Teach Me Skills

Безопасность Windows

Mini-quize по прошлым темам:

1. **Что такое Mittre D3fend?**
2. **Как можно выстроить безопасность электронной почты в компании?**
3. **Что такое эскалация привилегий?**
4. **Какие существуют техники горизонтального перемещения?**
5. **Что такое хэш-функция?**
6. **В чем суть и назначение кеширования?**
7. **Что такое Vulnerability Management и как его выстроить?**

Mini-quize по новой теме:

1. **Что такое kerberos?**
2. **Зачем нужны сервисы в ОС Windows?**
3. **Что такое dll?**
4. **Что такое реестр?**
5. **Как можно настроить ОС Windows с точки зрения ИБ?**

Teach Me Skills

План занятия

1. Изучим как устроена ос Windows
2. Разберемся с реестром, библиотеками dll
3. Посмотрим какие сервисы существуют и как ими управлять
4. Изучим основные методики для обеспечения безопасности OS Windows
5. Посмотрим политики безопасности и групповые политики
6. Поработаем с реестром

Историческая справка

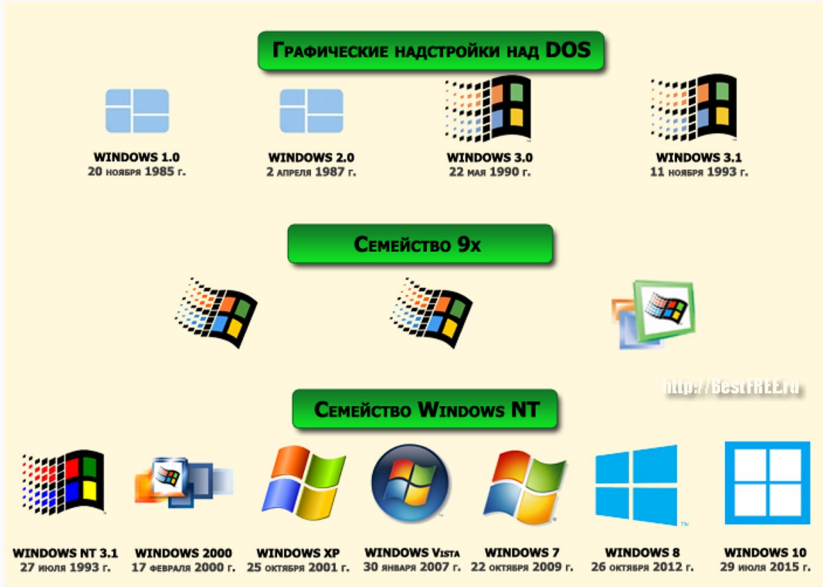
Teach Me Skills

MS-DOS

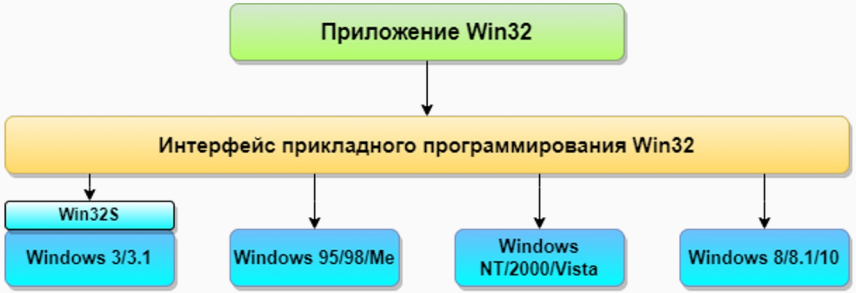
Однозадачная
X86
Cp/M, Unix
Монолитное ядро
Без GUI

Windows

Многозадачная
Arm, x86, MIPS, PowerPC
MS-DOS
Гибридое ядро
GUI



История развития ос Windows



DLL

Пример entrypoint dll

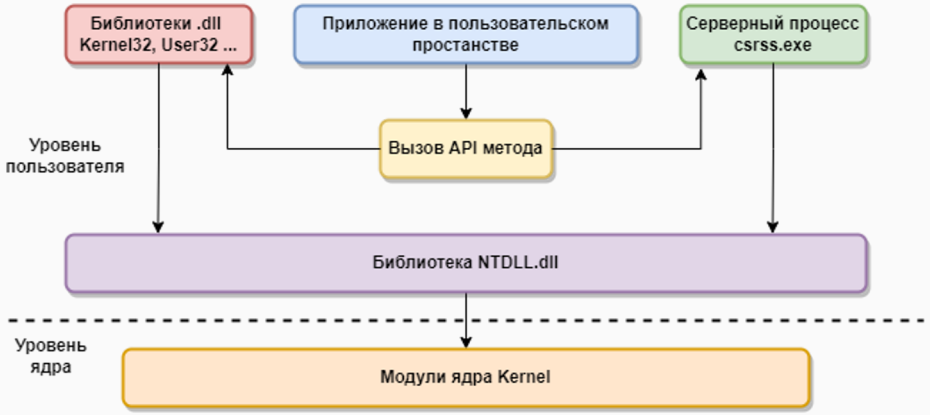
```
#include "pch.h"

BOOL APIENTRY DllMain( HMODULE hModule,
                       DWORD  ul_reason_for_call,
                       LPVOID lpReserved
                     )
{
    switch (ul_reason_for_call)
    {
        case DLL_PROCESS_ATTACH:
        case DLL_THREAD_ATTACH:
        case DLL_THREAD_DETACH:
        case DLL_PROCESS_DETACH:
        break;
    }
    return TRUE;
}
```

DLL (**библиотека динамической компоновки** или **динамически подключаемая библиотека**) - динамическая библиотека, позволяющая многократное использование различными программными приложениями.

Устройство ОС Windows

NT – New Technology

Вызов системных функций из пользовательского пространства

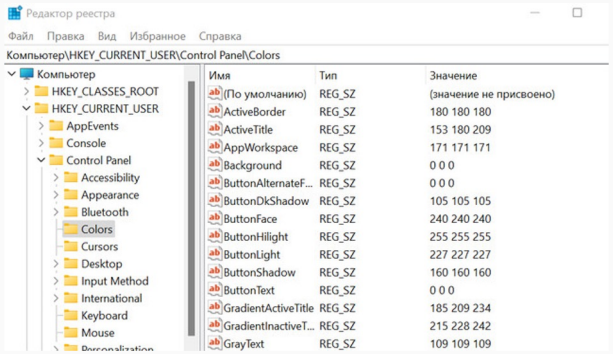


Компонент	Описание
Ядро операционной системы	Управляет аппаратными ресурсами компьютера и обеспечивает работу других компонентов
Подсистемы	Выполняют различные задачи и поддерживают работу с приложениями
Драйверы	Обеспечивают взаимодействие с аппаратными устройствами
Службы	Выполняют задачи в фоновом режиме
Графический интерфейс	Обеспечивает взаимодействие с пользователем
Файловая система	Управляет хранением и организацией файлов и папок
Процессы и потоки	Выполняют задачи и позволяют параллельно выполнять несколько задач
Сетевое взаимодействие	Поддерживает работу сетевых протоколов и предоставляет API для работы с сетевыми ресурсами

[Как работает операционная система Windows]

Реестр

Реестр Windows — иерархически построенная база данных параметров и настроек в большинстве операционных систем Microsoft Windows.



HKEY_CURRENT_CONFIG - сведения о профиле оборудования, используемом локальным компьютером при запуске системы
HKEY_DYN_DATA - Содержит динамически изменяемые данные о компьютере
HKEY_USERS - содержит информацию о профилях всех пользователей данного компьютера

HKEY_CURRENT_USER - настройки текущего активного пользователя
HKEY_LOCAL_MACHINE - параметры конфигурации, относящиеся к данному компьютеру
HKEY_CLASSES_ROOT - информацию о зарегистрированных типах файлов и объектах COM

Как открыть редактор реестра в Windows 10:

- В поле поиска на панели задач введите regedit, а затем выберите Редактор **реестра** (настольное приложение) в результатах.
- Щелкните правой кнопкой мыши кнопку Начните и выберите выполнить. Введите regedit в поле **Открыть**: и выберите ОК.

Microsoft Windows — **единственная** ОС из актуальных, в которой используется **механизм реестра**

Реестр#2

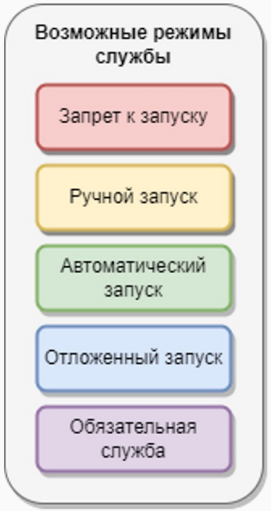
C:\Windows\System32\config

SYSTEM – информация о конфигурации ОС
DRIVERS – информация об обнаруженном оборудовании
BCD-Template – БД конфигурации загрузки
SAM – Информация об уч записях локальных пользователей
SECURITY – Информация службы lsass об уч записях
DEFAULT – Раздел по умолчанию для новых пользователей
SOFTWARE – Зарегистрированные в COM объекты
COMPONENTS – манифесты зависимостей для компонентов системы

Реестр Windows состоит из двух частей:
энергозависимая часть - пример: ключ «CurrentControlSet» куста «SYSTEM»
энергонезависимая часть синхронизируется с файлом реестра.

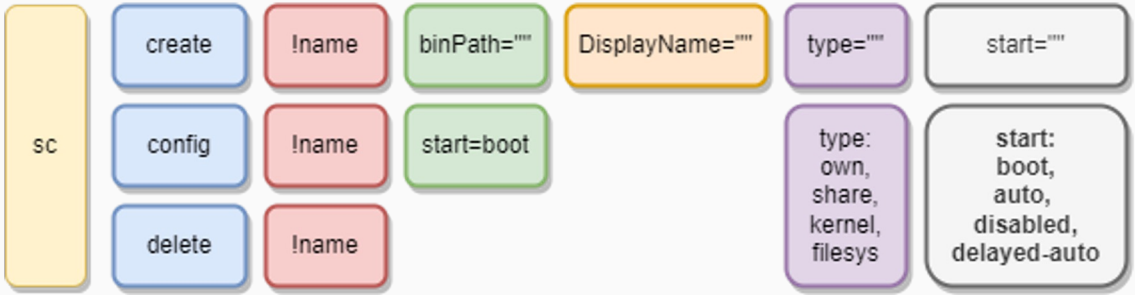
Сервисы/Службы

Служба Windows — приложение, автоматически или иным образом, запускаемое системой при запуске операционной системы, выполняющиеся вне зависимости от статуса пользователя. Подобно **демонам** в UNIX.



HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services

Создание своей службы windows:



Сервисы/Службы#2

Napagent - Агент защиты доступа к сети
Eventlog - Журнал событий
Winmgmt - Инструментарий управления Windows
Schedule - Планировщик заданий
W32Time - Служба времени Windows
CryptSvc - Службы криптографии
RpcSs - Удаленный вызов процедур
Dhcp - DHCP-клиент
Dnscache - DNS-клиент
TlntSvr - Telnet

LDAP+Kerberos

LDAP (Lightweight Directory Access Protocol) - открытый протокол, который используется для хранения и получения данных из каталога с иерархической структурой.

Kerberos - сетевой протокол аутентификации, с механизмом взаимной аутентификации клиента и сервера перед установлением связи между ними.

LDAP#2

Атрибуты - пара ключ-значение.
Запись – набор атрибутов.

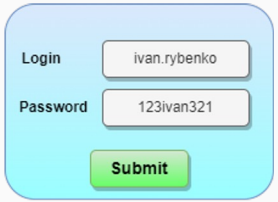
Синтаксис LDAP

Оператор	Символ	Описание
Равно	=	Создает фильтр по полю с указанным значением.
Любое значение	*	Соответствует полю с любым значением, кроме NULL.
Скобки	( )	Разделяет фильтры. Этот оператор необходим для работы логических функций.
И	&	Объединяет фильтры. Все условия должны иметь значение TRUE.
Или	|	Объединяет фильтры. Хотя бы одно условие должно иметь значение TRUE.
Не	!	Исключает все объекты, соответствующие фильтру.

Установка значения атрибута:
Login: ivanov
Сравнение значения атрибута:
User= ivan

Программа на Linux для работы с LDAP

LDAP-иньекции



Легетимный запрос:
(&(login=ivan.rubenko)(pswd=123ivan321))

(&(login=admin)(pswd=*))

(&(login=admin)(&))(pswd=test))

(&(login=admin)(|(!pswd=1)(pswd=1)))

Kerberos#2

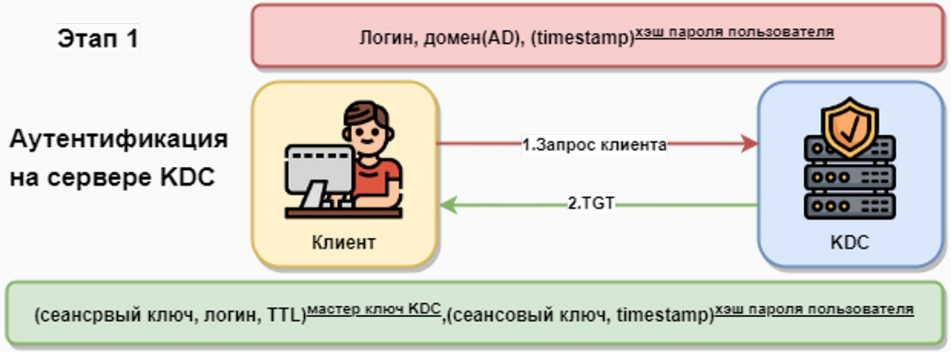
Ticket – зашифрованный пакет данных
KDC – третья доверенная сторона
TGT – удостоверение пользователя на доступ к ресурсам
TGS – удостоверение для доступа к ресурсам выданное на основе TGT
Timestamp – времнная метка

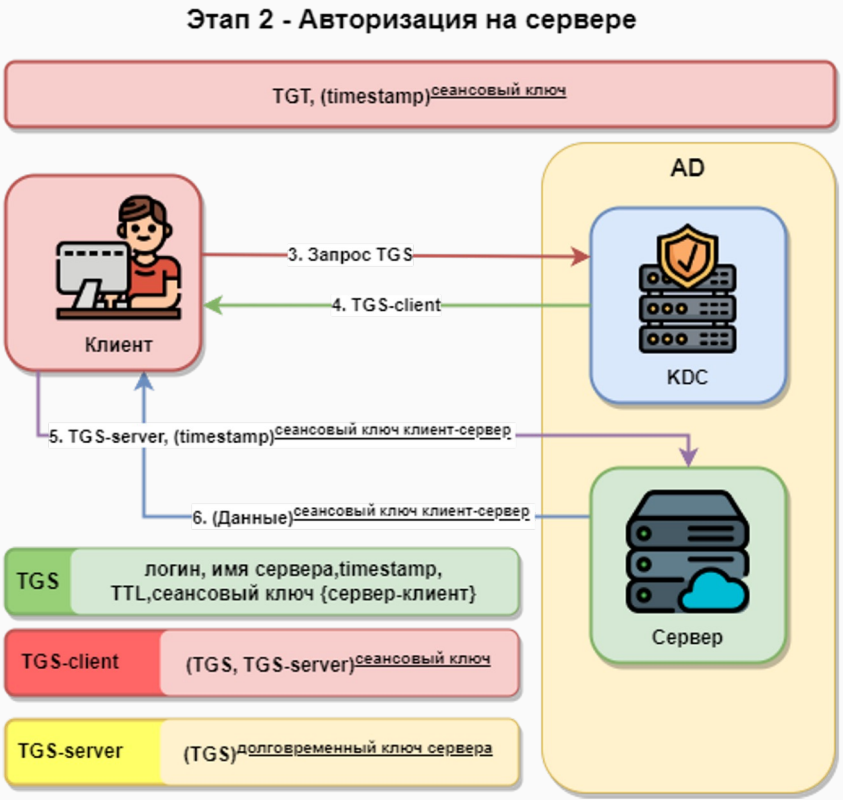
1- клиент 2- сервер 3- KDC

Требуется постоянное наличие центрального сервера.
Kerberos имеет строгие требования к времени.
Протокол администрирования не стандартизирован.
Каждый сервис, меняющий имя хоста, должен обновить набор ключей Kerberos.
Kerberos требует доверия от учетных записей пользователей, клиентов и пользователей услуг на сервере.
Kerberos не подходит, когда пользователи хотят подключаться к службам от неизвестных клиентов, как в обычном интернете.

Керберос работает опираясь на точное время!
В AD керберос – используется **по-умолчанию**.
KDC находится на AD сервере.

Kerberos#3





Этапы АА при помощи Kerberos-а:

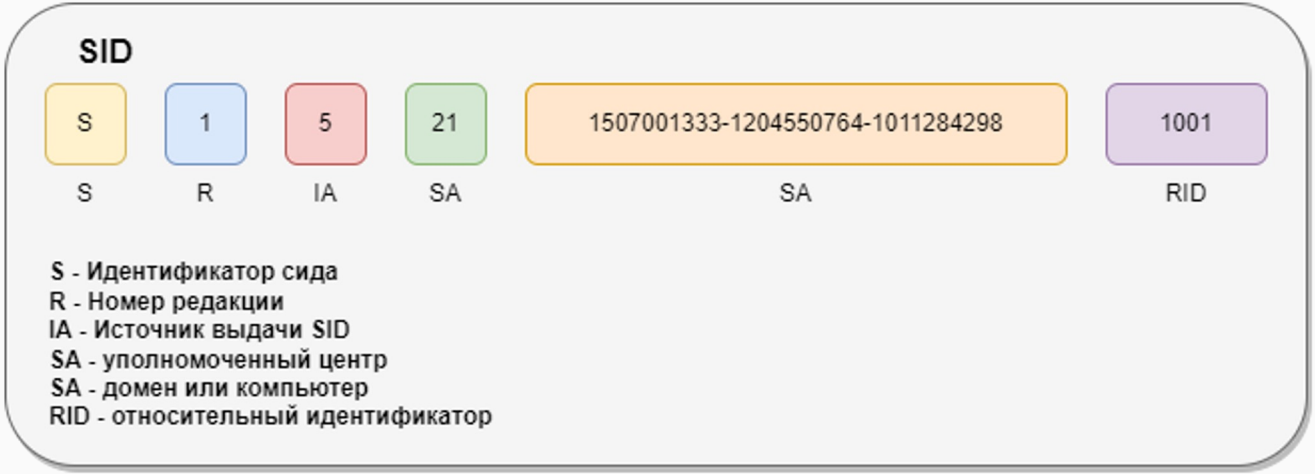
1) **Запрос TGT**
2) **Получение TGT**
3) **Запрос TGS**
4) **Получение TGS**
5) **Запрос к серверу с помощью TGS**
6) **Получение данных**

Аудит Windows

Аудит безопасности является одним из самых мощных средств, которые можно использовать для поддержания целостности системы.

За аудит безопасности отвечает **SACL** (system access control list) – список управления доступом к Microsoft windows используемый для аудита доступа.

DACL (discretionary access control list) — список избирательного управления доступом, контролируемый владельцем объекта и регламентирующий права пользователей и групп на действия с объектом.

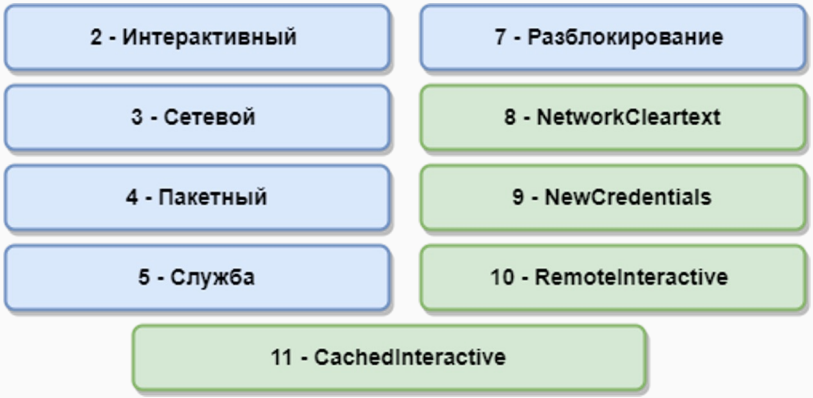


Аудит Windows#2

2 - пользователь вошел или попытался непосредственно введя имя пользователя и пароль в окне входа

3 - при подключении по сети к общим ресурсам

4 - при выполнении заданий без непосредственного участия пользователя



5 - когда Windows запускает службу от имени пользователя

7 - происходит когда пользователь разблокировывает или пытается, ранее заблокированный компьютер

8 - если пароль пользователя был получен по сети открытым текстом

9 -когда используется команда "Запустить от имени" вместе с опцией "/netonly"

10 -пользователь подключаетс к компьютеру с удаленного компьютера через RDP

11 - Когда пользователь входит в домен, Windows кэширует учетные данные пользователя локально, так что он позже может войти даже если контроллер домена будет недоступен.

Аудит Windows#3

LogonID – уникальной при входе
У ос – фиксированный **0x3E7**

TargetUserName	user
TargetDomainName	DESKTOP-T7GCMS8
TargetLogonId	0xb2fd46a
LogonType	2
LogonProcessName	User32

PID – process id, идентификатор процесса.

Имя	ИД процесса
svchost.exe	11292
svchost.exe	736
svchost.exe	5448
svchost.exe	8928
svchost.exe	12396
svchost.exe	10680
svchost.exe	4076
svchost.exe	7556

Инструкция по настройке ОС Windows

Настройка устройства. BIOS и TPM

1. Уникальный пароль на BIOS
    1. Зайти в BIOS устройства в зависимости от производителя (кнопка F2/Del/ESC при запуске).
    2. В большинстве случаев пароль на BIOS задается на вкладке Security.
    3. На каждом устройстве задать **уникальный** пароль.
       Пароль должен быть не менее 10 символов и содержать спец.символы и цифры.
2. Выставить режим загрузки UEFI
    1. Зайти в BIOS → вкладка Boot → пункт Boot Mode → выставить значение «UEFI».
3. Установлена опция «Secure Boot» и отключены все лишние варианты загрузки
    1. Зайти в BIOS → вкладка Security → пункт Secure Boot → выставить значение Enabled.
    2. На вкладке Boot - выставить для всех пунктов загрузки устройства на «Disable». кроме загрузки с жесткого диска (если такой пункт есть).
4. Обязательная активация чипа TPM (при наличии)
    1. Для проверки работы чипа зайти в ОС - запустить Выполнить - набрать «tpm.msc». Убедиться, что чип используется и проверить версию спецификации (желательная версия 2.0 и новее).
    2. Если чип выключен необходимо включить его через BIOS. Расположение может отличаться от версий BIOS, производителя устройства и чипсета. Чаще всего расположен в разделах «Security» или «Advanced».

Учетные записи и их настройка

1. Создать УЗ с административными правами
    1. При активации ОС создать УЗ с **уникальным** паролем.
    2. Записать в хранилище.

       Пароль должен быть не менее 10 символов и содержать спец.символы и цифры.
2. Создать УЗ без административных прав для сотрудника
    1. Для УЗ задать имя как указано в домене (пример: Ivan.Ivanov).
    2. При создании оставить включенной опцию «Требовать смены пароля при следующем входе в систему».
3. Отключить УЗ «Гость»
    1. ПКМ по кнопке Пуск → Управление компьютером → Локальные пользователи → Пользователи → Убедиться, что УЗ Гость не активна.
    2. Пуск → В поиске найти Локальная политика безопасности → Локальные политики → Параметры безопасности → Учетные записи: Состояние учетной записи «Гость» → Отключен.
4. Включить «контроль учетных записей» (UAC)
    1. Пуск → Панель управления → Учетные записи пользователей → Изменить параметры контроля учетных записей → Выставить значение «Уведомлять только при попытках приложений внести изменения в компьютер (по умолчанию)».

Учетные записи и их настройка

5. Настроить парольную политику

Пуск → В поиске найти Локальная политика безопасности → Политики учетных записей → Выставить следующие значения:

- Вести журнал паролей - 5 последних паролей
- Максимальный срок действия паролей - 90 дней
- Минимальная длина пароля - 8 символов
- Пароль должен отвечать требованиям сложности - Включен
- Пороговое значение блокировки - 5 ошибок
- Продолжительность блокировки УЗ - 15 мин
- Разрешить блокировку УЗ администратора - Включен.

6. Настройка парольной политики PIN (для Windows Hello)

Открыть CMD → Набрать команду gpedit.msc → Конфигурация компьютера → Административные шаблоны → Система → Сложность PIN-кода → Выставить следующие значения:

- Требовать использование цифр - Включена
- Требовать использование строчных букв - Включена
- Минимальная длина PIN-кода - 8 символов
- Срок действия - 90 дней
- Журнал - 5 последних паролей
- Требовать использование специальных символов - Включена
- Требовать использование прописных букв - Включена

Включение RDP для УЗ администратора

1. Windows 10
    1. Пуск → Параметры → Система→ Удаленный рабочий стол → Включить.
    2. Внизу раздела нажать на «Выберите пользователей, которые могут получить удаленный доступ к этому компьютеру» → Добавить УЗ администратора.
    3. Зайти в «Дополнительные параметры» → Поставить галку «Требовать использование устройствами аутентификации на уровне сети для подключения».
2. Windows 11
    1. Пуск → Параметры → Система→ Удаленный рабочий стол → Включить.
    2. Поставить галку «Требовать использование устройствами аутентификации на уровне сети для подключения».
    3. В разделе «Пользователи удаленного рабочего стола» добавить УЗ администратора.

Настройка блокировки рабочего стола

1. Пуск → В поиске найти Локальная политика безопасности → Локальные политики → Параметры безопасности.
2. Интерактивный вход в систему: предел простоя компьютера - Выставить значение 300 секунд.

Установка антивируса

1. Дистрибутив и инструкцию вы должны составить для своих сотрудников

Настройка установки обновлений

1. Windows 10
    1. Пуск → Параметры → Обновление и безопасность → Центр обновления Windows → Установить все доступные обновления.
    2. Зайти в раздел «Изменить период активности» → Снять галку по автоматическому изменению периода.
    3. Выставить «Текущий период активности» - 10-18 часов.
    4. Перейти в раздел Центр обновления Windows → Дополнительные параметры → Раздел Уведомления об обновлениях → Включить «Показать уведомление, когда компьютеру требуется перезагрузка для завершения обновления».
2. Windows 11
    1. Пуск → Параметры → Центр обновления Windows → Установить все имеющиеся обновления.
    2. Перейти в раздел «Дополнительные параметры» → Выставить период активности «Вручную».
    3. Текущий период поставить 10-18 часов.
    4. Так же в этом разделе включить «Уведомлять меня о необходимости перезагрузки для завершения обновления».

Шифрование жесткого диска устройства (BitLocker)

1. Подключить флэшку или другой съемный носитель к устройству.
2. Пуск → Панель управления → Шифрование диска BitLocker.
3. Нажать «Включить Bitlocker». Откроется «мастер настройки**»**.
4. Первым шагом будет запрос на архивацию ключей восстановления. Выбрать «Сохранить в файл».
5. Ключ восстановления необходимо сохранить на съемное устройство. В дальнейшем ключ необходимо скопировать в хранилище.
6. На следующем шаге выбрать «Шифровать весь диск**»**.
7. Далее выбрать «Новый режим шифрования**»** (перед этим необходимо убедиться, что на устройстве установлены все актуальные обновления и версия Windows новее 1511).
8. Поставить галку на «Запустить проверку системы BitLocker**»** и согласиться с перезагрузкой.
9. После перезагрузки зайти в BitLocker и проверить, что шифрование завершено.

Если на устройстве **нет TPM модуля** BitLocker не позволит запустить шифрование диска без указывания пароля.

Так же для включения возможности шифрования необходимо:

- Зайти в групповые политики устройства (gpedit.msc) → Конфигурация компьютера → Административные шаблоны → Компоненты Windows → Шифрование диска BitLocker → Диски операционной системы.
- Включить параметр «Этот параметр политики позволяет настроить требование дополнительной проверки подлинности при запуске» (только включить. Другие параметры изменять не надо)

Включить брандмауэр и настроить логирование

1. Пуск → Панель управления → Брандмауэр Защитника Windows → «Включение и отключение брандмауэра». Проверить, что он запущен.
2. Пуск → Панель управления → Брандмауэр Защитника Windows → Дополнительные параметры → ПКМ по «Монитор брандмауэра Защитника Windows**»** → Свойства.
3. На всех трех вкладках профилей (Общий, Частный, Домена) включить запись пропущенных пакетов и успешных подключений (Раздел «Ведение журнала**»**). Размер файла лога для всех - 10240 КБ.