**Практическое занятие № 27**

**Мониторинг активности портов**

**Цель занятия:** формирование умений и навыков блокировки и разблокировки портов подключения устройств.

**Краткие теоретические сведения**

Понятие порта в компьютере многозначно. Самое общее определение: порт – это соединение (физическое или логическое), через которое принимаются и отправляются данные. Обмен данными между любыми устройствами возможен только при наличии утвержденного стандарта на интерфейс.

В состав аппаратного обеспечения порта входит специализированный разъём, предназначенный для подключения оборудования определённого типа. Часто этот специализированный разъем и называют портом, например, USB-порт, но есть разъемы, которые портами называть не принято, например, RJ11. Как правило, каждый порт имеет обозначение, которое размещается рядом с разъемом.

Основные порты, используемые в компьютерах, ноутбуках:

– USB-порт;

– IEEE 1394 (FireWire);

– порт eSATA и комбинированный порт USB/eSATA;

– сетевой порт Ethernet;

– порт SCSI;

– последовательный порт RS-232;

– порты для подключения внешних мониторов VGA, DVI, S-Video, HDMI, DisplayPort;

– порт для док-станции и порт репликатор;

– порты для модулей расширения PCMCIA, ExpressCard.

USB – Universal Serial Bus – универсальная последовательная шина. USB-порты являются своего рода стандартом для подключения внешних устройств, к которому стремятся все производители этих устройств. К портам USB подключаются: мыши, клавиатуры, принтеры, сканеры, модемы, кардридеры, флэш накопители, фотоаппараты, сотовые телефоны, плееры, жёсткие диски, оптические дисководы и др.

IEEE 1394 – высокоскоростной последовательный порт для цифровых видеоустройств. Компания Apple продвигает стандарт IEEE 1394 под маркой FireWire, компания Sony – под маркой i.LINK. IEEE 1394 применяется для подключения видеокамер, цифровых фотоаппаратов и других мультимедийных устройств, а также принтеров, сканеров, внешних жестких дисков.

Основные преимущества по сравнению с USB 2.0 – более высокая скорость передачи, большая стабильность, большая длина кабеля до оконечного устройства.

eSATA – External Serial ATA (Advanced Technology Attachment – присоединение по передовой технологии) – последовательный интерфейс для подключения внешних устройств, поддерживающий режим «горячей замены». Стандарт eSATA предусматривает подключение внешних жестких дисков, оптических дисков, RAID-массивов. Скорость передачи данных гораздо выше, чем у USB 2.0 или IEEE 1394.

Недостатки eSATA:

– максимальная длина кабеля не превышает 2 метров;

– жёсткие диски, подключаемые через eSATA, потребуют дополнительного источника питания – это могут быть как разъёмы USB или 1394, так и розетка.

Порт Ethernet предназначен для подключения ноутбука к компьютерной сети с помощью сетевого кабеля через разъем RJ45 (RJ-45). Технология Ethernet описывается стандартами IEEE группы 802.3. Существует несколько стандартов технологии Ethernet.

Стандарты различаются скоростью передачи данных и передающей средой. В ноутбуках обычно устанавливают порт Ethernet 10/100/1000, который поддерживает стандарты 10BASE- T, 100BASE-TX и 1000BASE-T для расстояний до 100 м. Стандарт 10BASE-T позволяет передавать данные со скоростью 10 Мбит/с. Для передачи используется 4 провода кабеля витой пары категории 3 или категории 5. По стандарту 100BASE-TX скорость передачи данных составляет 100 Мбит/c. Стандарт применяется для построения сетей топологии «звезда». Задействована витая пара категории 5, поддерживается дуплексная передача данных. Стандарт 1000BASE-T – гигабитный (Gigabit, Geth) Ethernet позволяет передавать данные со скоростью до 1 Гбит/с. Стандарт предусматривает использование витой пары категорий 5e.

RS-232 (англ. Recommended Standard) – стандарт последовательной асинхронной передачи двоичных данных между двумя устройствами на расстоянии до 15 метров. Порт RS-232 в последнее время не часто встречается в бизнес-ноутбуках, но может быть полезен в промышленных ноутбуках. Он используется для реализации систем сбора данных в реальном времени, подключения научного ряда контактов. Карты Type III поддерживают 16- или 32-разрядный интерфейс. Они имеют толщину 10,5 мм, что позволяет устанавливать на карту стандартные разъёмы внешних интерфейсов и избавиться, таким образом, от дополнительных кабелей.

Разъем имеет четыре ряда контактов. Разъем PCMCIA представляет собой щель шириной 54 мм, которая закрыта либо откидной шторкой, либо пластиковой заглушкой. Разъем (слот) PCMCIA (вверху) и заглушка, внизу – кардридер.

Большинство ноутбуков оснащается лишь одним разъемом PCMCIA типа II. А современные ноутбуки уже обходятся и вовсе без этих разъемов.

Порт ExpressCard. Стандарт ExpressCard для карт расширения был разработан ассоциацией PCMCIA на смену стандарту PC Card. Новый стандарт был создан на базе новой скоростной последовательной шины PCI Express. Стандарт ExpressCard не только более производительный, чем PC Card, но и более универсальный. Через ExpressCard можно подключаться к шине USB. Карты ExpressCard бывают двух типов, отличающихся по ширине: 34 мм и 54 мм. Соответственно и разъемы бывают двух типов ExpressCard/34 и ExpressCard/54. При этом карты 34 мм можно устанавливать как в разъем ExpressCard/34, так и в разъем ExpressCard/54. Через разъемы ExpressCard подключают ТВ- тюнеры, звуковые карты, карты Wi-Fi, флеш-накопители (они часто подключаются через USB- составляющую интерфейса ExpressCard), модемы для работы в сотовых сетях и др.

Разъем RJ11(RJ-11 Registered jack) – разъем модема ноутбука. Используется для подключения к Интернету через модем по телефонной линии.

Одной из важных особенностей современных корпоративных сетей является их размер, который зачастую исчисляется тысячами, а и иногда и десятками тысяч компьютеров. При этом деятельность пользователей может быть распределена среди различных компьютеров, а одна и та же проблема часто решается группами пользователей.

Важной задачей является контроль работы, как отдельных пользователей, так и групп пользователей.

Основными целями контроля являются: обеспечение информационной безопасности, выявление случаев некорректного, непрофессионального или нецелевого использования ресурсов, оценка характеристик функционирования корпоративной сети и параметров использования ресурсов.

Основной задачей обеспечения информационной безопасности является «раннее обнаружение» внутренних вторжений, т.е. выявление действий пользователей, которые могут предшествовать внутренним вторжениям. Чем крупнее организация, тем актуальней является для нее проблема предотвращения внутренних вторжений, в частности кражи информации, так как именно кража является конечной целью большинства внутренних вторжений. Связано это с тем, что в больших организациях затрудняется контроль над обращением информации и существенно возрастает цена ее утечки. Указанные обстоятельства определяют высокий уровень озабоченности данной проблемой со стороны крупного бизнеса и правительственных организаций. Решение данной проблемы заключается в применении «жесткой» политики информационной безопасности в организации и использовании средств мониторинга действий пользователей.

**Spector 360** включает в себя средства для автоматического развертывания и удаленного управления, осуществляет запись разнообразных действий, включая: Email, чаты, мгновенные сообщения, посещаемые веб-сайты, онлайновые поисковые запросы, нажимаемые клавиши и используемые программы. Spector 360 также включает в себя средство для записи образов экрана в режиме видеокамеры.

Все эти инструменты ведут запись одновременно, скрытно, под защитой тройного уровня безопасности. Приложение Recorder хорошо конфигурируется и может быть настроено для записи только интересующих событий.

В дополнение к мониторингу и ведению записи Spector 360 обладает развитой системой определения и обнаружения ключевых слов, которая будет немедленно извещать о каждом случае, когда пользователь контролируемого ПК отклонится от допустимого использования ПК или Интернет.

Регистратор Spector 360 можно перевести в скрытый режим, который обеспечивает невозможность обнаружения программы неуполномоченными пользователями. В скрытом режиме Spector 360 не будет виден пользователю в системном меню задач, диспетчере задач или в меню установки/удаления программ панели управления.

При помощи Spector 360 можно сгенерировать высококачественные отчеты для руководства, которые могут регулярно распечатываться или рассылаться по почте.

Spector 360 разработан для коммерческих, образовательных и правительственных организаций, использующих сети на платформе Windows.

**Security Curator** – это система обеспечения информационной безопасности нового поколения, объединяющая в себе возможность наблюдения за деятельностью сотрудников, контроля их действий и блокировки потенциально опасных путей утечки информации.

Security Curator ведёт мониторинг в реальном времени практически всех действий сотрудников при работе за компьютером. Информация о действиях пользователей обновляется в реальном режиме времени. При этом постоянно производится сохранение снимков экрана при совершении любых действий, также существует возможность наблюдения за рабочим столом пользователя в режиме онлайн. В случае работы пользователем с USB- устройствами производится резервное копирование файлов.

Внедрение Security Curator позволяет ограничить доступ к нежелательным сайтам, программам и приложениям на определенный промежуток времени либо постоянно.

Например, работодатель может разрешить сотрудникам посещать сайты ВКонтакте и Одноклассники только во время обеденного перерыва, а доступ к бухгалтерской программе 1С запретить после окончания рабочего дня и на выходных.

**Activity Monitor** мощный инструмент, который позволяет отслеживать любые действия в сети и предоставляет детальную информацию о том, что, как и когда делали сотрудники организации. Будь то сеть библиотеки, университета или коммерческой организации, Activity Monitor поможет установить эффективный контроль над ней.

Приложение состоит из серверной и клиентской частей. Сервер Activity Monitor может быть установлен на любом компьютере в сети. Модуль-шпион (агент) устанавливается на всех компьютерах, действия на которых необходимо отслеживать. Он может быть установлен даже удалённо с системы, на которой установлена серверная часть Activity Monitor.

Действия на сетевых компьютерах отслеживаются удалённо. Можно настроить программу таким образом, что она будет отслеживать и регистрировать действия на всех компьютерах в сети одновременно. Данные мониторинга могут быть использованы для более глубокого анализа и создания детальных отчётов.

Activity Monitor является эффективным средством повышения общей производительности труда в компаниях, использующих данную программу для мониторинга локальных сетей.

**Net Vizor** – программа для мониторинга сети. Net Vizor позволяет наблюдать за всей локальной сетью из одного рабочего места. Программа может следить за рабочими станциями и индивидуальными пользователями, которые используют различные компьютеры, находящиеся в сети.

Программа позволяет следить за сетевыми компьютерами, осуществлять фильтрацию контента и управлять сетевыми компьютерами дистанционно.

Существует возможность ведения журналов адресов посещенных сайтов, соединений с интернетом, открываемых файлов, чатов, пересылаемых сообщений электронной почты и так далее. Net Vizor также обезвреживает шпионские программы и помогает следить за безопасностью.

Таблица 1 - Сравнительный анализ программ

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Мониторинг** | | **Spector 360** | | **Security Curator** | | **Activity Monitor** | | **Net Visor** | |
| Экран | | Да | | Да | | Да | | Да | |
| Снимки экрана | | Да | | Да | | Да | | Да | |
| Запущенные процессы | | Да | | Да | | Да | | Да | |
| Время запуска и выключения программ | | Да | | Да | | Да | | Да | |
| Бесплатные сервисы электронной почты | | Нет | | Да | | Да | | Нет | |
| Нажатие клавиш | | Да | | Да | | Да | | Да | |
| E-mail | | Да | | Да | | Да | | Да | |
| Посещенные сайты | | Да | | Да | | Да | | Да | |
| Переписка в IM агентах | | Да | | Да | | Да | | Да | |
| Социальные сети | | Да | | Да | | Да | | Да | |
| Поисковые запросы | | Да | | Да | | Да | | Да | |
| USB устройства | | Да | | Да | | Да | | Да | |
| Обнаружение ключевых слов | | Да | | Да | | Да | | Да | |
| Установка, удаление программ | | Да | | Да | | Да | | Да | |
| Контроль рабочего времени | | Да | | Да | | Да | | Да | |
| Загружаемые файлы | | Да | | Да | | Да | | Да | |
| Доступ к файлам, папкам | | Да | | Да | | Да | | Да | |
| Активность пользователя | | Да | | Да | | Да | | Да | |
| FTP | | Да | | Да | | Да | | Да | |
| Сетевые соединения | | Да | | Да | | Да | | Да | |
| Выборочный мониторинг | | Да | | Да | | Да | | Да | |
| Запись по расписанию | | Да | | Да | | Да | | Да | |
| Блокировка событий (запуск приложений, сайты,запрет файловых операций) | | Да | | Да | | Да | | Да | |
| Блокировка запуска любых процессов | | Да | | Да | | Да | | Да | |
| Блокировка подключения/отключения  всех типовUSB накопителей и устройств | | Да | | Да | | Да | | Да | |
| Блокировка сетевых соединений (по порту, ipадресу) | | Да | | Да | | Да | | Да | |
| Блокировка сайтов по домену | | Да | | Да | | Да | | Да | |
| Блокировка чатов и Интернет пейджеров | | Да | | Да | | Да | | Да | |
| Блокировка доступа в Интернет по протоколу илипорту | | Да | | Да | | Да | | Да | |
| Запрет действий с файлами/папками | | Да | | Да | | Да | | Да | |

Продолжение таблицы 1

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Отчетность** | **Spector 360** | **Security Curator** | **Activity Monitor** | **Net Viso r** |
| Генерация отчетов с привязкой к отдельномупользователю | Да | Да | Да | Да |
| Поиск, по ключевым словам, | Да | Да | Да | Да |
| Генерация графических отчетов | Да | Да | Да | Да |
| Конвертация отчетов в PDF | Да | Да | Да | Да |
| Конвертация отчетов в HTML | Да | Да | Да | Да |
| Конвертация отчетов в CSV | Да | Да | Да | Да |
| Конвертация отчетов в Excel | Да | Да | Да | Да |
| Конвертация отчетов в Rich Text | Нет | Да | Да | Нет |
| Экспорт отчетов | Да | Да | Да | Да |
| Отправка отчетов по электронной почте | Да | Да | Да | Да |
| Отправка отчетов по FTP | Да | Да | Да | Да |
| Печать отчетов | Да | Да | Да | Да |
| Генерация отчетов по расписанию | Да | Да | Да | Да |

Продолжение таблицы 1

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Управление** | **Spector 360** | **Security Curator** | **Activity Monitor** | **Net Visor** |
| Централизованное управление клиентами | Да | Да | Да | Да |
| Централизованное управление лицензиями | Да | Да | Да | Да |
| Централизованное конфигурирование безопасности | Да | Да | Да | Да |
| Централизованное конфигурирование сети | Да | Да | Да | Да |
| Централизованное конфигурирование WEB-фильтра | Да | Да | Да | Да |
| Резервирование и восстановление базы данных | Да | Да | Да | Да |
| Управление резервными копиями | Да | Да | Да | Да |
| Многопользовательский дискреционный контроль доступа к данным | Да | Да | Да | Да |
| Разделение доступа к функциям администрирования | Да | Да | Да | Да |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Возможность группировки компьютеров | Да | Да | Да | Да |
| Возможность группировки пользователей | Да | Да | Да | Да |

Продолжение таблицы 1

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Безопасность** | **Spector 360** | **Security Curator** | **Activity Monitor** | **Net Visor** |
| Контроль компьютеров в сети | Да | Да | Да | Да |
| Удаленная установка | Да | Да | Да | Да |
| Невидимый режим работы | Да | Да | Да | Да |
| Авторизация при запуске административного модуля | Да | Да | Да | Да |

Продолжение таблицы 1

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Стоимость** | **Spector 360** | **Security Curator** | **Activity Monitor** | **Net Visor** |
| Цена за 1 лицензию (от 5 до 99 хостов) | $128,00 | - | 3 419$ | 0,55 € |
| Цена за 1 лицензию (от 100 до 249 хостов) | $112,0 | - | Нет | 0,45 € |
| Цена за 1 лицензию (от 250 до 1000 хостов) | $96,00 | - | Нет | 0,40 € |

Spector 360 незаменим в крупных организациях, где решаются задачи оперативного мониторинга огромного количества рабочих станции.

Если делать акцент на возможность контроля и блокировки действий пользователей, тут подойдет Security Curator, Net Visor и Activity Monitor.

Рассмотрим два способа улучшения безопасности работы сети.

Шаг 1. Меняем учетную запись администратора (Пользователь Администратор с пустым паролем – это уязвимость) (убираем уязвимость 1).

При установке Windows в автоматическом режиме с настройками по умолчанию, мы имеем пользователя Администратор с пустым паролем и любой User может войти в такой ПК с правами администратора. Чтобы решить проблему, выполним команду Мой компьютер – Панель управления- Администрирование – Управление компьютером – Локальные пользователи – Пользователи.

Здесь по щелчку правой кнопкой мыши на Администраторы зададим администратору пароль, например, 12345. Теперь в окне Администрирование зайдем в Локальную политику безопасности. Далее идем по веткам дерева: Локальные политики – Параметры безопасности – Учетные записи – Переименование учетной записи – Администратор.

Пользователя Администратор заменим на Admin.

Перезагружаем ОС. После наших действий получилась учетная запись Admin с паролем 12345 и правами администратора.

Теперь мы имеем пользователя Администратор с паролем, одна из уязвимостей системы устранена.

Операцию по изменению имени пользователя и заданию пароля мы также могли бы выполнить без использования системного реестра, использовав окно Учетные записи пользователей.

Учетная запись Гость позволяет входить в ПК и работать на нем (например, в Интернет) без использования специально созданной учетной записи. Запись Гость не требует ввода пароля и по умолчанию блокирована. Гость не может устанавливать или удалять программы. Эту учетную запись можно отключить, но нельзя удалить.

**Шаг 1. Меняем учетную запись администратора**

Уязвимость: Учетная запись "Администратор" с пустым паролем, которая позволяет любому пользователю получить административные права.

1. Задание пароля учетной записи "Администратор":
   * Перейдите в Панель управления.

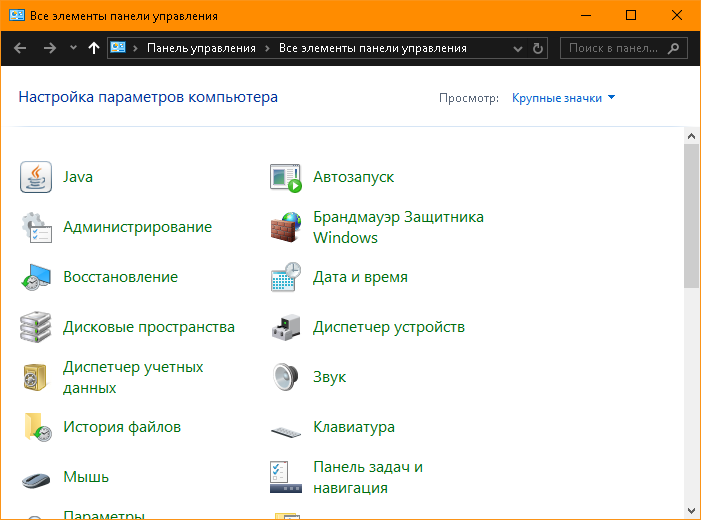


Рисунок 1 – Панель управления

* + Выберите Администрирование → Управление компьютером.

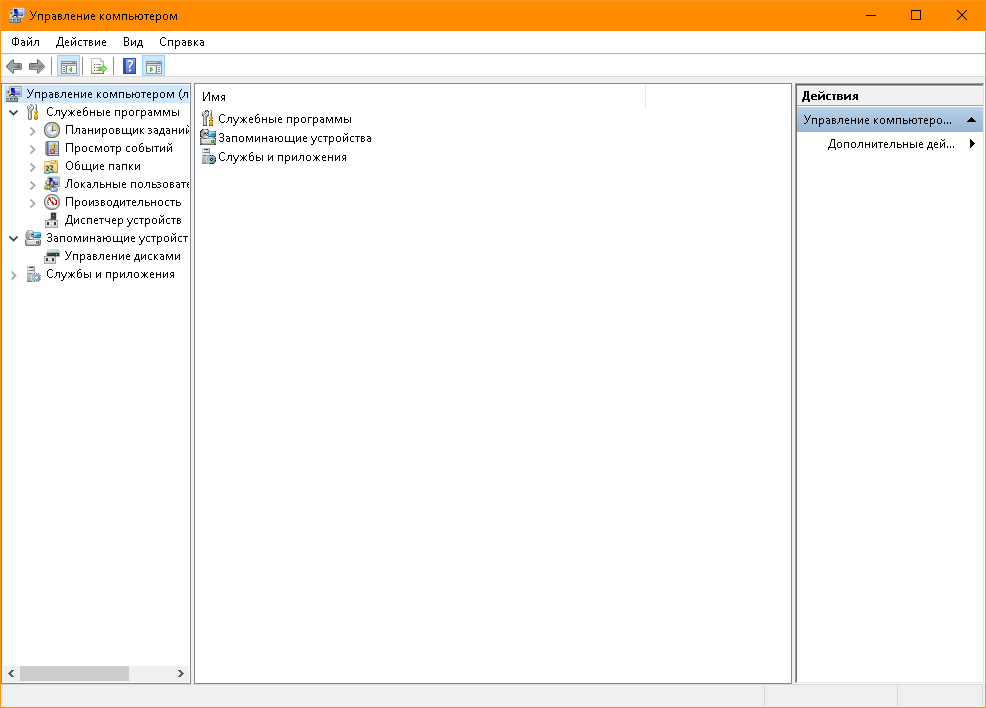


Рисунок 2 – Управление компьютером

* + В левой части окна выберите Локальные пользователи и группы → Пользователи.

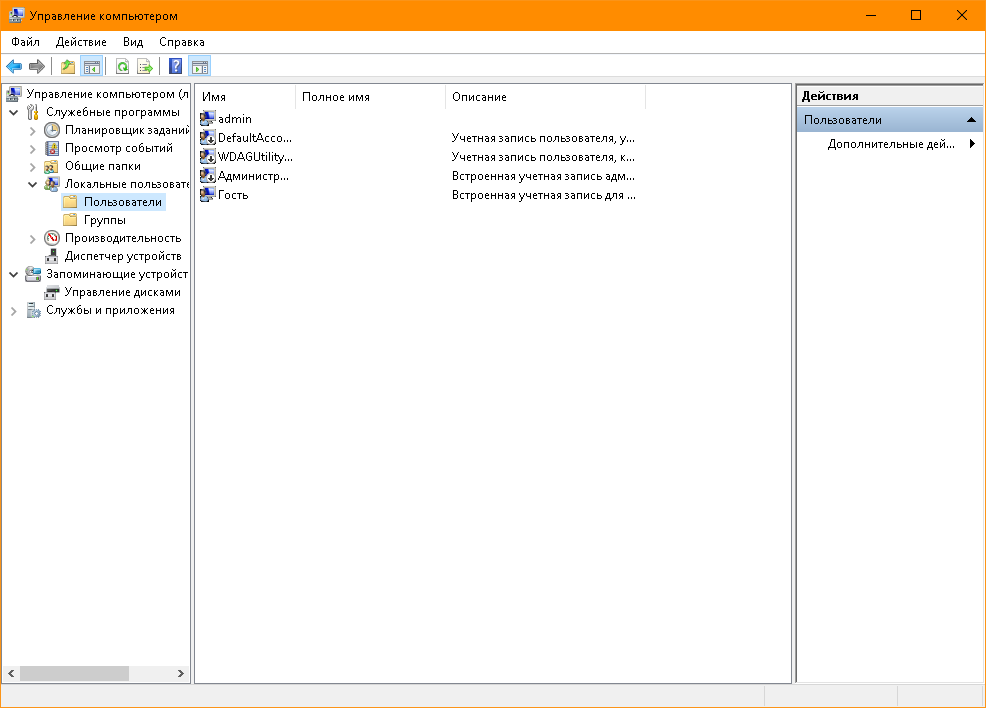


Рисунок 3 - Пользователи

* + Найдите учетную запись Администратор, щелкните на ней правой кнопкой мыши и выберите Задать пароль.

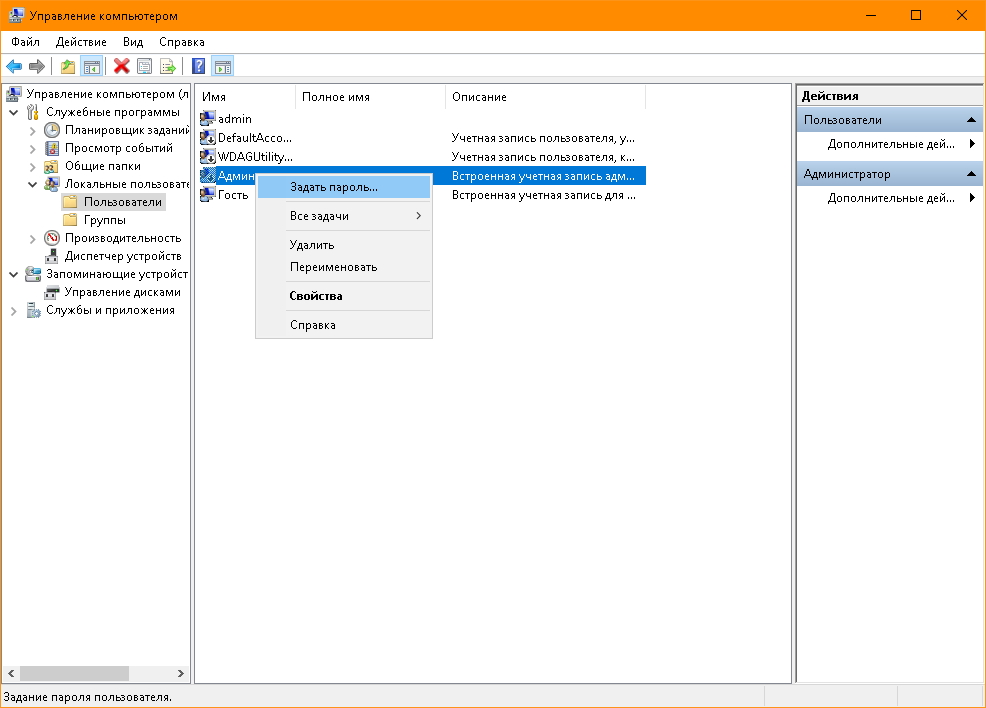


Рисунок 4 – Задание пароля

* + Установите надежный пароль

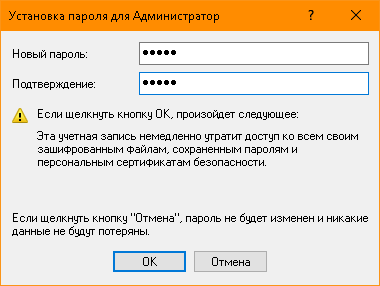


Рисунок 5 – Задание пароля

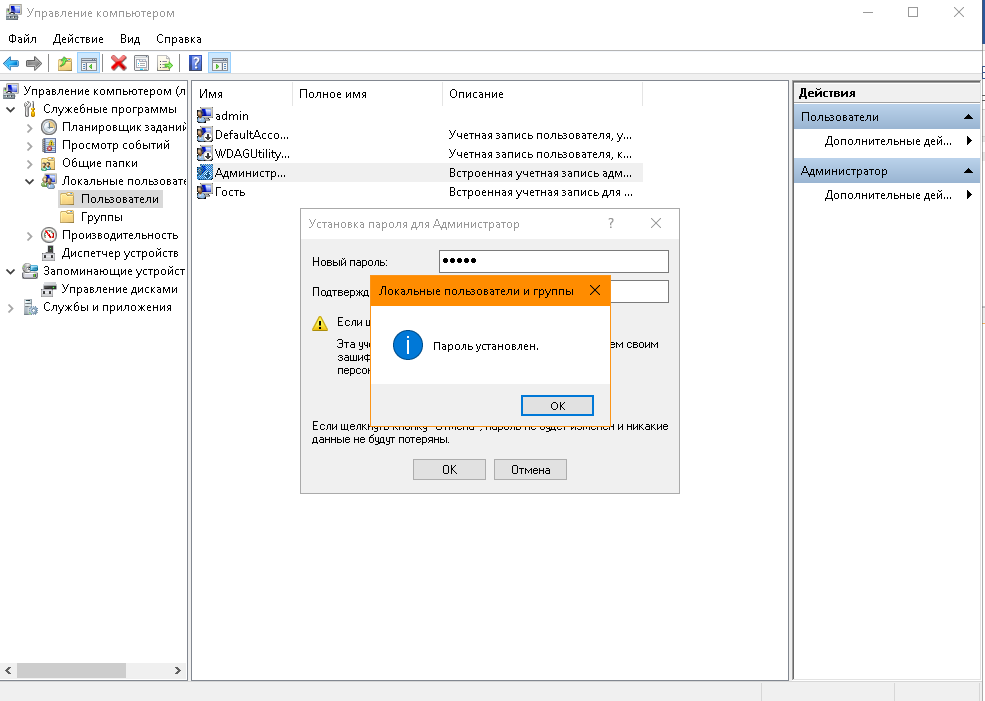


Рисунок 6 – Задание пароля

* Откройте Управление компьютером -> Переименовать и задайте новое название пользователю (Рисунок 7,8).

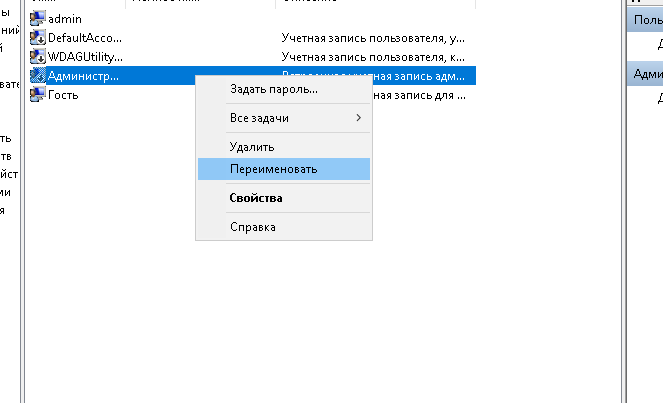


Рисунок 7 – Переименование пользователя

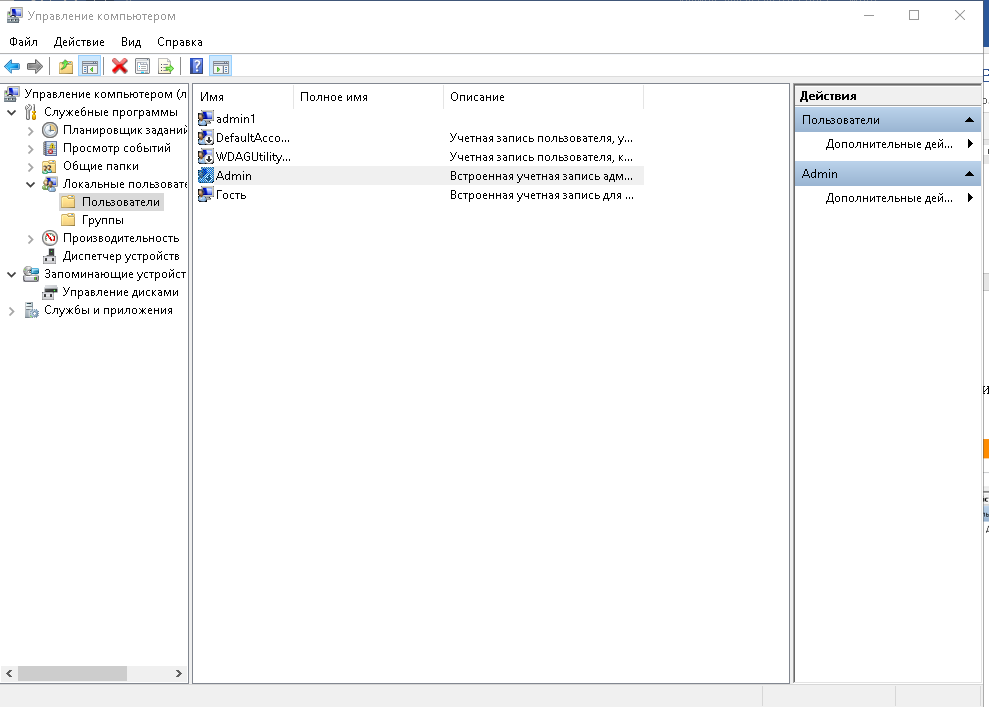


Рисунок 8 – Пользователи

Изменение имени учетной записи и задания пароля можно выполнить через Учетные записи пользователей:

Шаг 2. Делаем окно приветствия пустым (убираем уязвимость 2).

У нас окно входа в систему содержит подсказку Admin, давайте ее уберем, сделав окно пустым. Для начала в окне Учетные записи пользователей жмем на кнопку Изменение входа пользователей в систему и уберем флажок Использовать страницу приветствия.

Теперь повысим безопасность сети еще на одну условную ступень, сделав оба поля окна приветствия пустыми.

Выполним команду Панель управления – Администрирование – Локальные политики безопасности – Локальные политики – Параметры безопасности – Интерактивный вход: не отображать последнего имени пользователя. Эту запись необходимо включить.

Теперь после завершения сеанса пользователь должен угадать не только пароль, но и имя пользователя.

**Шаг 2. Делаем окно приветствия пустым**

Уязвимость: Окно входа в систему отображает имя пользователя, что может облегчить подбор пароля.

1. Требуется открыть редактор локальной групповой политики через команду «Выполнить». Для этого нажмите на Win + R и введите в появившемся окошке gpedit.msc

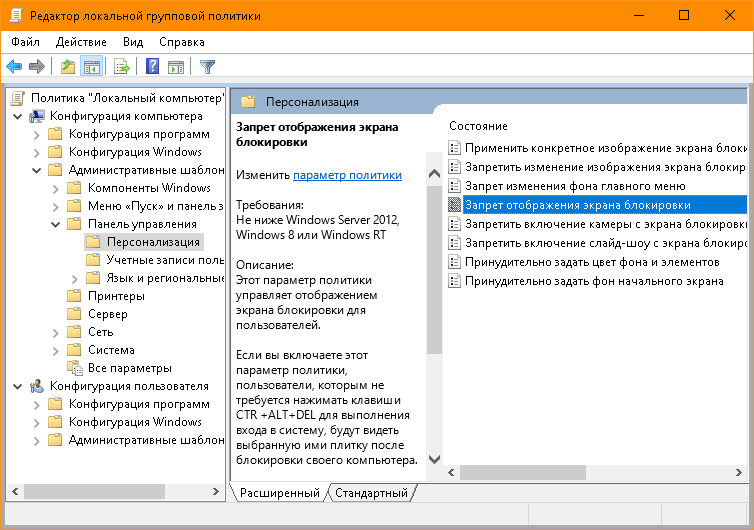


Рисунок 9 – Редактор локальной группы

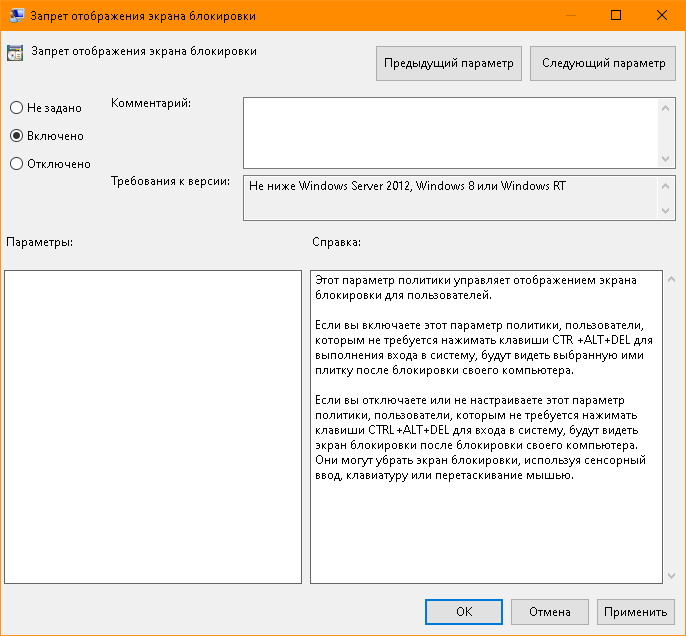


Рисунок 10 – Запрет на отображение экрана блокировки

* Щёлкните два раза по пункту «Запрет отображения экрана блокировки» и поставьте галочку на параметре «Включено». Нажмите на кнопку ОК.

1. Скрытие имени последнего пользователя:
   * Откройте Панель управления → Администрирование → Локальная политика безопасности.
   * Перейдите в Локальные политики → Параметры безопасности.
   * Найдите пункт Интерактивный вход: не отображать последнего имени пользователя.
   * Дважды щелкните по этому пункту, выберите Включено, и нажмите ОК.
2. Проверка:
   * Завершите текущий сеанс (или перезагрузите компьютер).
   * На экране входа в систему теперь будут пустые поля для ввода имени пользователя и пароля.

Злоумышленники используют сканирование портов ПК для того, чтобы воспользоваться ресурсами чужого ПК в Сети. При этом необходимо указать IP адрес ПК и открытый port, к примеру, 195.34.34.30:23. После этого происходит соединение с удаленным ПК с некоторой вероятностью входа в этот ПК.

TCP/IP port – это адрес определенного сервиса (программы), запущенного на данном компьютере в Internet. Каждый открытый порт – потенциальная лазейка для взломщиков сетей и ПК. Например, SMTP (отправка почты) – 25 порт, WWW – 80 порт, FTP – 21 порт.

Хакеры сканируют порты для того, чтобы найти дырку (баг) в операционной системе. Пример ошибки, если администратор или пользователь ПК открыл полный доступ к сетевым ресурсам для всех или оставил пустой пароль на вход к компьютеру.

Одна из функций администратора сети – выявить недостатки в функционировании сети и устранить их. Для этого нужно просканировать сеть и закрыть (блокировать) все необязательные (открытые без необходимости) сетевые порты. Ниже, для примера, представлены службы TCP/IP, которые можно отключить:

– finger – получение информации о пользователях

– talk – возможность обмена данными по сети между пользователями

– bootp – предоставление клиентам информации о сети

– systat – получение информации о системе

– netstat – получение информации о сети, такой как текущие соединения

– rusersd – получение информации о пользователях, зарегистрированных в данный момент.

Просмотр активных подключений утилитой Netstat. Команда netstat обладает набором ключей для отображения портов, находящихся в активном и/или пассивном состоянии. С ее помощью можно получить список серверных приложений, работающих на данном компьютере. Большинство серверов находится в режиме LISTEN– ожидание запроса на соединение. Состояние CLOSE\_WAIT означает, что соединение разорвано. TIME\_WAIT – соединение ожидает разрыва. Если соединение находится в состоянии SYN\_SENT, то это означает наличие процесса, который пытается, установить соединение с сервером. ESTABLISHED – соединения установлены, т. е. сетевые службы работают (используются).

Итак, команда netstat показывает содержимое различных структур данных, связанных с сетью, в различных форматах в зависимости от указанных опций. Для сокетов (программных интерфейсов) TCP допустимы следующие значения состояния:

CLOSED – закрыт, сокет не используется; LISTEN – ожидает входящих соединений;

SYN\_SENT – активно пытается установить соединение; SYN\_RECEIVED – идет начальная синхронизация соединения;

ESTABLISHED – соединение установлено;

CLOSE\_WAIT – удаленная сторона отключилась; ожидание закрытия сокета; FIN\_WAIT\_1 – сокет закрыт; отключение соединения; CLOSING – сокет закрыт,

затем удаленная сторона отключилась; ожидание подтверждения;

LAST\_ACK – удаленная сторона отключилась, затем сокет закрыт; ожидание подтверждения;

FIN\_WAIT\_2 – сокет закрыт; ожидание отключения удаленной стороны;

TIME\_WAIT – сокет закрыт, но ожидает пакеты, ещё находящиеся в сети для обработки.

**Обнаружение открытых на ПК портов утилитой Netstat.**

Для выполнения практического задания на компьютере необходимо выполнить команду Пуск – Выполнить. Откроется окно Запуск программы, в нем введите команду cmd.

Чтобы вывести все активные подключения TCP и прослушиваемые компьютером порты TCP/ UDP введите команду netstat. Мы видим Локального адреса (это ваш ПК) прослушиваются 6 портов. Они нужны для поддержки сети. На двух портах мы видим режим ESTABLISHED – соединения установлены, т. е. сетевые службы работают (используются). Четыре порта используются в режиме TIME\_WAIT – соединение ожидает разрыва.

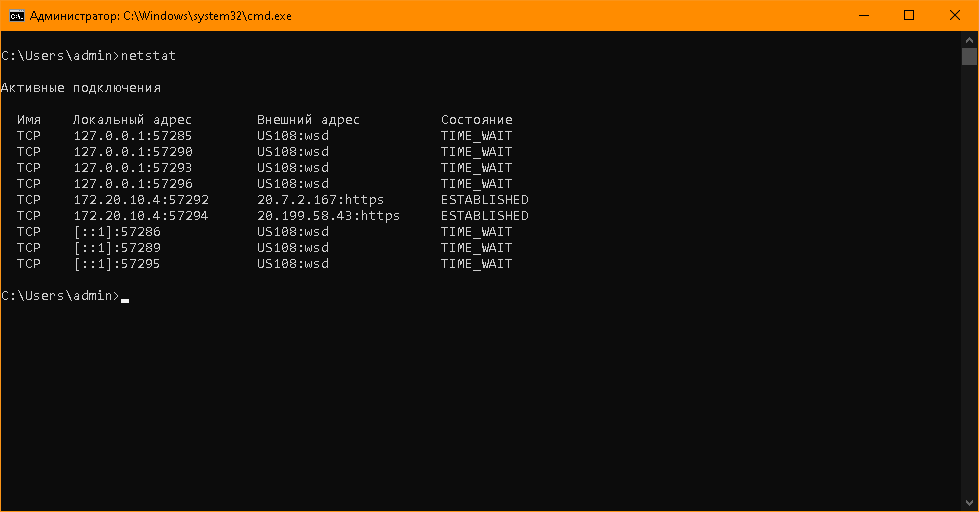


Рисунок 11 – Выполнение команды netstat

Запустите на вашем ПК Интернет и зайдите, например на www.yandex.ru. Снова выполните команду netstat. Как видим, добавилось несколько новых активных портов с их различными состояниями.

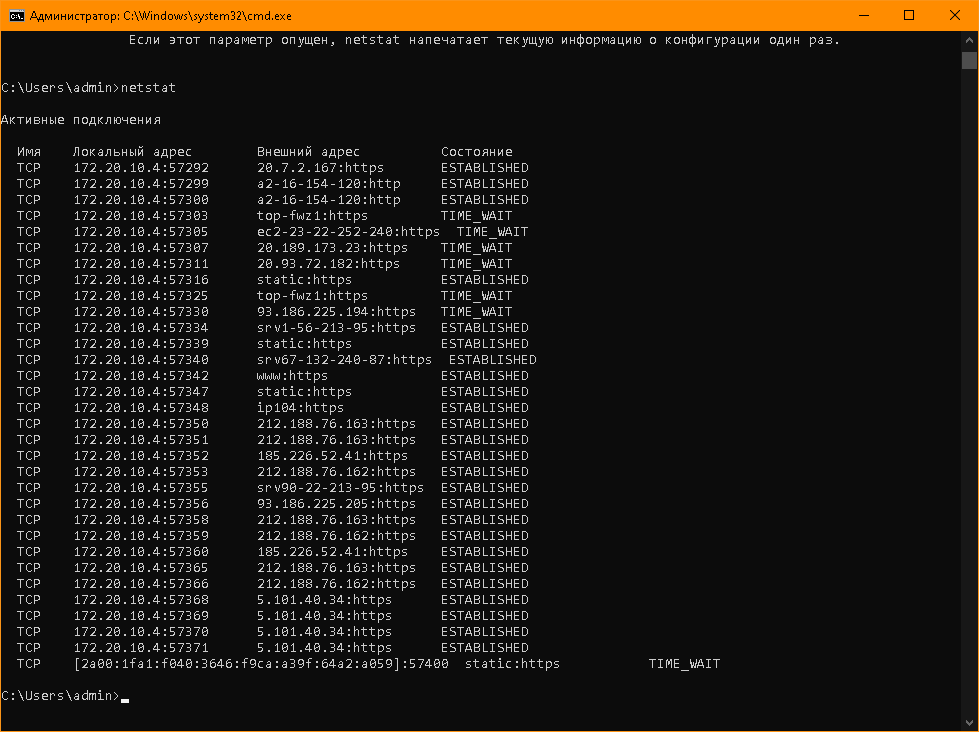


Рисунок 12 - Выполнение команды netstat

Опции команды netstat приведены в таблице 1.

Таблица 1 – Ключи для команды netstat

|  |  |
| --- | --- |
| **Опция (ключ)** | **Назначение** |
| -a | Показывать состояние всех сокетов; обычно сокеты, используемые серверными процессами, не показываются. |
| -A | Показывать адреса любых управляющих блоков протокола, связанных с сокетами; используется для отладки. |
| -i | Показывать состояние автоматически сконфигурированных (auto-configured) интерфейсов. Интерфейсы, статически сконфигурированные в системе, но ненайденные во время загрузки, не показываются. |
| -n | Показывать сетевые адреса как числа. netstat обычно показывает адреса как символы. Эту опцию можно использовать с любым форматом показа. |
| -r | Показать таблицы маршрутизации. При использовании с опцией - s, показывает статистику маршрутизации. |
| -s | Показать статистическую информацию по протоколам. При использовании с опцией - r, показывает статистику маршрутизации. |
| -f семейство адресов | Ограничить показ статистики или адресов управляющих блоков только указанным семейством адресов, в качестве которого можно указывать:**inet** |
| -I  интерфейс | Выделить информацию об указанном интерфейсе в отдельный столбец; по умолчанию (для третьей формы команды) используется интерфейс с наибольшим объёмом переданной информации с момента последней перезагрузки системы. В качестве интерфейса можно указывать любой из интерфейсов, перечисленных в файле конфигурации системы, например, emd1 или lo0. |
| -p | Отобразить идентификатор/название процесса, создавшего сокет (-p, — programs display PID/Program name for sockets) |

С помощью программы NetStat Agent можно найти причину проблемы и заблокировать ее. Иначе говоря, NetStat Agent – полезный набор инструментов для мониторинга Интернет соединений и диагностики сети. Программа позволяет отслеживать TCP и UDP соединения на ПК, закрывать нежелательные соединения, завершать процессы, обновлять и освобождать DHCP настройки адаптера, просматривать сетевую статистику для адаптеров и TCP/IP протоколов, а также строить графики для команд Ping иTraceRoute.

В состав программы NetStat Agent вошли следующие утилиты:

– NetStat – отслеживает TCP и UDP соединения ПК (при этом отображается географическое местоположение удаленного сервера и имя хоста);

– IPConfig – отображает свойства сетевых адаптеров и конфигурацию сети;

– Ping – позволяет проверить доступность хоста в сети;

– TraceRoute – определяет маршрут между вашим компьютером и конечным хостом, сообщая все IP-адреса маршрутизаторов;

– DNS Query – подключается к DNS серверу и находит всю информацию о домене (IP адрес сервера, MX-записи (Mail Exchange) и др.).

– Route – отображает и позволяет изменять IP маршруты на ПК;

– ARP – отслеживает ARP изменения в локальной таблице;

– Whois – позволяет получить всю доступную информацию об IP-адресе или домене;

– HTTP Checker – помогает проверить, доступны ли Ваши веб-сайты;

– Statistics – показывает статистику сетевых интерфейсов и TCP/IP протоколов.

**Сканер портов Nmap (Zenmap)** – популярный сканер портов, который обследует сеть и проводит аудит защиты. Сканером портов Nmap можно определить открытые порты компьютера, а для безопасности сети пользователям рекомендуется закрыть доступ к этим портам с помощью брандмауэра.

Обычно для того, чтобы просканировать все порты какого- либо компьютера в сети вводится команда nmap –p1-65535 IP- адрес\_компьютера или nmap –sV IP-адрес компьютера, а для сканирования сайта – команда nmap –sS –sV –O – P0 адрес сайта.

**Монитор портов TCPView** показывает все процессы, использующие Интернет- соединения.

Запустив TCPView, можно узнать, какой порт открыт и какое приложение его использует, а при необходимости и немедленно разорвать соединение.

**Контрольные вопросы:**

**1. Какие виды мониторинга рабочих операций пользователя существуют?**

Существует несколько видов мониторинга:

* **Системный мониторинг**: отслеживание активности на уровне ОС (использование ресурсов, запуск программ, процессы).
* **Сетевой мониторинг**: контроль сетевой активности (подключения, трафик, использование протоколов).
* **Логический мониторинг**: фиксация действий пользователя в приложениях (ввод данных, выполнение команд).
* **Физический мониторинг**: контроль физических действий (записи камер, использование периферийных устройств).
* **Отчетный мониторинг**: сбор статистики о действиях пользователя с последующим формированием отчетов.

**2. Дайте характеристику современных программных средств мониторинга действий пользователей.**

Современные средства мониторинга имеют следующие характеристики:

* **Автоматизация**: работают в фоновом режиме, не отвлекая пользователя.
* **Гибкость настроек**: позволяют адаптировать уровень контроля под нужды организации.
* **Сбор логов**: фиксируют подробные данные о действиях (запуск программ, открытие файлов, сетевые подключения).
* **Аналитика**: инструменты обработки данных для выявления аномалий и создания отчетов.
* **Защита данных**: соответствуют стандартам безопасности и конфиденциальности.

Примеры программ: StaffCop, Teramind, Kickidler.

**3. Какое программное средство вы порекомендовали? Почему?**

**Рекомендация**: Teramind.

**Причины**:

* Поддерживает глубокую аналитику действий пользователей.
* Обеспечивает мониторинг в реальном времени и генерацию отчетов.
* Удобный интерфейс и гибкость настроек.
* Соответствует требованиям конфиденциальности и стандартам безопасности.

**4. Какие уязвимости операционной системы Windows были устранены в данной работе и какими путями?**

Примеры уязвимостей и их устранение:

* **Закрытие незадействованных портов**: предотвращение несанкционированного доступа к системным службам.
* **Обновление ОС**: установка последних патчей для защиты от известных уязвимостей.
* **Настройка файрвола**: использование встроенного брандмауэра для контроля трафика.
* **Ограничение привилегий пользователей**: минимизация риска выполнения вредоносного кода.

**5. Как узнать закрытые порты?**

Для проверки портов можно использовать:

* Команду netstat -an в терминале (выводит список активных портов).
* Утилиту **Nmap**: команда nmap -p- <IP-адрес> покажет открытые и закрытые порты.
* Специализированные приложения, например, **TCPView** или **NetStat Agent**.

**6. Как открыть нужный порт?**

Открыть консоль **Windows PowerShell** или настройки брандмауэра.

Вручную добавить правило в файрвол:

* Перейти в "Брандмауэр Windows с расширенной безопасностью".
* Создать новое входящее или исходящее правило.
* Указать номер порта и разрешить соединения.

Использовать команду:

netsh advfirewall firewall add rule name="Порт 8080" dir=in action=allow protocol=TCP localport=8080

**7. Для чего используется программа NetStat Agent?**

NetStat Agent используется для:

* Мониторинга активных сетевых подключений.
* Определения открытых и прослушивающих портов.
* Диагностики проблем с сетевой безопасностью.
* Выявления подозрительных подключений.

**8. Для чего используется программа Nmap?**

Nmap (Network Mapper) применяется для:

* Сканирования сети на наличие активных устройств и открытых портов.
* Выявления уязвимостей в сетевой инфраструктуре.
* Проведения аудита безопасности.
* Определения типов ОС и сервисов на хостах.

**9. Для чего используется программа TCPView?**

TCPView позволяет:

* Отслеживать все активные TCP/UDP подключения в реальном времени.
* Определять, какие процессы используют сетевые порты.
* Завершать нежелательные или подозрительные соединения.
* Анализировать сетевую активность для устранения проблем.