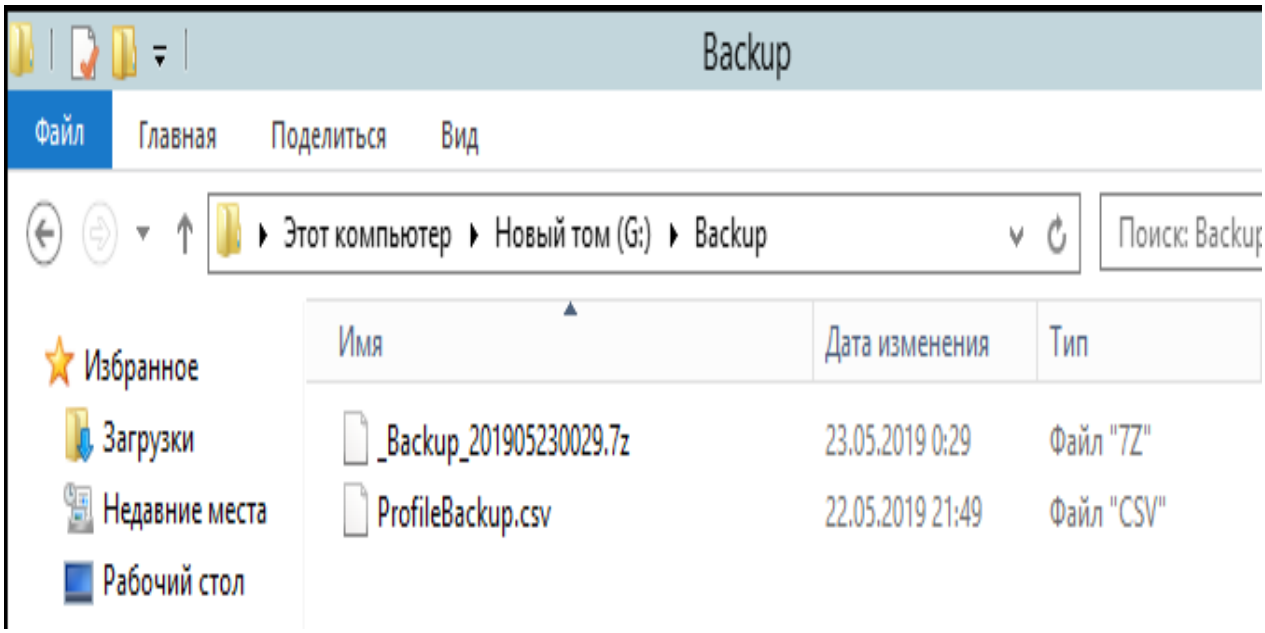


Рисунок 3.52 – Backup файл

Листинг сценария:

```
Write-Verbose "Начали..."
#Сохраняем значение переменной окружения $VerbosePreference
$tmpVerbpref=$VerbosePreference
$VerbosePreference="Continue"
#Путь к сетевой папке, в которую будем копировать архив
$NetworkBackupPath="\\DESKTOP-
G1D2L6H\Users\Nazymbek.ICOO\Desktop\Backup$\DESKTOP-
G1D2L6H\Users\Nazymbek.ICOO\Desktop\BMR"
#Имя раздела, на котором будем создавать архив
$VolumeTarget="G:"
# Количество копий бэкапа, которые необходимо сохранить на локальном
носителе
$BackupQuantity=1
# Количество копий бэкапа, которые необходимо сохранить на сетевом
носителе
$NetBackupQuantity=1
#Путь к файлу-списку бэкапов
$csvFile="G:\Backup\ProfileBackup.csv"
#Путь к папке, в котой будем создавать архив 7zip
$Path2Arc="G:\Backup"
# подключаем оснастку Server Backup
Add-PSSnapin Windows.Serverbackup -ErrorAction SilentlyContinue
# создаём задание бэкапа
$policy = New-WBPolicy
<#
# создаём и добавляем в задание бэкапа о бэкапируемых файлах
$source = New-WBFileSpec -FileSpec "C:\Users"
Add-WBFileSpec -Policy $policy -FileSpec $source
#>
#
#Get list of critical volumes
$VolSources = Get-WBVolume -CriticalVolumes
#Add volumes to be backed up
Add-WBVolume -Policy $policy -Volume $VolSources
#Define VSS Backup Otions
Set-WBVssBackupOptions -policy $policy -VssCopyBackup
#Enable SystemState backup
Add-WBSystemState -policy $policy
#Enable Bare Metal Recovery
Add-WBBareMetalRecovery -Policy $policy
#
# указываем локальный том, на который будет копироваться архив
$target = New-WBBackupTarget -VolumePath $VolumeTarget
```

```
Add-WBBackupTarget -Policy $policy -Target $target
Write-Verbose "Начинаем процесс создания backup'a"
# выполняем бэкап
Start-WBBackup -Policy $policy
# проверяем код возврата с результатом выполнения бэкапа
if ((Get-WBSummary).LastBackupResultHR -eq 0) {
   # переименовываем архив в более понятное имя
   $newname = "_Backup_$(Get-Date -f yyyyMMddHHmm)"
   Write-Verbose "Переименовываем папку с только что созданным архивом в
$newname ..."
   Ren $VolumeTarget\WindowsImageBackup -NewName $newname
   # Запаковываем архив при помощи 7zip
   $arc="C:\Program Files\7-Zip\7zG.exe"
   $arc_params="a -t7z -m0=LZMA2 -mmt -mx9"
   $arc_source="$VolumeTarget\$newname"
   $arc_dest="$Path2Arc\$newname.7z"
   Write-Verbose "Запаковываем папку $newname при помощи 7zip в
$newname.7z"
   Start-Process $arc -ArgumentList "$arc_params $arc_dest $arc_source" -Wait
   # копируем архив в сетевую папку
   #copy $VolumeTarget\$newname $NetworkBackupPath -Recurse
   Write-Verbose "Копируем файл $arc_dest в сетевую папку..."
   copy "$arc_dest" $NetworkBackupPath
   if ($?) {
      #если копирование прошло без ошибок, удаляем файл-архива и папку,
которая была запакована в этот архив
      del "$arc_dest" -Force -Verbose
      del $VolumeTarget\$newname -Recurse -Force #-Verbose
   }
   # удаляем старые архивы из сетевой папки, за исключением последних
$BackupQuantity архивов
   $NetBackups=dir $NetworkBackupPath | ?{$_.Name -match "_.+(\d)+\.7z$"}
   $NetBackupsCount=$NetBackups.count
   if (($NetBackupsCount - $NetBackupQuantity) -gt 0) {
      $NetBackups | sort lastwritetime | select -First ($NetBackupsCount -
$NetBackupQuantity) | del -Force -Verbose #-Recurse -WhatIf
   }
   # читаем наш собственный каталог бэкапов
   $csv=@()
   if (Test-Path $csvFile) {$csv = @(Import-Csv $csvFile)}
   # считываем данные о последнем бэкапе
   $current = Get-WBBackupSet | select -Last 1  | select VersionID, SnapshotId
   # и добавляем его в массив объектов действующих бэкапов
   $csv += $current
```

```
   # чтобы не было путаницы, снова сортируем объекты и пишем обратно в
CSV файл
   $csv | sort @{Expression={[datetime]($_.VersionId)}}| select -Last
$BackupQuantity | Export-Csv $csvFile -NoTypeInformation
   # и считаем сколько там записей
   $count = $csv.count
   # если записей больше BackupQuantity, то считаем сколько лишних архивов
нужно удалить.
   # если меньше BackupQuantity записей, то ничего удалять не надо и просто
добавляем новую запись
   if ($count -gt $BackupQuantity) {
      $old = $count - $BackupQuantity
      # генерируем случайное имя для скрипта, который будет использоваться
в diskshadow
      $file = [System.IO.Path]::GetRandomFileName()
      # выбираем все лишние архивы и пропускаем их по конвейеру на
удаление
      $csv | sort @{Expression={[datetime]($_.VersionId)}}| select -First $old | %{
         #Read-Host 'Press Enter to continue...' | Out-Null
         #Write-Verbose $file
         ##Read-Host 'Press Enter to continue...' | Out-Null
         # записываем команду во временный файл
         "delete shadows ID {$($_.SnapshotID)}"|Out-File -FilePath
$Env:TEMP\$file -Encoding OEM
         #gc $Env:TEMP\$file
         #Read-Host 'Press Enter to continue...' | Out-Null
         # и запускаем diskshadow в режиме скрипта
         diskshadow /s $Env:TEMP\$file | Out-Default
      }
      del $Env:TEMP\$file
   }
} else {
   # ругаемся, что бэкап не был завершён успешно
   Write-Verbose "Ошибка выполнения бэкапа"
}
Write-Verbose "Скрипт закончил работу"
#Восстанавливаем значение переменной окружения $VerbosePreference
$VerbosePreference=$tmpVerbpref
```

4 Безопасность жизнедеятельности

4.1 Анализ условий труда

В выполнении дипломной работы рассматривается проектирование системы защиты пользовательских данных в организации. Проект был разработан с целью улучшения системы защиты пользовательских данных на уровне операционной системы. Были рассмотрены ряд способов реализации проекта. Изначальное позиционирование проекта направлено на развитие информационной безопасности в разных организациях. Факт того что была проведена полноценная аналитика и мониторинг, говорит о том что, подобранная тема была востребована в направлении информационной безопасности организации. В сравнении с предыдущими состояниями безопасности, было выявлено ряд улучшенных мер в направлении информационной безопасности. Качество безопасности пользовательских данных в системах было развито. Сотрудники организаций были проинформированы данным проектом, что послужило приятным бонусом в корпоративной культуре. Рассматривая проект, были реализована система защиты с помощью групповых политик операционной системы Windows. Политики применимые в безопасности являются базовыми мерами защиты. Основные технические оборудования предназначенные для реализации задачи были установлены непосредственно в помещении офиса.

Компания, в которой внедрялся проект, называется «InformConsulting». На рынке информационного сервиса, компания имеет значительное место. Род деятельности компании, это обслуживание различных организаций также продажи антивирусного программного обеспечения. Данная компания имеет офис в виде жилого дома. Подсчитывая количество сотрудников, можно сказать, что количество работающих в организаций составляет 30 человек. Непосредственно в офисе имеются свои отделы, каждая их которых занимается своим делом. К примеру, отдел администрирования занимается управлением всего оборудования, в частности своих клиентов. В организаций насчитывается 6 отделов. В процессе работы сотрудники организаций тесно взаимодействуют с другими отделами. Так как целью компании является клиентская удовлетворённость и продажи продуктов организаций. Также присутствует отдел программистов. В отделе программистов разрабатываются программные обеспечения, как на компьютер так и на телефон.

Оборудования применимые для защиты пользовательских данных требуют минимальных затрат. Компания, в которой проектировалась защита пользовательских данных, дала возможность реализации запланированных действии. Технические средства организации были достаточными для улучшения качества безопасности пользовательских данных организации. Главные сотрудники отдела администрирования предоставляют возможность выполнения проекта, предлагая все средства организации.

В процессе работы над проектом на позиции младшего сотрудника администрирования, выявил вредный производственный недостаток.

Недостатком было: плохая вентиляция производственного помещения. Вентиляция производственного помещения – это совокупность мероприятий и устройств, необходимых для обеспечения заданного качества воздушной среды в рабочем помещении. Вентиляция принадлежит главенствующую роль в нормализации воздушной среды на рабочих местах и в производственных помещениях. Естественная вентиляция помещений может быть неорганизованной и организованной. При неорганизованной вентиляции поступление и удаление воздуха происходит через окна, форточки, специальные проемы, а также через неплотности наружных ограждений. Организованная естественная вентиляция производственных помещений называется аэрацией. Она осуществляется с помощью специально создаваемых конструктивных элементов промышленных зданий - аэрационных фонарей или с помощью специальных каналов или шахт, функционирующих под действием теплового напора.

Исследуя организацию, а в частности местность нахождения здания, то офис находится в благоприятных условиях для сотрудников организаций. Если брать в счет род деятельности младшего сотрудника отдела администрирования, то это ежедневная работа на персональном компьютере, конструкция рабочего места является оптимально размещенным на рабочей поверхности используемого оборудования с учетом его количества и конструктивных особенностей (размер монитора, клавиатуры и других). Конструкция рабочей мебели (столы и кресла) обеспечивает возможность индивидуальной регулировки. Рабочие места, высотой 0,8 м, размещены боковой стороной к окну. При эксплуатации электрооборудования существует опасность поражения электрическим током. В связи с этим фактом все вилки и розетки имеют контакты зануления, а все кабели спрятаны в кабель-каналы. Оборудования является практически бесшумным.

В помещении, где располагаются сотрудники, применяется естественное освещение, осуществляемое через боковое окно, ориентированное на запад. Для защиты от избыточного света и ярких лучей используются регулируемые жалюзи с вертикальными ламелями.

Внутри помещения офиса у рабочего места младшего сотрудника администрирования уровень опасных и вредных факторов не превышает установленных нормативов и каждое рабочее место сотрудников работающих в помещении, где работодатели выполняют свои должностные обязанности максимально приспособлено для характера выполняемых работ. Помещение является светлым, сухим и чистым, соответствующее санитарно-гигиеническим нормам.

4.2 Расчет тепловых нагрузок в помещении

В помещениях различного назначения действуют в основном тепловые нагрузки, возникающие снаружи помещения (наружные); а также тепловые нагрузки, возникающие внутри зданий (внутренние).

В помещениях различного назначения действуют в основном тепловые нагрузки, возникающие снаружи помещения (наружные); а также тепловые нагрузки, возникающие внутри зданий (внутренние)

Наружные тепловые нагрузки

В зависимости от времени года и времени суток наружные тепловые нагрузки могут быть положительными. Теплопоступления и тепло потери в результате разности температур определяются по формуле 0.1:

$Q_{огр} = V_{пом} * X_о * (t_{Нрасч} – t_{Врасч})$, Вт (0.1), где

$V_{пом}$ – объем помещения, $м^3$;

$V_{пом} = 3.5*3.5*3=36.75$ $м^3$;

$X_о$ – удельная тепловая характеристика, $Вт/м^3*^0C$;

$X_о= 0,42$ $Вт/м^3*^0C$;

$t_{Нрасч}$ – наружная температура (параметр А). Для холодного периода – средняя температура самого холодного месяца в 14 часов, для теплого периода – средней температуре самого жаркого месяца в 14 часов.

$t_{Врасч}$ – внутренняя температура, выбирается с учетом комфортных условий или технологических требований, предъявляемых к производственным процессам.

Для теплого времени года:

$t_{Нрасч} = 28,4\ ^0C$

$t_{Врасч} = 26\ ^0C$

$Q_{огр}= 36,75*0,42·2,4=37,04$ Вт

Для холодного времени года

$t_{Нрасч} = -8\ ^0C$

$t_{Врасч} = 19\ ^0C$

$Q_{огр} = 36,75·0,42·27 = 416,74$ Вт

Избыточная теплота солнечного излучения в зависимости от типа стекла почти до 90% поглощается средой помещения, остальная часть отражается. Максимальная тепловая нагрузка достигается при максимальном уровне излучения, которое имеет прямую и рассеянную составляющие. Интенсивность излучения зависит от ширины местности, времени года и времени суток.

Теплопоступление от солнечного излучения через остекление определяется по формуле 0.2:

$Q_р = (q^I F^I_о + q^{II} F^{II}_о) * βс.з$ (0.2), где

q^I, q^{II} – тепловые потоки от прямой и рассеянной солнечной радиации, $Вт/м^2$;

F^{I}_{0}, F^{II}_{0} – площади светового проема, облучаемые и необлучаемые прямой солнечной радиацией, $м^2$;

βс.з. – коэффициент теплопропускания. Для штор-жалюзи с металлическими пластинами:

βс.з. = 0,15

При отсутствии наружных затеняющих козырьков, ребер и т. д. для периода облучения остекления солнцем, когда его лучи проникают через окно в помещение $F^{I}_{0} = F^{II}_{0} = F_0 = 0$:

$Q_р = q^{II} F_0 * βс.з = q_{вр} * K^{T}_{1} * K_2 * βс.з * n * S_0$ (0.3), где

$q_{вп}$; $q_{вр}$ – тепловые потоки от рассеянной радиации, $Вт/м^2$. Для широты в 44^0 СШ после полудня в 14-15 ч. при расположении ЮВ:

$q_{вр} = 63$ $Вт/м^2$;

$F_о = nS_о = 2*2 = 4$ $м^2$ – площадь светового проема (n – число окон; $S_о$ – площадь 1 окна);

K_1 – коэффициент затемнения остекления переплетами (K^{T}_{1} – для проемов в тени).

$K^{T}_{1} = 1,28$;

K_2 – коэффициент загрязнения остекления:

$K_2 = 0,95$.

Тогда:

$Q_р = 63*1,28*0,95*0,15*4=45,96$ Вт

Для широты в 44^0СШ после полудня в 14-15 ч. при расположении ЮЗ:

$q_{вр} = 101$ $Вт/м^2$;

$F_о = nS_о = 2*2 = 4$ $м^2$

Тогда:

$Q_р = 101*1,28*0,95*0,15*4=73,69$ Вт

Тогда общее теплопоступление солнечного излучения с обеих сторон равно:

$Q_р = 45,96+73,69 = 119,65$ Вт

Внутренние тепловые нагрузки

Внутренние нагрузки в жилых, офисных или относящихся к сфере обслуживания помещениях слагаются в основном из тепла:

– выделяемого людьми;

– выделяемого лампами и осветительными, электробытовыми приборами;

– выделяемого компьютерами, печатающими устройствами фотокопировальными машинами пр.;

Летом при 24 ^{0}С один мужчина выделяет явного тепла 68 Вт, а общего – 104 Вт. Женщина выделяет 85% от нормы тепловыделений взрослого мужчины. Тогда выделение явного тепла в помещении составит:

$Q_л^{я} = 68*2 + 68*1*0,85 = 193,8$ Вт

А выделение общего тепла:

$Q_л^{о} = 104*2 + 104*1*0,85 = 296,4$ Вт

Зимой при 18 ^{0}С один мужчина выделяет явного тепла 89 Вт, а общего – 104 Вт. Тогда выделение явного тепла в помещении составит:

$Q_з^я$ = 89*2 + 89*1*0,85= 253,65 Вт.

А выделение общего тепла:

$Q_з^о$ = 104*2 + 104*1*0,85= 296,4 Вт

Теплопоступление от осветительных приборов, оргтехники и оборудования рассчитывается следующим образом. Теплопоступление от ламп определяется по формуле:

$$Q_{осв} = \eta \cdot N_{осв} \cdot F_{пол}, \quad Вт \quad (0.4)$$

где η – коэффициент перехода электрической энергии в тепловую (для лампы накаливания η=0,92-0,97);

$N_{осв}$ – установленная мощность ламп (N=60 Вт/м^2);

$F_{пол}$ – площадь пола:

$F_{пол}$ = 3,5*3,5=12,25 м^2

Тогда:

$Q_{осв}$ = 0,92*60*12,25 = 676,2

Тепло, выделяемое производственным оборудованием, определяется по формуле:

$$Q_{об} = N_{уст} \cdot K \quad (0.5)$$

$Q_{об}$ = 0,3 * 3 * 0,75 * 10^3 = 675 кВт.

Теплопритоки, возникающие за счёт находящейся оргтехники – это 30% мощности оборудования:

$Q_{орг}$ = 3 * 0,3 * 0,3 * 10^3 = 270 кВт

4.3 Расчет теплового баланса помещения

На основании выполненных расчетов составим баланс теплопоступлений в помещении:

$$Q_{изб} = Q_р + Q^я + Q_{осв} + Q_{об} + Q_{орг} + Q_{огр}$$

Лето: $Q_{изб}^Л$ = 119,65 + 193,8 + 676,2 + 675 + 270 + 37,04 = 1,97 кВт

Зима: $Q_{изб}^З$ = 119,65 + 253,65 + 676,2 + 675 + 270 + 416,74 = 2,41 кВт

Так как тепловой баланс для лета больше зимнего теплового баланса, то рассчитаем теплонапряженность воздуха по формуле:

$$Q_н = \frac{Q_{изб.лето} \times 860}{V_{пом}}$$

$$Q_н = \frac{2,41 \cdot 860}{60.75} = 34,11 \text{ ккал/м3}$$

При $Q_н$ >20ккал/м^3, Δt =8 °С,

при $Q_н$ <20ккал/м^3, Δt =6 °С.

Определение количества воздуха, необходимое для поступления в помещение:

$$L = \frac{Q_{изб} \times 860}{C \times \Delta t \times \gamma}$$

$$L = \frac{2{,}41 \cdot 860}{0{,}24 \cdot 8 \cdot 1{,}206} = 895{,}01 \text{ м3/час}$$

где C=0,24 ккал/(кг · °C) – теплоемкость воздуха,

γ=1,206 кг/м^3 – удельная масса приточного воздуха.

Выбор кондиционера и место расположения

Исходя из полученных результатов, для удаления лишнего тепла и очистки воздуха нужно использовать вентиляционную систему, которая способна обеспечить требуемую подачу воздуха L=895,01 (м3/ч). В данном случае подойдет Кондиционер MIDEA MDSA-09HRFN1 INVERTER . Данный кондиционер способен обеспечить подачу воздуха до 1200 м3 /ч.

Технические характеристики:

- Мощность (охлаждение): 2.93 кВт
- Мощность (обогрев): 2.93 кВт
- Потребляемая мощность при охлаждении: 2200 Вт
- Потребляемая мощность при обогреве: 2240 Вт
- Подача воздуха более: 895.01 м3/ч
- Обслуживаемая площадь: 28 м2
- Уровень шума внутреннего блока: 37-41 дБ
- Уровень шума внешнего блока: 48 дБ
- Цвет: серый

Характеристики подключения:

- Вентиляция: 1200 м3/час
- Класс энергоэффективности при охлаждение/обогреве: А++/А+
- Электропитание, В/Гц/Ф:220 Вт
- Энергопотребление в режиме ожидания не более 1 Вт

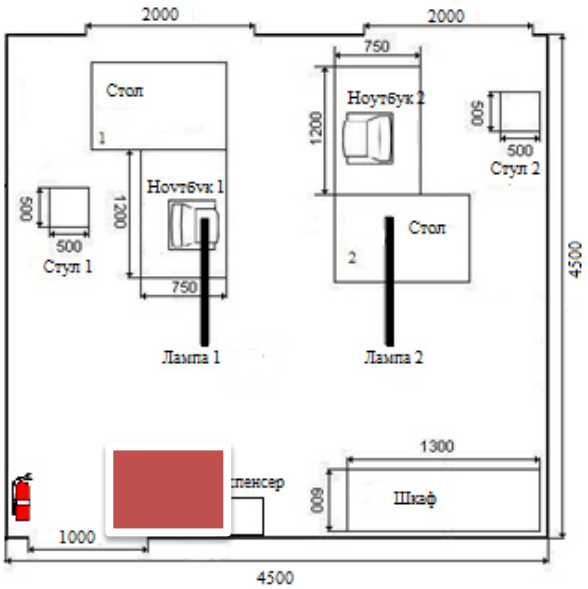


Рисунок 4.1 – Расположение кондиционера в помещений

Таблица 4.1 - Нормы микроклимата в помещении

Период года	Категории работ по уровню энерготрат, ВТ	Температура воздуха, град. С	Температура поверхностей, град. С	Относительная влажность воздуха, %	Скорость движения воздуха
Холодный	Ia (до 139)	22-24	21-25	60-40	0,1
	Iб (140-174)	21-23	20-24	60-40	0,1
	IIa (175-232)	19-21	18-22	60-40	0,2
	IIб (233-290)	17-19	16-20	60-40	0,2
	III (более 290)	16-18	15-19	60-40	0,3
Теплый	Ia (до 139)	23-25	22-26	60-40	0,1
	Iб (140-174)	22-24	21-25	60-40	0,1
	IIa (175-232)	20-22	19-23	60-40	0,2
	IIб (233-290)	19-21	18-22	60-40	0,2
	III (более 290)	18-20	17-21	60-40	0,3

4.4 Вывод по части безопасность жизнедеятельности

Здание - это совокупность помещений, представляющих собой ограниченный объем, в пределах которого протекает жизнедеятельность человека. Процесс жизнедеятельности сопровождается взаимодействием человека с окружающей его средой помещения. Правильная организация помещений и здания в целом открывает возможность обеспечения в них безопасных и эффективных условий пребывания человека. Внутренняя среда помещения, проявляющаяся в большом числе факторов воздействия на человека, называется микроклиматом помещения. Среди факторов внутренней среды выделим комплекс микроклиматических условий, оказывающих наиболее ощутимое физиологическое воздействие на человека. К ним относят тепловые условия в помещении и состав внутреннего воздуха. Человек познает мир частично через ощущения, частично сознанием. При этом непосредственно поступающая информация об окружающей среде соотносится в мозгу с информацией, накопленной в памяти на базе предыдущего опыта. Это обстоятельство свидетельствует об индивидуальности восприятия человеком внутреннего микроклимата помещения. Окружающая среда, которая не содержит раздражающих и возбуждающих факторов, препятствующих физической и умственной работе, а также отдыху, называется комфортной. Приведенное определение распространяется также на тепловые условия и состав воздуха помещения. Тепловые условия в настоящее время принято оценивать температурой

воздуха, радиационной температурой помещения, относительной влажностью и подвижностью воздуха.

Состав воздуха характеризуется концентрацией углекислоты, концентрацией вредных газов, паров, пыли. Восприятие воздуха характеризуется также озоно-ионным составом и запахами. Перечисленные параметры являются исходными при проектировании зданий и систем обеспечения микроклимата и нормируются. При этом определение нормативных параметров исходит из стремления к достижению оптимальных значений,т.е. таких, прикоторых как можно меньшее число людей было бы им и недовольно. Использование оптимальных параметров микроклимата не во всех зданиях бывает целесообразным и экономически оправданным. Поэтому в отечественных нормах широко используется понятие допустимых параметров, представляющих собой разумные граничные значения, при которых не наблюдается отрицательного воздействия на организм человека.

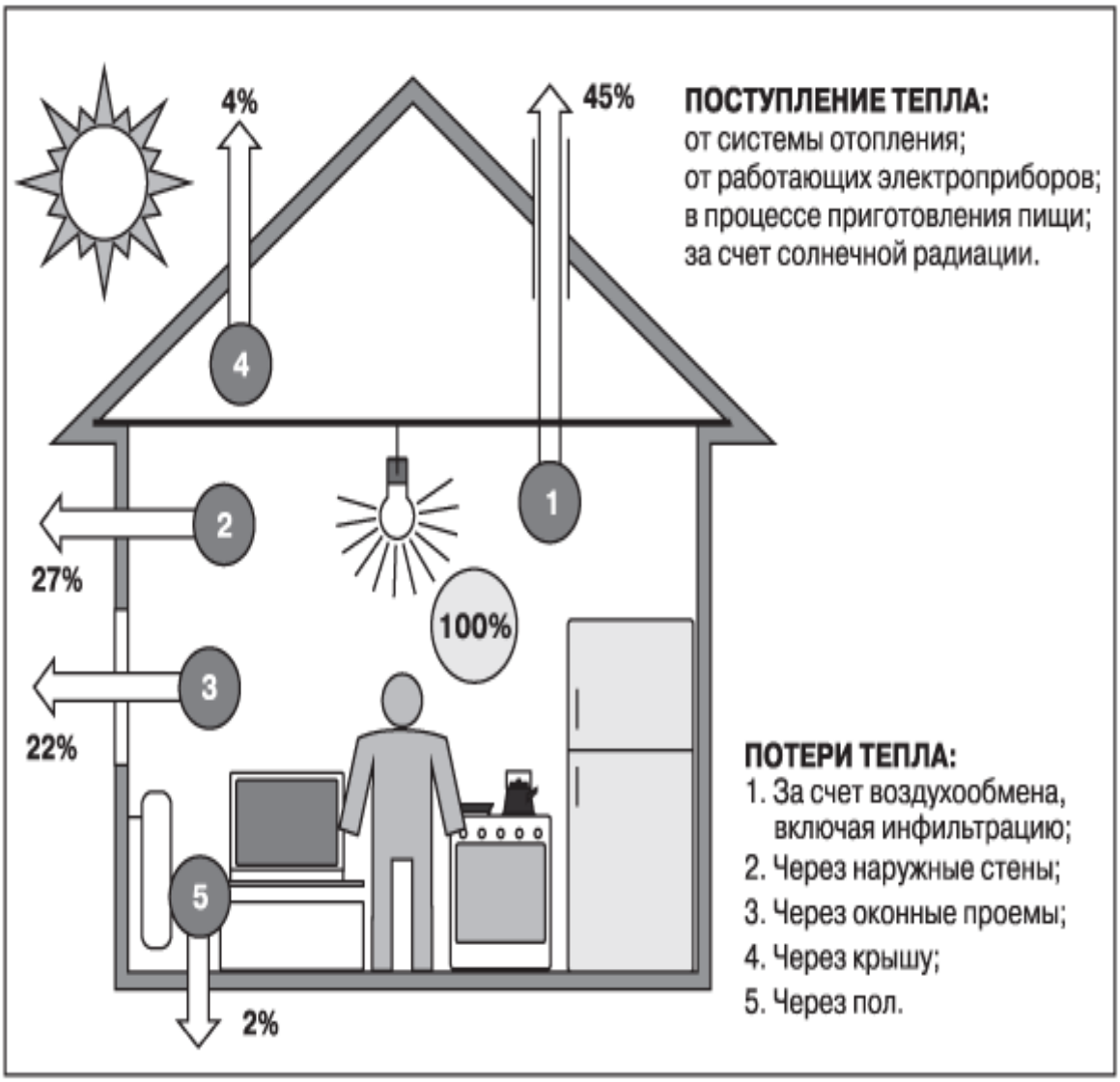


Рисунок 4.2 – Поступление и потери тепла в помещении

5 Технико-экономическое обоснование

Дипломная работа была посвящена проектированию системы защиты пользовательских данных на уровне операционной системы, которая тестировалась в виртуальной машине. Тема дипломной работы была полностью протестирована в соответствии с поставленными задачами. Капитал знаний в сфере информационных технологий позволял осуществить запланированный проект.

Технико-экономическое обоснование содержит следующие пункты:

- определение трудности построения системы защиты;
- расчет затрат на внедрение системы защиты;
- определение ценности проекта;
- оценка результатов работы системы защиты.

5.1 Определение трудности построения системы защиты

В качестве выявления трудности защиты системы, нужно выполнить разделение общей задачи на более мелкие этапы. Разделение поможет эффективно наблюдать за развитием системы защиты, за счет разделения сложной задачи на несложные легкие подзадачи. Этот метод разделения, по моему мнению, является более эффективным и позволяет результативно и быстро обрабатывать подзадачи. С помощью выведения этапов, появляется возможность определения и изучения эффективности построения. Модель распределения сложности системы защиты и стадии проектирования представлены в таблице 5.1.

Таблица 5.1 – Этапы построения системы защиты

Этапы построения системы защиты	Вид работы	Трудоемкость, чел. час.
Этап 1	Определение целей и задач	15
Этап 2	Проектирование и утверждение ТЗ на проектирование системы защиты	20
Этап 3	Поиск и изучение подобных мер защиты	20
Этап 4	Поиск и изучение сопутствующей литературы	20
Этап 5	Составление аналитических графиков системы защиты	15
Этап 6	Оформление теоретической части проекта	15
Этап 7	Разработка практической части проекта	25

Этап 8	Реализация проекта	30
Этап 9	Отладка и устранение недоработок	20
Этап 10	Тестирование системы защиты	15
Этап 11	Подведение итогов и организация отчета	40
Этап 12	Внедрение	25
Итого:		260

Продолжительность рабочего дня равна 8 часам. В результате для реализации системы защиты необходимо 32 рабочих дней.

5.2 Расчет затрат на проектирование системы

Определение затрат необходимых для построения системы защиты пользовательских данных производится на основе имеющейся сметы, которая включает следующие элементы:

- материальные затраты;
- затраты на оплату труда;
- социальный налог;
- амортизация основных фондов;
- прочие затраты.

Материальные затраты делятся на основные и вспомогательные затраты на материалы, энергию и другие затраты необходимые для построения системы защиты с помощью групповых политик. Расчет материальных затрат происходит по форме, предоставленной в таблице 5.2.

Таблица 5.2 – Затраты на материальные ресурсы

Наименование материала	Марка	Ед. измерения	Количество	Цена за ед. в тенге	Сумма в тенге
Бумага для офиса	Double A	Упаковка	4	1 950	7800
Тетрадь (96 листов)	Fruit time	Штук	3	250	750
Блокнот	Realman	Штук	3	435	1305
Ручки	Scotland	Штук	4	100	400
Компьютерная мышь	Crown	Штук	2	5 000	10000
Итого:					20 255

В процессе выполнения проекта необходимо использовать ноутбук HP Pavilion g6, технические данные ноутбука соответствуют требованиям выполнения поставленных задач перед проектом.

Общую сумму, необходимую на материальные средства ($З_м$) можно рассчитать по следующей формуле:

$$З_м = \sum P_i * Ц_i, \quad (5.1)$$

где P_i - расход i-го вида материального ресурса, натуральные единицы;

$Ц_i$ - цена за единицу i-го вида материального ресурса, тг;

i - вид материального ресурса;

n - количество видов материальных ресурсов.

Расчет затрат на необходимое оборудование и программное обеспечение производится по форме, приведенной в таблице 5.3.

Таблица 5.3 – Расчет затрат на оборудование и ПО, необходимого для проекта

Наименование материала	Марка	Ед. измерения	Количество	Цена за ед. в тенге	Сумма в тенге
Ноутбук	HP Pavilion	Штук	1	100 000	100 000
Принтер	Epson Expression Home XP-352	Штук	1	42 599	42 599
Хостинг	hostgator.com	Штук	2	3 350	6 700
Модем	Tenda D810R	Штук	1	2 900	2 900
Домен	hostgator.com	Штук	1	4 448	4 448
Итого:					156 647

Зм = 20 255 + 156 647 = 176 902 (тг)

Для реализации программного обеспечения необходимы материалы на сумму 176 902 тенге.

5.3 Расчет затрат на электроэнергию

В выполнении проекта, целью которой является проектирование системы защиты на уровне операционной системы необходимо использование электроэнергии. Справедливым будет произвести расчет на электроэнергию.

Согласно таблице 5.1 для проектирования системы защиты необходимо порядка 260 часов, теперь необходимо рассчитать стоимость электроэнергии, которая будет потрачена в течении 260 часов. Для принтера расчет будет проводиться для периода в 24 часа, так как нет необходимости постоянно использовать принтер.

$$Э = З_{эл.эн.обор.} + З_{доп.нужды.}, \quad (5.2)$$

где $З_{эл.эн.обор.}$ – затраты на электроэнергию оборудования;

$З_{доп.нужды.}$ – затраты электроэнергии на дополнительные нужды.

Расчет электроэнергии, которая необходима для оборудования определяется по следующей формуле:

$$З_{эл.эн.обор.} = \sum W * К_{исц} * S * T, \quad (5.3)$$

где W – потребляемая мощность, Вт;

$К_{исц}$ – коэффициент использования ($К_{исц}$ = 0,7..0,9);

Т – время работы;

S – тариф (1кВт/ч = 18,32 тг).

Итоги по расчетам стоимости затрачиваемой электроэнергии представлены в таблице 4.4.

Таблица 5.4 – Затраты на электроэнергию

Наименование приборов	Паспортная мощность, кВт	Коэффициент мощности	Время работы оборудования, ч	Цена ЭЭ тг/кВтч	Сумма, тг.
Ноутбук	0,6	0,7	260	18,32	2000,54
Модем	0,08	0,9	260	18,32	342,95
Принтер	0,5	0,9	24	18,32	197,85
Кондиционер	0,8	0,9	180	18,32	2374,27
Освещение	0,3	0,7	260	18,32	1000,27
Итого:					5915,88

$$З_{эл.эн.обор.} = 5915{,}88 \text{ (тенге)}$$

На дополнительные потребности расходы подсчитываются на основе повышенного показателя в объеме 5% от расходов на электроэнергию:

$$З_{доп.нужды} = 5\% * З_{эл.эн.обор.}, \quad (5.4)$$

Определим затраты на дополнительные потребности согласно формуле (4.4):

$$З_{доп.нужды} = 0.05 * 5915{,}88 = 295{,}794 \text{ (тенге)}$$

Исходя из всех расчетов, полные расходы на электроэнергию составляют:

$$Э = 295{,}794 + 5915{,}88 = 6211{,}674 \text{ (тенге)}$$

5.4 Расчет затрат на оплату труда

Для проектирования системы защиты, как указывалось ранее, необходимо два работника:

- руководитель проекта (управление рабочим временем, корректировка рабочих процессов, координация, изучение предметной области);
- проектировщик системы защиты, тестирование и сопровождение.

Сумму расходов на оплату труда можно рассчитать по следующей формуле:

$$З_{тр} = \sum ЧС_i * T_i \quad (5.5)$$

где $ЧС_i$ - часовая ставка i-го работника, тг;

T_i - трудоемкость разработки модели, чел.×ч; i - категория работника;

n - количество работников, занятых разработкой ПП.

Во время реализации проекта рабочее время участников не равномерно, поэтому имеет смысл установить часовую ставку каждого работника и общий объем заработной платы.

Часовую ставку сотрудника можно рассчитать по следующей формуле:

$$ЧС_i = \frac{ЗП_i}{ФРВ_i} \quad (5.6)$$

где $ЗП_i$ - месячная заработная плата i-го работника, тг;

$ФРВ_i$ - месячный фонд рабочего времени i-го работника, час.

Месячная заработная плата руководителя равняется 178 000 тенге и месячная заработная плата проектировщика равняется 142 000 тенге. Рассчитаем часовую ставку каждого работника согласно формуле (5.6):

$$ЧС_{руководитель} = \frac{178\,000}{22 * 8} = 1\,011{,}36 \text{ тг/ч}$$

$$ЧС_{проектировщик} = \frac{142\,000}{22 * 8} = 806{,}8 \text{ тг/ч}$$

Часовая ставка руководителя составляет 1 011,36 (тг/ч), трудоемкость проектирования равняется 100 часам. Часовая ставка проектировщика составляет 806,8 (тг/ч), трудоемкость разработки равняется 260 часам. Согласно формуле (4.5) можно рассчитать сумму расходов на заработную плату работников:

$$З_{тр} = 1011{,}36 * 100 + 806{,}8 * 260 = 101136 + 209\,768 = 310\,904$$

Расчеты затрат по оплате труда показаны в таблице (5.5).

Таблица 5.5. – Расчет заработной платы

Категория работника	Квалификация	Трудоемкость разработки ПП, час.	Часовая ставка, тг/ч	Сумма, тг.
Руководитель проекта	Инженер-проектировщик	100	1011,36	101 136
Проектировщик	Системный администратор	260	806,8	209 768
Итого:				310 904

5.5 Расчет затрат по социальному налогу

Согласно Налоговому кодексу Республики Казахстан социальный налог составляет 9,5% от фонда оплаты труда. Социальный налог можно рассчитать по следующей формуле:

$$С_н = (ФОТ - ПО) * 0{,}095 \quad (5.7)$$

где ПО - отчисления в пенсионный фонд, они составляют 10% от ФОТ.

$$ПО = 310\,904 * 0{,}1 = 31\,090{,}4 \text{ тенге}$$

$$С_н = (310\,904 - 31\,090{,}4) * 0{,}095 = 26\,582{,}2 \text{ тенге}$$

Результаты расчетов представлены в таблице (5.6):

Таблица 5.6 – Начисление социального налога

Категория работника	Количество человек	Заработная плата, тг	Пенсионные отчисления, тг	Социальный налог, тг
Руководитель проекта	1	101 136	10 113	8 647,1
Проектировщик	1	209 768	20 976	17 935,2
Итого:				26 582,3

5.6 Амортизация основных фондов и прочие затраты

Нормы амортизации ОФ необходимо определить в соответствии с налоговым кодексом РК. Амортизацию ОФ можно определить по следующей формуле:

$$A_г = \frac{С_{об} * Н_а}{100} \quad (5.8)$$

где, $С_{об}$ – стоимость оборудования;

$Н_а$ – норма амортизации (норма амортизация = 25);

Формула (5.8) позволяет рассчитать нужную сумму для амортизационных отчислений за год для ноутбука:

$$A_г = \frac{100\,000 * 25}{100} = 25\,000 \text{ тенге}$$

Теперь необходимо рассчитать норму амортизации за период проектирования:

$$A_г = \frac{25000 * 32}{365} = 2\,191{,}7 \text{ тенге}$$

Подобным образом необходимо рассчитать норму амортизации для всего оборудования. Результаты расчетов приведены в таблице (5.7).

Таблица 5.7 – Амортизация ОФ

Наименование оборудования и ПО	Стоимость оборудования и ПО, тг	Годовая норма амортизации, %	Сумма амортизации за год, тг	Сумма амортизации за время проектирования, тг
Ноутбук	100 000	25	25 000	2 191,7
Принтер	42 599	25	10 649	933,61
Модем	2 900	20	580	50,8
Хостинг	3 350	20	670	58,73
Домен	4 448	15	667	58,47
Итого:			37 566	3 293,31

Смета расходов на разработку ПО.

На основе всех представленных расчетов необходимо оформить смету расходов на проектирование системы защиты согласно форме, которая приведена в таблице (5.8). На рисунке (5.1) продемонстрирована диаграмма рабочих расходов.

Таблица 5.8 – Смета затрат на проектирование системы защиты

Статьи затрат	Сумма, тг
Затраты на оборудование	156 647
Затраты на программное обеспечение	0
Затраты на оплату труда	310 904
Социальные налоги	26 582,3
Затраты на электроэнергию	5915,88
Амортизация основных фондов	3 293,31
Прочие расходы	30 600
Итого по смете:	533 942,49

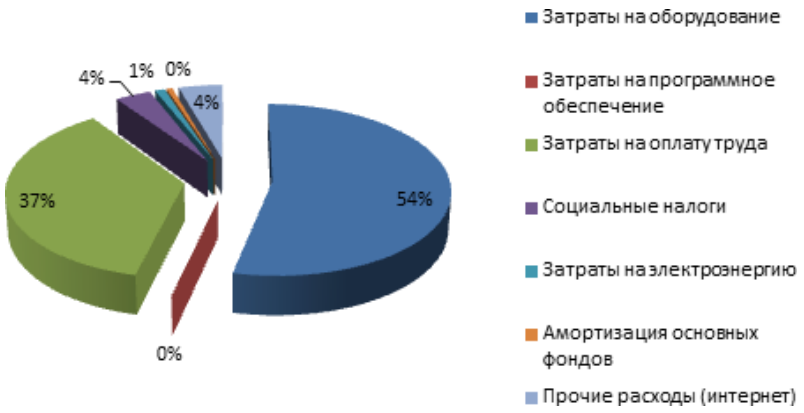


Рисунок 5.1 – Диаграмма затрат

5.7 Определение возможной (договорной) цены системы защиты

Стоимость системы защиты определяется на основе качества разработанной системы, сроков его проектирования и производительности. Стоимость $Ц_Д$ для системы защиты можно рассчитать по следующей формуле:

$$Ц_Д = З_{нир}\left(1 + \frac{P}{100}\right), \qquad (5.9)$$

где $З_{нир}$ – затраты на проектирование системы защиты, тг;

Р – средний уровень рентабельности, (%). Данный параметр принят равным 25%.

Прибыль = 533 942,49 * 0,25 = 133 485, 62 тенге

$$Ц_Д = 533\,942{,}49\left(1 + \frac{25}{100}\right) = 533\,942{,}49 + 533\,942{,}49 * 0{,}25$$
$$= 667\,428{,}11 \text{ тенге}$$

Далее необходимо определить стоимость реализации с учетом НДС, ставка НДС устанавливается законодательством РК. На 2019 года ставка НДС составляет 12%. Стоимость реализации учитывая НДС можно рассчитать по следующей формуле:

$$Ц_р = Ц_д + Ц_д * НДС, \qquad (5.10)$$

$$Ц_р = 667\,428{,}11 + 667\,428{,}11 * 0{,}12 = 747\,519{,}49 \text{ тенге}$$

Результатом расчетов является: прибыль равна 133 485, 62 тенге , смета затрат на проектирование системы защиты равна 533 942,49 тенге , стоимость равна 667 428,11 тенге.

Заключение

В процессе написания дипломного проекта была спроектирована и внедрена система защиты пользовательских данных на уровне операционной системы в виртуальной машине “VMware Workstation”. При проектировании были изучены принципы и методы построения системы защиты пользовательских данных, включая анализ технологических средств обеспечения защиты, таких как межсетевой экран, групповые политики, а также антивирусы. Программное обеспечение выбрано с учетом функциональных возможностей, системных требований, совместимости с операционными системами. С учетом требовании безопасности корпоративной сети, была построена система защиты с помощью встроенных возможностей безопасности операционной системы. Были применены ряд политик относящиеся к параметрам безопасности. Для построения сети были установлены две операционные системы в виртуальной машине. Windows 10, который был клиентом и на ней применялись политики безопасности в целях улучшения защиты пользователя от несанкционированного доступа. Windows Server 2012, где были установлены каталоги службы безопасности Active Directory. Развернуты и внедрены были такие службы как DHCP и DNS. Также в процессе работы была установлена корпоративная доменная сеть, где доменом сети являлся icoo.kz. В корпоративном домене была определенная структура, которая включала в себя подразделения, группы и пользователей. Компьютер, который параллельно был установлен в виртуальной машине, впоследствии был добавлен в домен. Для развития защиты пользовательских данных были выполнены работы с резервным копированием и шифрованием.

В проекте также были рассчитаны оптимальные условия труда при проектировании системы защиты пользовательских данных, включающие в себя расчет тепловых нагрузок в помещении, необходимого для нормального функционирования сети. Система является целесообразной с точки зрения экономической эффективности, так как затраты на проектирование системы защиты являются минимальными.

Список литературы

1. Справочник системного администратора, И.В.Коробко. Операционные системы и сети, 2009.
2. Microsoft Windows 7. Руководство администратора, Алексей Чермарев. Операционные системы и сети, 2010.
3. Windows IT Pro/RE, Открытые системы. Операционные системы и сети, 2013.
4. Jason Todd. Deploying a Vyatta Core Firewall – USA: Sans Institute, 2010.
5. Tim Boyles. CCNA Security Study Guide – Indianapolis USA: SyBEX, 2012.
6. Белов С.В. Безопасность жизнедеятельности. М: Высшая школа 1999.
7. Баклашов Н.И., Китаева Н.Ж., Терехов Б.Д. Охрана труда на предприятиях связи и охрана окружающей среды. – М.: Радио и связь, 1989.
8. Кошулько Л.П., Суляева Н.Г., Генбач А.А. Производственное освещение. Методические указания. – Алматы:АИЭС, 1989.
9. Абдимуратов Ж.С., Мананбаева С.Е. Безопасность жизнедеятельности. Методические указания к выполнению раздела «Расчет производственного освещения» в выпускных работах для всех специальностей. – Алматы, 2009.
10. Корольченко А.В. Естественное и искусственное освещение. - М.: Издательство Москва, 2004.
11. Дюсебаев М.К. Безопасность жизнедеятельности: методические указания к выполнению раздела дипломных проектов. – Алматы.: АИЭС, 2003.
12. Голубицкая Е. А.,. Жигульская Г. М. Экономика связи. – М.: Радио и связь, 2000.
13. Аманжолова К. Б., Алибаева С. А. Экономика предприятии телекоммуникации: Учебное пособие. - Алматы: АИЭС, 2003.
14. Облачные технологии для бизнеса. URL: http://profitday.kz/cloud (дата обращения: 17.03.2016)
15. Cbtnuggets: GNS3 1.x Fundamentals. URL: www.cbtnuggets.com/it-training/gns3-1-x-fundamentals (дата обращения: 26.02.2016)