**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**Одеський коледж комп’ютерних технологій «Сервер»**

циклова комісія «Професійної та практичної підготовки з комп’ютерних технологій»

**РОЗРАХУНКОВО-ГРАФІЧНА РОБОТА З ТЕХНОЛОГІЙ ЗАХИСТУ ІНФОРМАЦІЇ**

Тема роботи **– «**Впровадження алгоритмів шифрування, та інші засоби інформаційної безпеки в сучасні підприемства**»**

Спеціальність 121 - Інженерія програмного забезпечення

Дипломна робота молодшого спеціаліста

ВИКОНАВ:

Студент групи  К17      \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_     В.В. Шишелов

КЕРІВНИК:      \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_    Д.С. Шибаєв

Одеса – 2020

СОДЕРЖАНИЕ

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ ДЛЯ ДИПЛОМНОГО ПРОЕКТА**

В дипломній роботі розглядається принцип роботи, можливості та особливості ролі мережевого екрану на підприємстві під управлінням операційної системи Windows Server 2019 .

«DATA.Net» - підприємство інтернет-провайдер, яке забезпечує якісним інтернет покриттям місто з населенням 2500 чоловік. Підприємство займається постачанням якісного та захищеного інтернет трафіку користувачам за допомогою технологій GPON та FireWall.

**Мета дипломної роботи**

Метою дипломної роботи є впровадження технології FireWall у підприємство постачання інтернет трафіку під управлінням ОС Windows Server 2019.

**Вхідні дані**

Підприємство «DATA.Net» базується у двох будівлях. Перша двоповерхова будівля призначена для керуючого та обслуговуючого персоналу підприємства. Друга будівля призначена для технічного персоналу та зберігання матеріалів монтажу та ремонту ліній передачі трафіку. В цих будівлях знаходяться наступні кабінети:

* Генеральний директор - 1 працівник (через своїх заступників і відповідні відділи здійснює керівництво всією виробничої, господарської та фінансової діяльністю).
* Заступник директора - 1 працівник, як правило, є першим заступником директора. Він безпосередньо керує основною виробничою діяльністю.
* Головний інженер - 1 працівник, здійснює технічне керівництво. Він очолює роботи з розвитку та реконструкції мереж.
* Заступник з економічних питань - 1 працівник, керує роботами по перспективному і поточному планування та обліку господарської діяльності, займається питаннями оптимізації та ефективності діяльності підприємства, організацією праці та заробітної плати, автоматизацією управління персоналом.
* Комерційний відділ - 3 працівника, розробляє проекти договірних умов з клієнтурою, проекти місцевих тарифів на надання послуг провайдера, розглядає претензії і позови.
* Відділ матеріально-технічного постачання - 2 працівника, забезпечує підприємство обладнанням, матеріалами, інструментом. Складає зведені заявки на всі види постачання і організовує задоволення цих заявок. Організовує прийом, зберігання і видачу обладнання і матеріалів за заявками, контролюючи при цьому норми витрат.
* Відділ організації праці та заробітної плати - 2 працівника, займається питаннями нормування праці та його вдосконаленням, розробкою місцевих норм праці; складає штатний розклад і здійснює контроль за витрачанням фонду заробітної плати, контролює дотримання штатної дисципліни і трудового законодавства; готує матеріали по підведенню його підсумків.
* Бухгалтерія - 3 працівника, веде облік, контроль і аналіз виробничо-фінансової діяльності підприємства в грошовому вираженні; контролює прийом і витрачання матеріалів та платіжок за послуги підприемства, нараховує і видає заробітну плату, складає звіти і баланси.
* Відділ серверної - 1 працівник, забезпечується збір інформації, її обробка відповідно до характеру вирішуваних завдань, проводиться аналіз отриманої інформації, здійснюється розробка оптимальних рішень і передає їх для виконання відповідним підрозділам підприємства.
* Відділ кадрів - 2 працівника займається підбором, вивченням і розстановкою кадрів за діловими якостями; розробляє заявки на підготовку інженерно-технічних працівників і робітників; закріплення кадрів; аналізує та узагальнює причини плинності кадрів і вживає заходів до усунення цього явища; веде облік кадрів.
* Відділ маркетингу – 2 працівника займаються розповсюдженням інформації про підприємство, розробляють нові маркетингові ідеї для притянення нових клієнтів.
* Відділ абонентів – 3 працівника займаються прийняттям і обробкою запитів від абонентів.
* Технічний відділ – 20 працівників що займаються монтажем, демонтажем, модернізацією, ремонтом мереж та підключенням нових абонентів.
* Відділ безпеки – 2 працівника агенства охорони, відповідають за безпеку будівлі і майна підприємства.
* Кол-центр – 3 працівника, відповідають на питання та переадресовують на інші відділи.
* Юридичний відділ – 2 працівника займаються юридичними питаннями та проблемами.

**Завдання дипломної роботи**

До виконання дипломної роботи входять наступні пункти:

* Виконати порівняльний аналіз технологій мережевих екранів.
* Зробити проектування локальної мережі: вибір технології, топології, та мережної адресації, обладнання, підключення до глобальної мережі, кабельні системи.
* Зробити розрахунок вартості мережевого обладнання: комп'ютерів, периферійних пристроїв, серверного та мережевого обладнання для підприємства.
* Виконати опис конфігурування мережевого екрану та інших служб серверів підприємства за допомогою Windows Server 2019.
* Виконати впровадження FireWall у підприєство.
* Розрахувати економічні витрати на реалізацію дипломного проекту.

**Вимоги дипломної роботи**

* Налаштувати мережеві пристої на підприємстві.
* Забезпечити доступ до мережі Інтернет зі швидкістю 1000 Мбіт/сек.
* Реалізувати резервний iнтернет-канал.
* Забезпечити резервне щоденне копіювання даних.
* Втілити впровадження технології FireWall на підприємстві.
* Забезпечити облік бухгалтерії на підприємстві.
* Забезпечити доступ користувачів різних підрозділів підприємства до файлового серверу.
* Реалізувати відмовостійкість серверноі інфраструктури.

**План будівлі та топологія мережі**

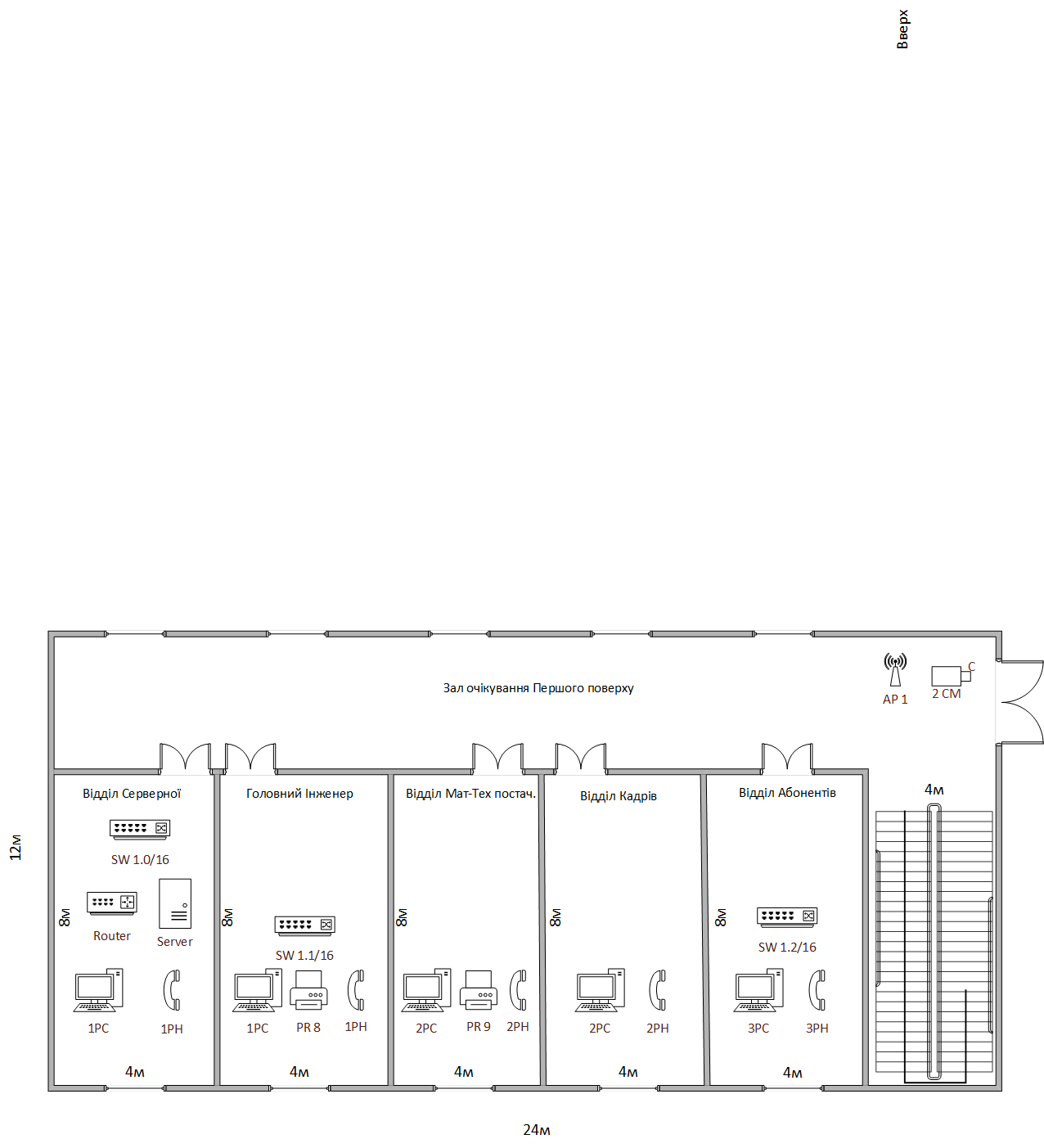


Рисунок 1. План першого поверху будівлі

 Рисунок 2. План другого поверху будівлі

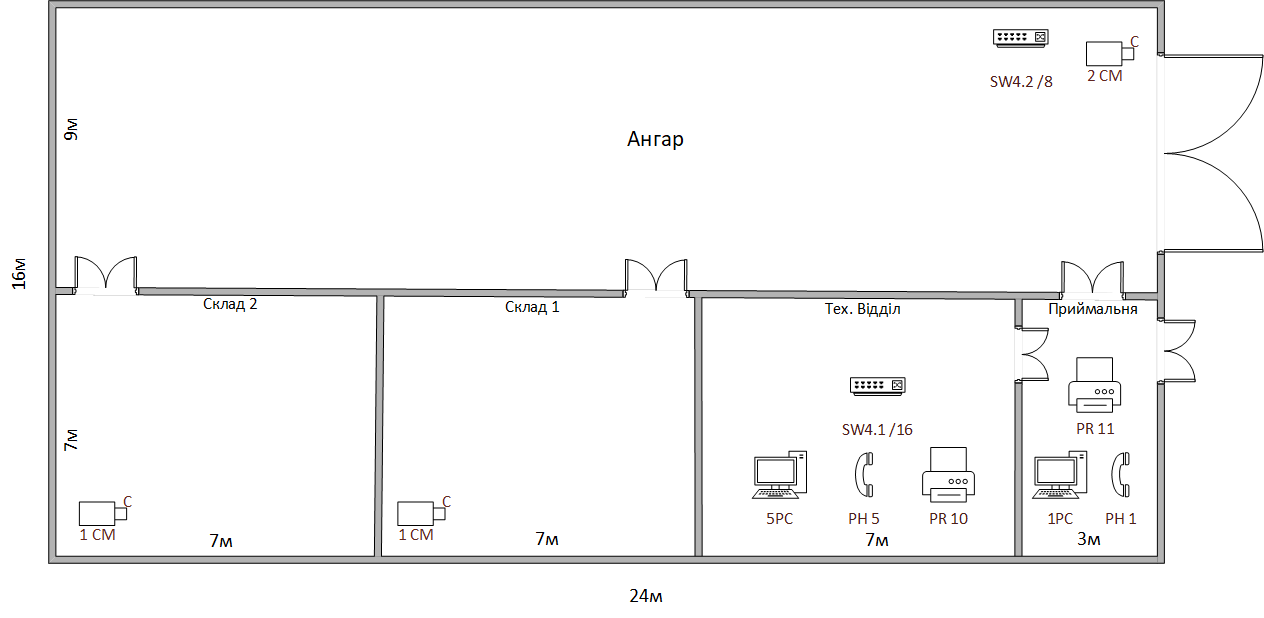


Рисунок 3. План технічної будівлі

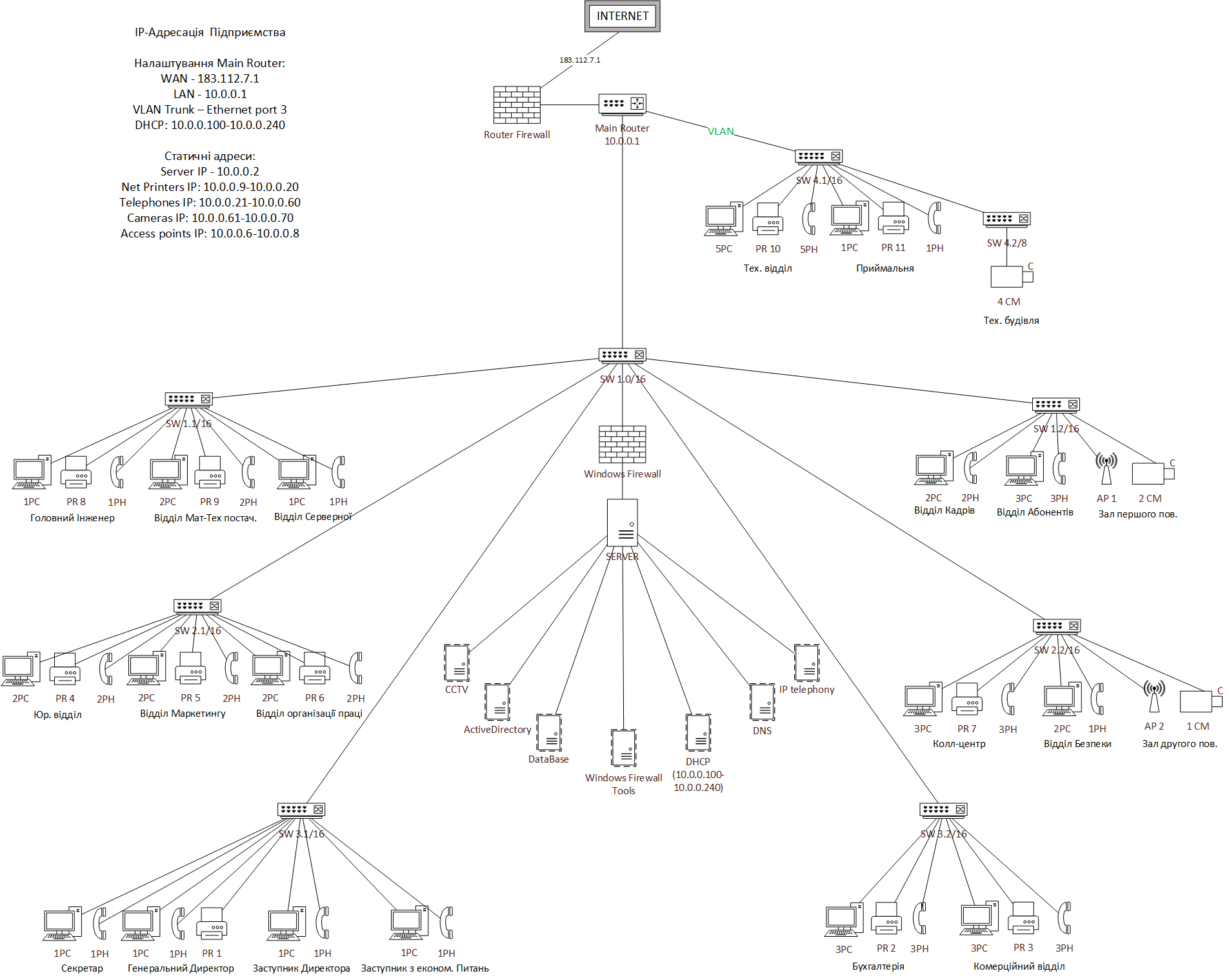


Рисунок 4. Топологія локальної мережі підприємства

**СМЕТА ДИПЛОМНОГО ПРОЕКТА**

# Сетевое оборудование используемое в проэкте.

1. Серверы AD - Lenovo ThinkSystem SR530 SILVER4108 16GB/7X08A01W(рис 1.)



Рисунок 1

Технические характеристики:

* Форм-фактор - 1U
* Оперативная память - DDR4 2933MHz
* Разъемы расширения - 3 PCIe 3.0
* Отсеки для накопителей - 8
* Сетевые интерфейсы - 2 порта 1GbE + 1GbE для управления.
* Процессор - 2 х Intel Xeon scalable

1. Сервер FTP - Synology RS1219+ (рис 2.)



Рисунок 2

Технические характеристики:

* Форм-фактор - 2U
* Количество отсеков под жесткие диски – 8
* Скорость сетевеой карты – 1Гбит/с
* Память – DDR3 2GB (с расширением до 16GB)
* Производительность – 1310Мб/с
* Глубина – 12 дюймов
* Процессор – 4 ядра, 2.4 ГГц
* Максимальная емкость – 128 ТБ

1. Маршрутизатор - MIKROTIK CCR1009-7G-1C-1S+ (рис 3.)



Рисунок 3

Технические характеристики:

* Форм-фактор - 1U
* SFP порты - 2
* Ethernet порты – 8
* COM
* USB 4G
* Скорость сетевеой карты – 1Гбит/с
* VPN

1. Коммутатор 8п.(сервер) - CISCO SG110D-08HP-EU(рис 4.)



Рисунок 4

Технические характеристики:

* Тип -неуправляемый
* Форм-фактор - настольный
* Количество портов - 8
* Порты - Gigabit Ethernet
* Требования PoE - PoE 802.3af (PSE) до 15.4 Вт на порт

1. Коммутатор 16п.(для офиса) - TP-LINK TL-SF1016DS(рис 6.)



Рисунок 6

Технические характеристики:

* Тип - неуправляемый
* Форм-фактор - настольный/в стойку U1
* Количество портов16
* ПортыFast Ethernet

1. Точка доступа - MIKROTIK RBCAPGI-5ACD2ND(рис 9.)



Рисунок 9

Технические характеристики:

* Режимы работыWi-Fi точка
* Стандарты сетейb (до 11 Мбит/с), g (до 54 Мбит/с), n (до 300 Мбит/с), ac (до 867 Мбит/с)
* Рабочая частота2.4 / 5 ГГц
* Тип антеннывстроенная/несъемная

1. Кабель сетевой - OK-NET UTP-CAT.5E LSFROH 305М (рис 10.)

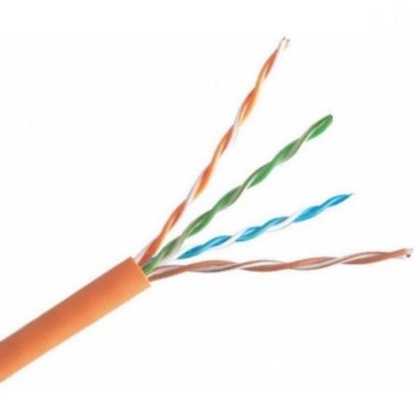


Рисунок 10

Технические характеристики:

* Артикул – КП Внг-HF-ВП(350) 4\*2\*0,51
* Тип кабеля - UTP
* Материал - медь
* Длина - 305 м
* Сечение - 0.51 мм
* Категория - cat 5e

1. Телекоммуникационный шкаф (рис 11.)



Рисунок 11

* Вместимость - 15U
* Окно органайзер
* Замок



# Перечень конфигураций ПК и перифирии.



# Перечень выполняемых монтажных работ.



ПРОФИЛАКТИКА И ВЫЯВЛЕНИЕ ПРОБЛЕМ С БЕЗОПАСНОСТЬЮ

В рамках работы по информационной безопасности, стоит выделить некоторые пожелания и уязвимости в предприятии, которые необходимо решить:

* Шифрование жестких дисков.
* Проблема паролей.
* Авторизация в системе.
* Защита от атак типа «Denial Of Service».
* Защита веб-приложений.

1. СПЕЦИФИКА ОРГАНИЗАЦИИ ПРЕДПРИЯТИЯ С ОБЕСПЕЧЕНИЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

Темой работы является IT-компания, что делает ее намного более ценной жертвой, чем любое другое лицо. Как минимум уже существует возможность угрозы со стороны конкурентов, взломщиков, целю которых является вымогательство денег, новички в сфере информационной безопасности, желающие закрепить свои умения на практике. Именно поэтому стоит выделить самые популярные уязвимости, встречающиеся на предприятиях и решить их, дабы отсечь большую часть возможных атак.

Возвращаясь к первому разделу, следует разобрать каждый пункт и тем или иным образом решить его:

* Шифрование жестких дисков.

Большое количество компаний подписывает контракт со своими работниками о неразглашении, что подразумевает нахождении разработки и исходного проекта в состоянии полной секретности. Компания должна быть в силах обеспечить невозможность компрометации данных как через сеть, так и через непосредственное взаимодействие пользователя с аппаратной частью. Самым лучшим решением в этой ситуации было бы шифрование жестких дисков.

Так как работа на предприятии происходит с операционными системами Windows 10, Windows Server, лучшим решением в этой ситуации является использование программы bitlocker.

Bitlocker в качестве алгоритма шифрования использует алгоритмы AES 128, AES 256 и создает ключ, который может храниться как на USB, так и на компьютере. Шифр AES является симметричным алгоритмом шифрования. Использует 10 – 14 раундов (в зависимости от ключа).

Последовательность работы с bitlocker изображена на примере flash-накопителя на операционной системе Windows 10 Pro на рисунках 3.1 – 3.10.

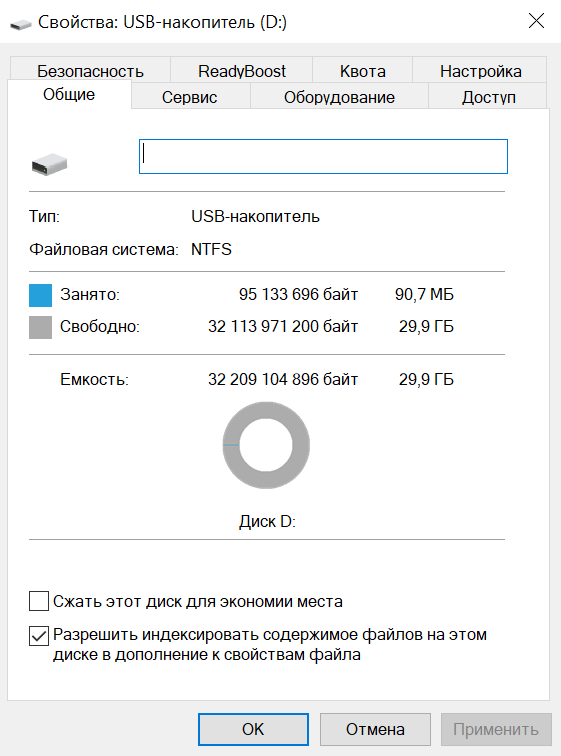


Рисунок 3.1.1 – Изначальное состояние флеш-накопителя.

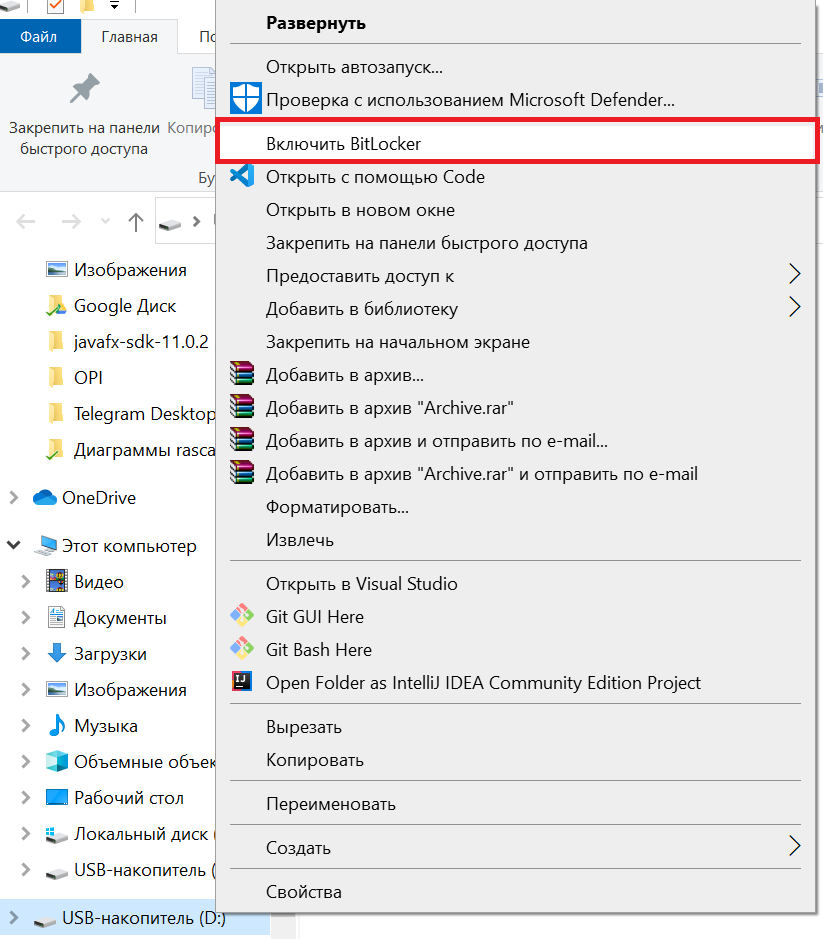


Рисунок 3.1.2 – Инициируем запуск BitLocker на флэш-накопителе.

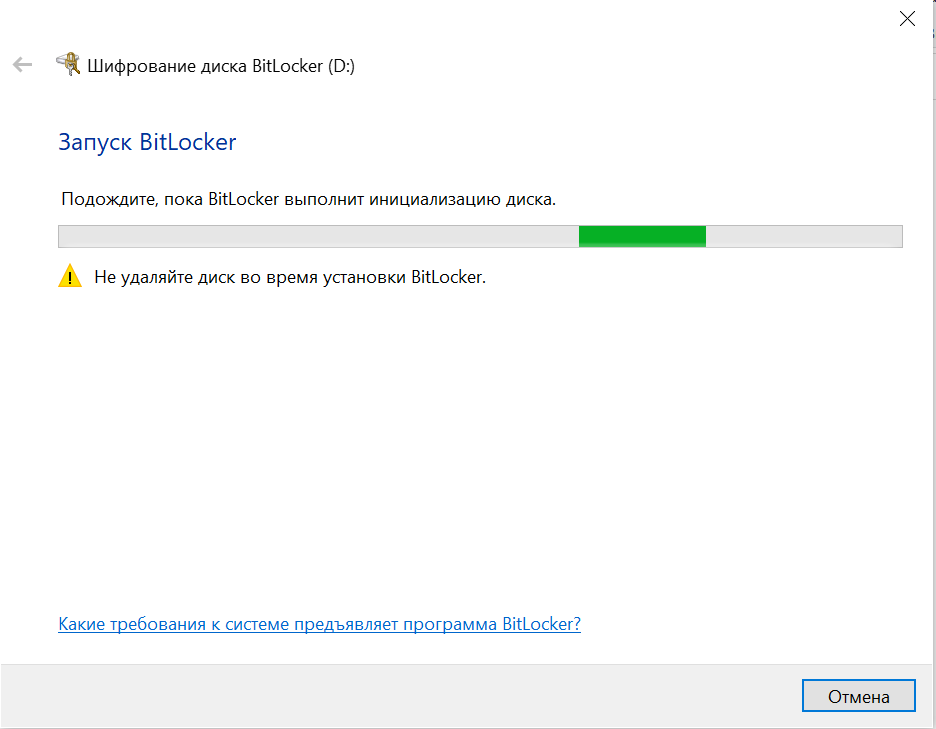


Рисунок 3.1.3 – Запуск Bitlocker.

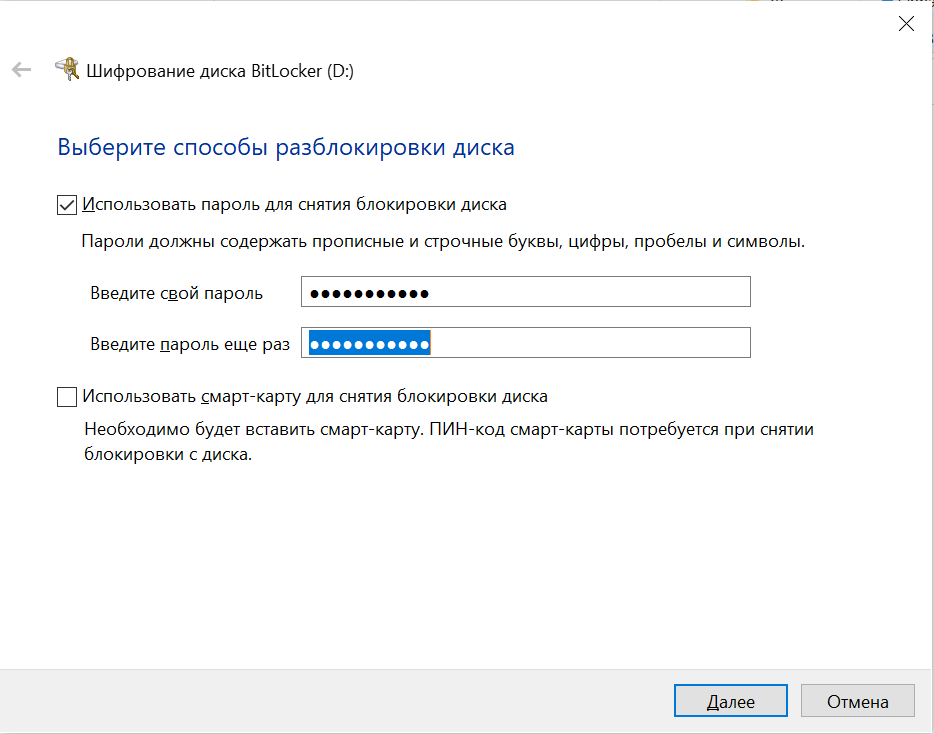


Рисунок 3.1.4 – Выбор способа разблокировки.

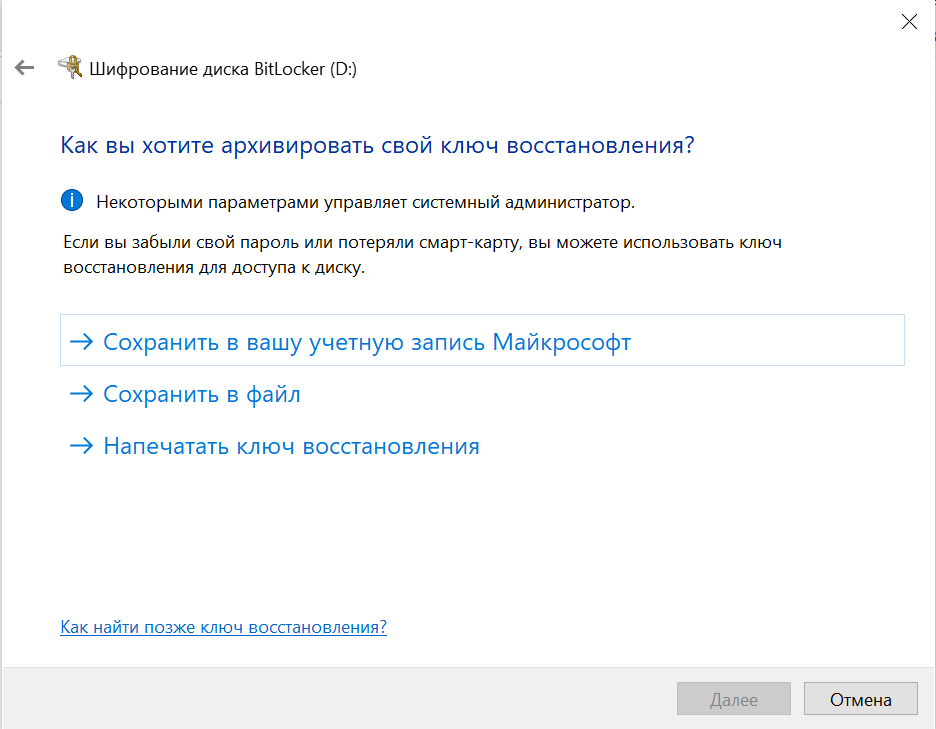


Рисунок 3.1.5 – На случай потери пароля, добавляем возможность восстановления.

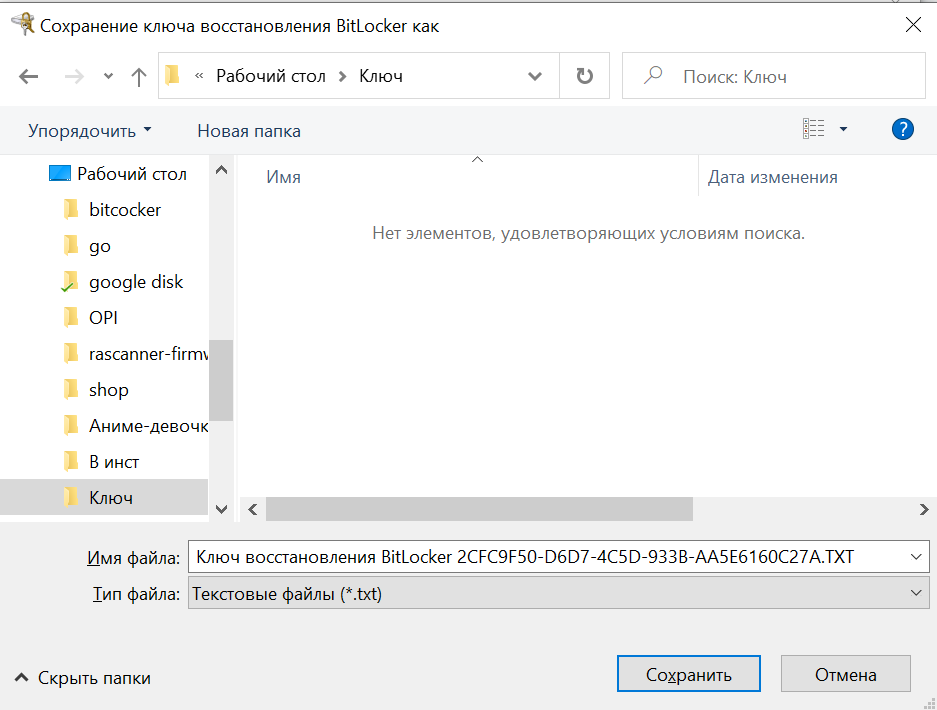


Рисунок 3.1.6 – Выбираем путь сохранения файла.

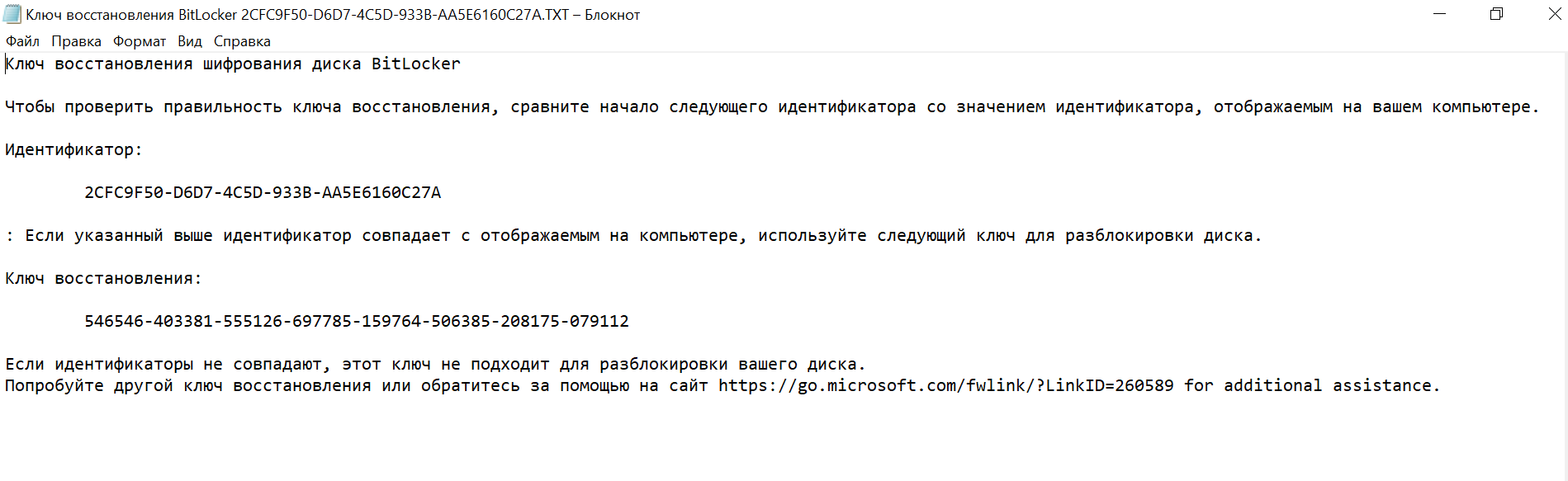


Рисунок 3.1.7 – Содержимое файла с ключом восстановления.

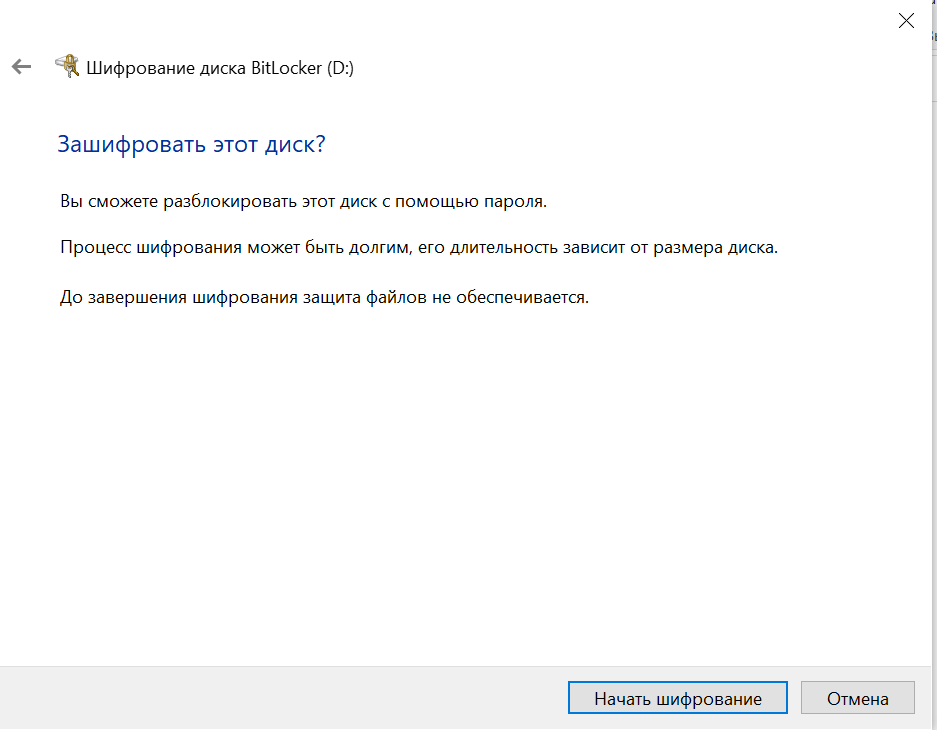


Рисунок 3.1.8 – Начинаем шифрование.

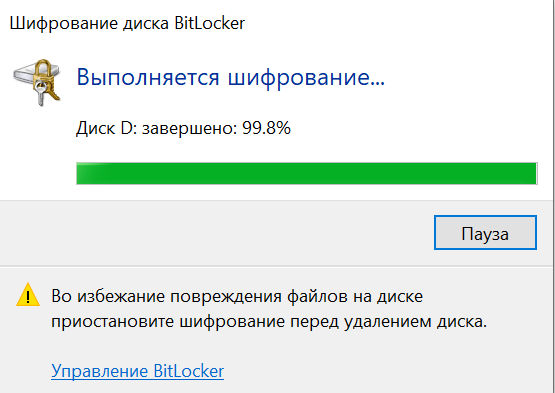


Рисунок 3.1.9 – Процесс шифрования.

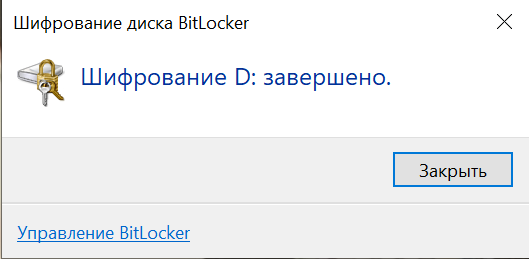


Рисунок 3.1.10 – окончание процесса шифрования.

После шифрования флэш-накопителя, вставляем его в другой заново в компьютер и видим предложение разблокировать флэш-накопитель (рис. 3.11).

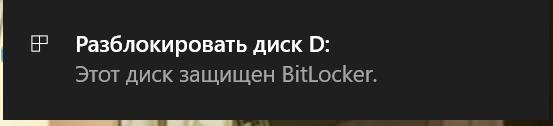


Рисунок 3.1.11 – Предложение разблокировать bitlocker.

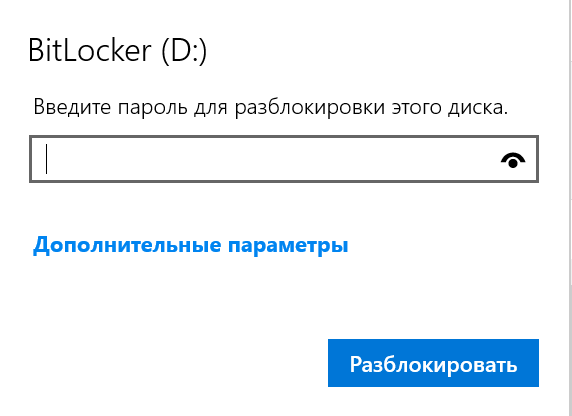


Рисунок 3.1.12 – Ввод ключа.

После этих действий, данные флэш-накопителя становятся доступными.

При использовании bitlocker, любой, кто сможет забрать жесткий диск с важной информацией не сможет прочитать его без соответствующего ключа. Подобная защита сможет защитить как от обычного промышленного шпионажа, так и от прямого рейдерского захвата.

* Проблема паролей.

Суть проблемы паролей заключается в том, что пользователь в силу нежелания запоминать пароли, используют слабые пароли или же повторяющиеся пароли на сайтах, в системе, что обеспечивает человеку со стороны более простую задачу в плане взлома пароля пользователя и несанкционированного входа в систему. В качестве решения было решено создать программное обеспечение, представляющее из себя зашифрованную базу данных, доступ к которой можно получить, зная всего один, но сложный пароль.

Одним из лучших решений в этой сфере является Kaspersky Password Manager. Он предоставляет на выбор большое количество функционала, включая расширение для браузеров chrome, firefox, для автоматизации рутинных задач. Kapsersky password manager использует такие виды шифрования, как: DES, 3DES, 3DES TWO KEY, RC2, RC4, AES.

Демонстрация работы изображена на рисунках 3.2.1 – 3.2.

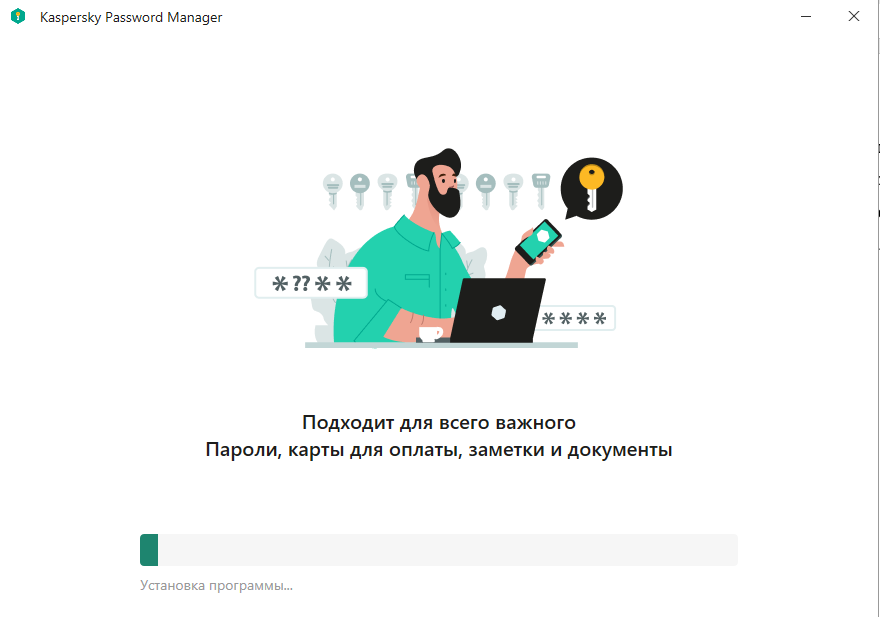


Рисунок 3.2.1 – Установка.

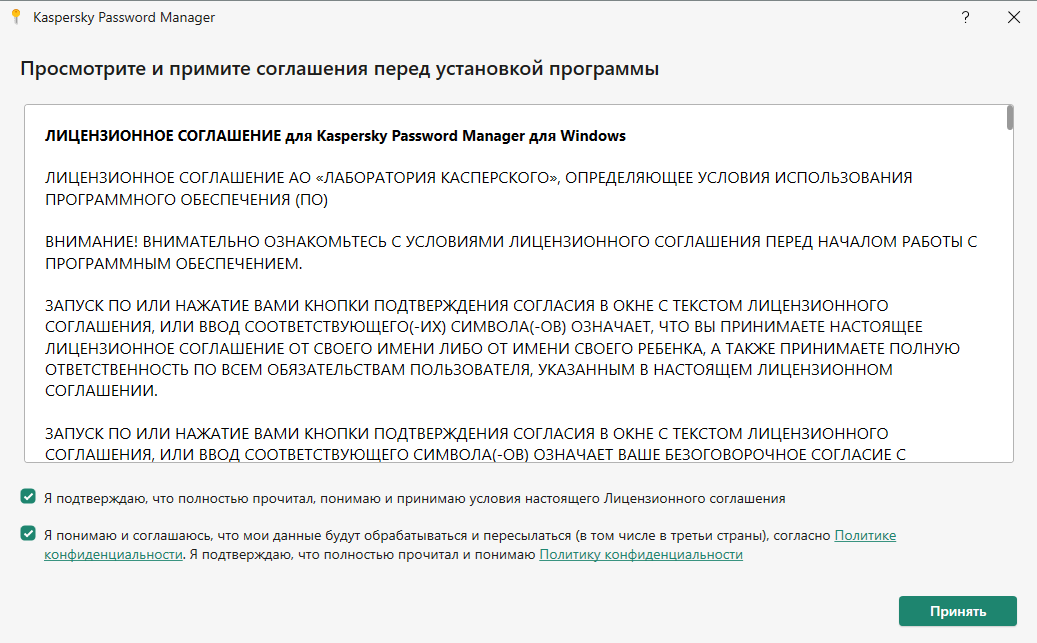


Рисунок 3.2.2 – Принятие лицензионного соглашения.

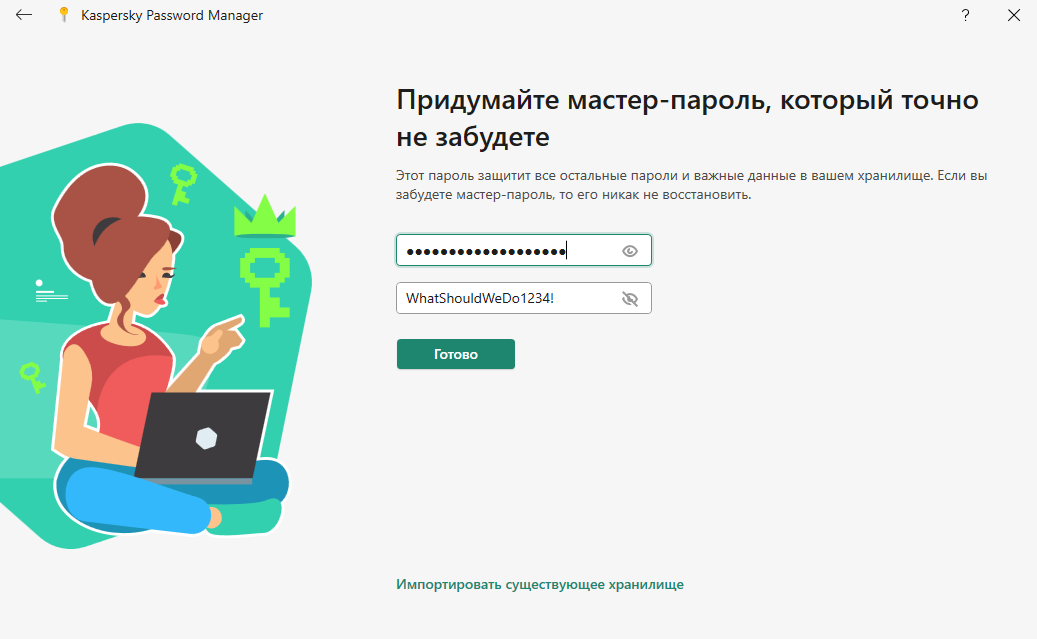


Рисунок 3.2.3 – Ввод главного пароля.

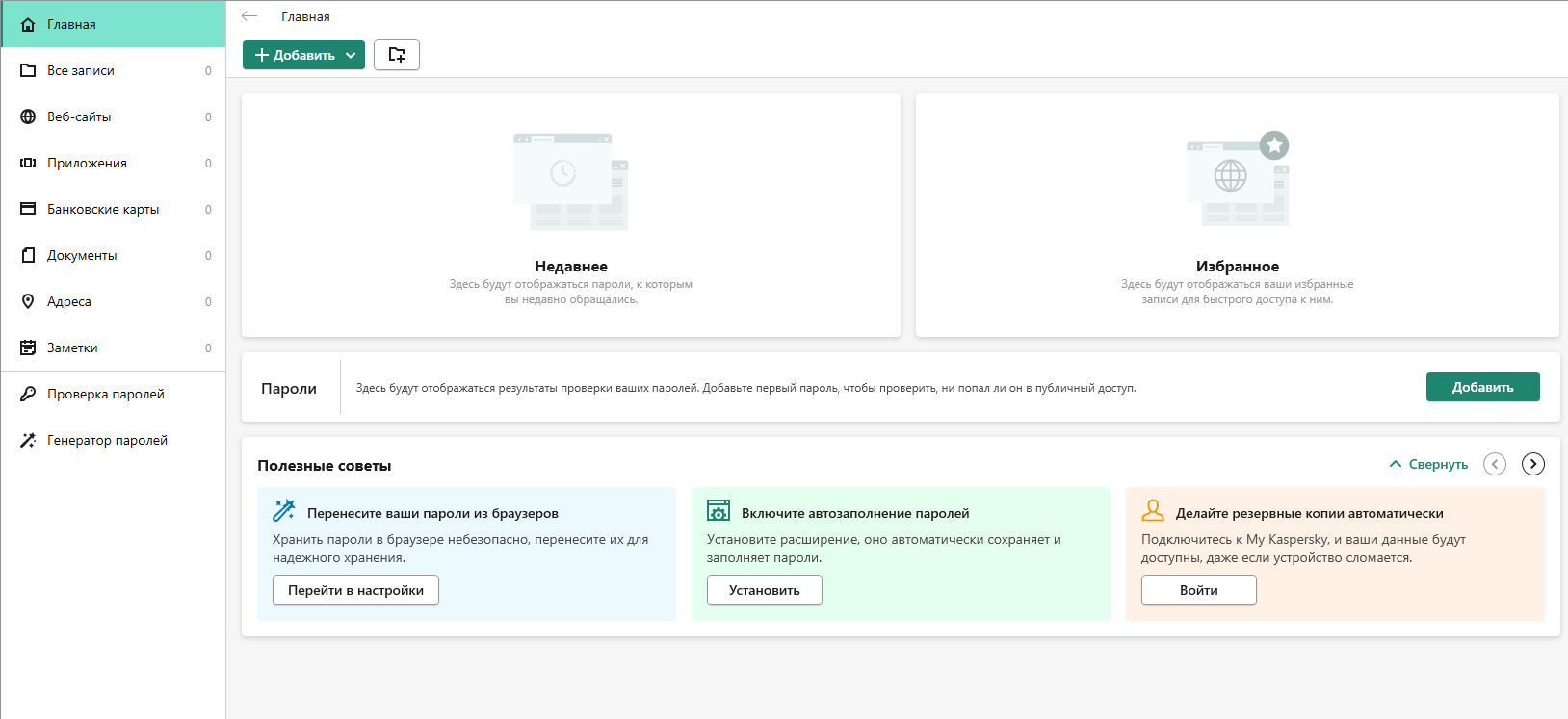


Рисунок 3.2.4 – Главное окно.

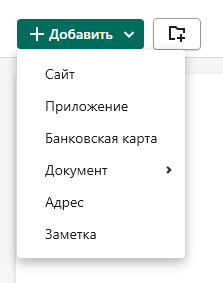


Рисунок 3.2.5 – Возможные виды сохранения форматов.

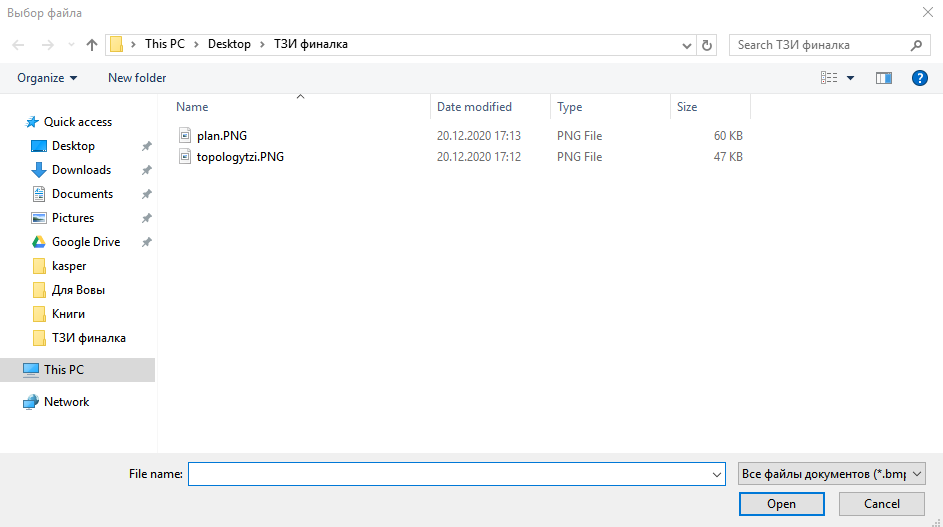


Рисунок 3.2.6 – Выбираем опцию «Документ» и выбираем документ, который мы хотим зашифровать. В нашем случае “plan.png”.

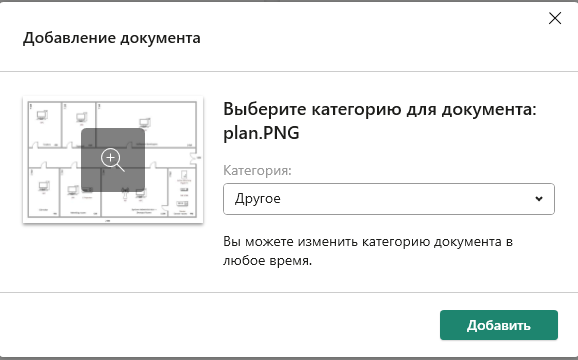


Рисунок 3.2.7 – Добавляем документ.

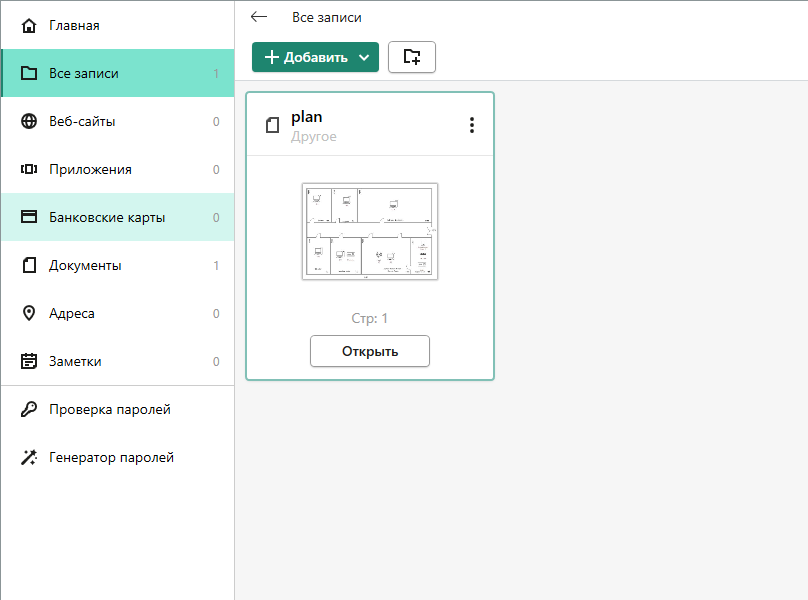


Рисунок 3.2.8 – Результаты добавления документа.

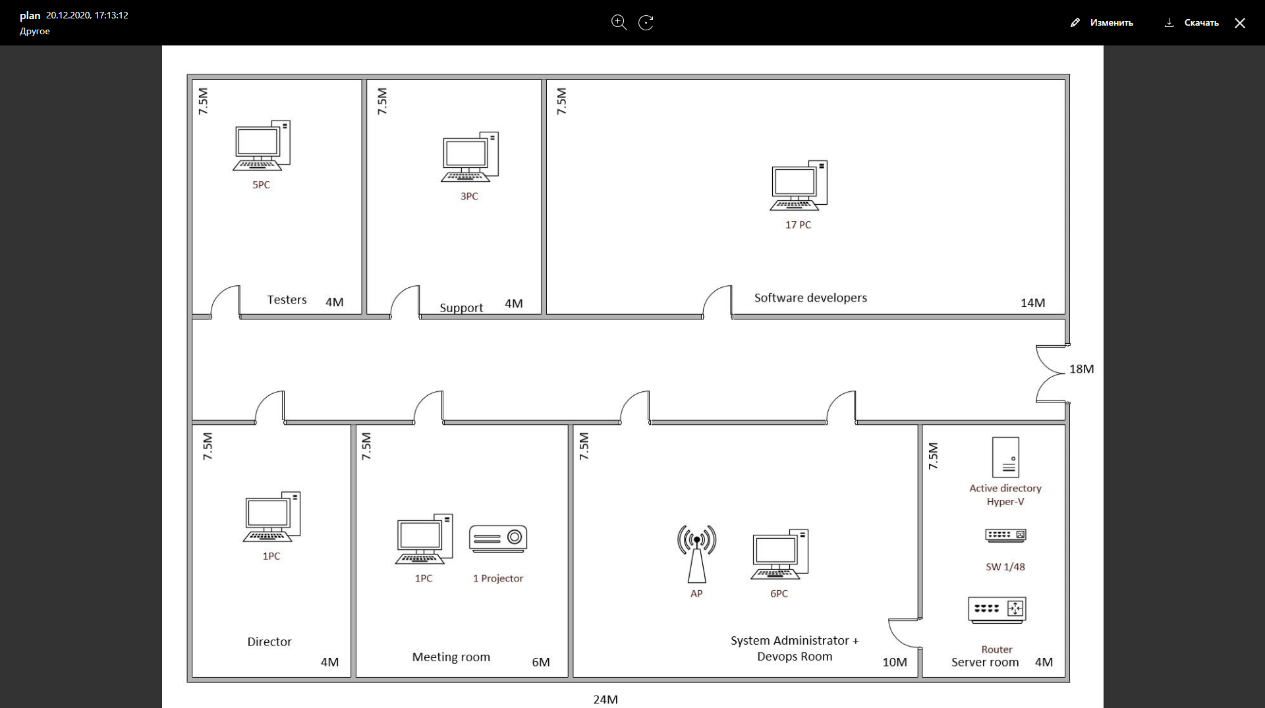


Рисунок 3.2.9 - Открываем документ в специальном окне.

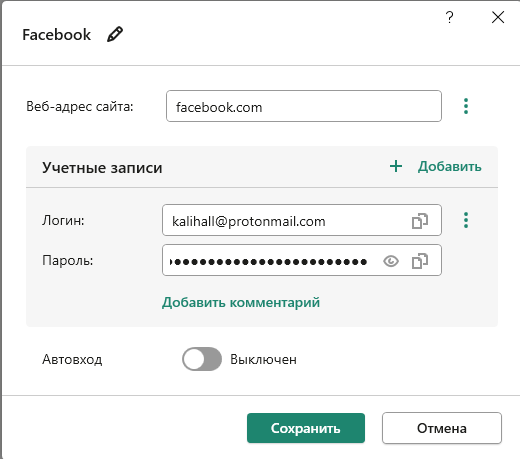


Рисунок 3.2.10 – Выбираем формат «Пароль от веб-страницы» и вводим данные.

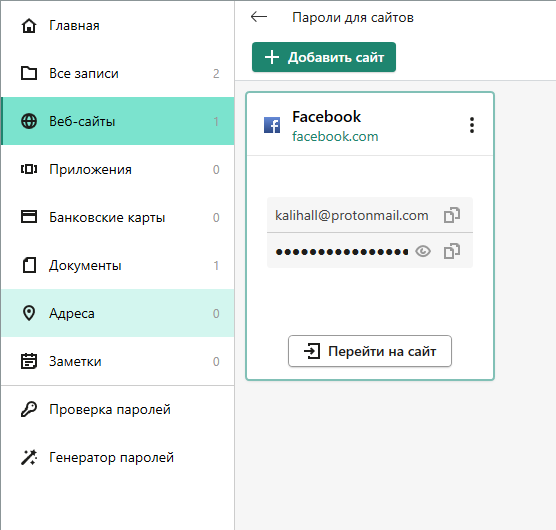


Рисунок 3.2.11 - Результаты сохранения.

* Защита веб-приложения.

Так как предприятие занимается разработкой программного обеспечения, у нее имеется свой веб-сайт, который работает на локальном сервере предприятия, находящемся в демилитаризованной зоне. Но даже так сервер подвластен возможности взлома, проблем с уязвимостями и прочим. В качестве выбора веб-сервера для сайта предприятия был выбран nginx, а точнее его защищенная docker-контейнер версия – “Bunkerized nginx” (<https://github.com/bunkerity/bunkerized-nginx/>).

Основная суть заключается в большом количестве сильных особенностей в плане безопасности, включающие в себя:

* Поддержка HTTPS с TLS-сертификат Let’s Encrypt!
* Встроенный firewall Modsecurity с набором правил от OWASP.
* HTTP-заголовки безопасности.
* Защита от бот-атак (проверка по капчам, cookies и customjs).
* Блокировка соединений по tor-proxy- и другим подозрительным соединениям и User-Agent-ам.
* Лимит на запросы.

Установка bunkerized-nginx в docker показана на рисунках 3.3.1 – 3.3.2.

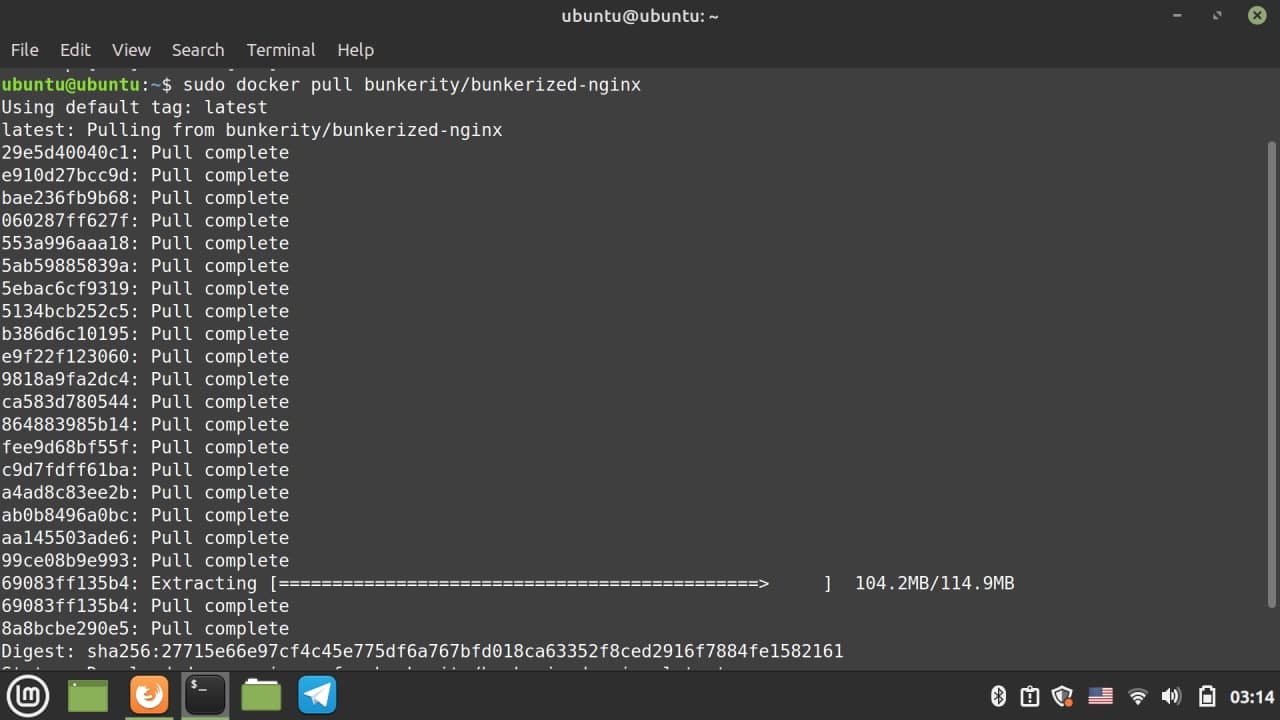


Рисунок 3.3.1 – Установка контейнера.

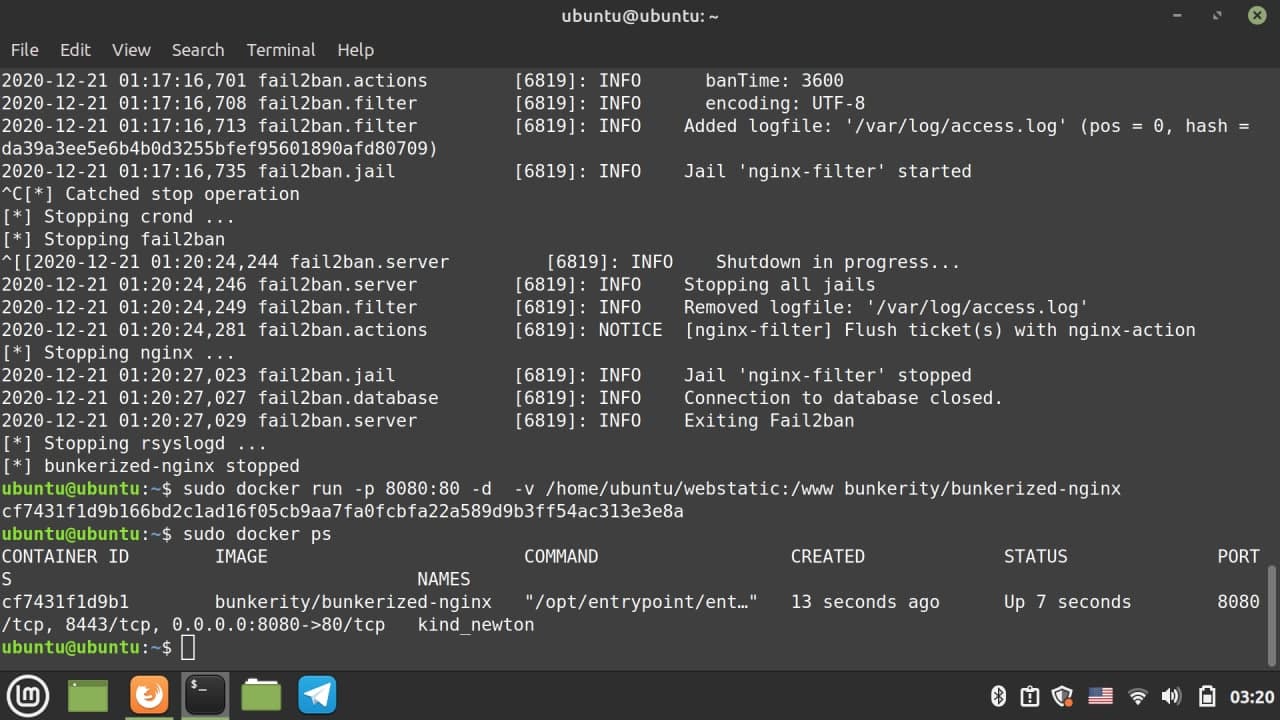


Рисунок 3.3.2 – Запуск контейнера с пробросом портов и указанием рабочей папки.

После этого веб сервер на устройстве, на котором запущен docker и данный контейнер, начинается функционирование веб-сервера.

* Авторизация в системе.

Каждый, кто попадает в локальную сеть и хочет получить доступ к серверу должен быть авторизирован и иметь надлежащие права. Так как предполагается, что все работники будут взаимодействовать с операционной системой Windows 10, лучшим решением для организации будет Windows Server + Active directory. Из-за отличной интеграции и других разных сервисов внутри системы Windows Server, есть возможность качественную систему безопасности.

* Безопасность при работе с сетью.

Для обеспечения устойчивой работы сети без риска вторжения со стороны, предприятие должно использовать соответствующие версии и виды протоколов. Зачастую предприятия могут пренебречь настолько важной темой, из-за чего позже могут произойти непредвиденные ситуации. Следующие протоколы довольно безопасно использовать при работе в сети:

* HTTPS – протокол безопасной передачи гипертекста, является надстройкой над HTTP, которая работает с помощью SSL/TLS.
* SSH2 – сетевой протокол, необходимый для установки удаленного соединения. Альтернативой является небезопасный telnet, который не шифрует передаваемую информацию.
* SFTP – безопасная версия протокола FTP для передачи файлов.
* SSL/TLS – не является протоколом передачей данных, но обеспечивает дополнительную безопасность сети. Они представляют из себя безопасные протоколы для работы с сетью, использующие ассиметричную криптографию для шифрования.
* RDP – протокол работы с удаленным рабочим столом. Использует шифр RSA RC4.
* L2TP + IPsec – набор протоколов для подключения к локальной сети с помощью VPN через глобальную сеть. На данный момент является одним из самых популярных методов обеспечения VPN.

ВЫВОДЫ

Был разработан инженерный проект: план, топология и смета предприятия по разработке программного обеспечения. Ко всему прочему были описаны методы обеспечения более продвинутой безопасности с использованием шифрования и других методов информационной безопасности.

ЛИТЕРАТУРА

1. <https://habr.com/ru/company/vdsina/blog/524466/>
2. <https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview>
3. <https://www.docker.com/>
4. https://www.kaspersky.com/password-manager