

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Хоменко Елена Семеновна

Должность: исполняющая обязанности заведующей филиалом, начальник отдела

учебно-производственной работы

Дата подписания: 12.05.2023 04:35:46

Уникальный программный ключ:

03c04d4933a2307f9c20d0107fe3c7a0c84980be

Министерство образования и науки РС (Я)
ГБПОУ РС (Я) «Ленский технологический техникум»
филиал «Пеледуйский»

**Методические указания по выполнению
Практических работ по учебной дисциплине
«Информационная безопасность»**

09.01.03. «Мастер по обработке цифровой информации»

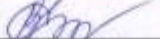
п. Пеледуй 2022 г.

Методические рекомендации по выполнению практических работ соответствует рабочей программе дисциплины ОП.7 «Информационная безопасность», разработанной в соответствии с федеральным государственным образовательным стандартом по программе подготовки квалифицированных рабочих (служащих) по профессии 09.01.03 Мастер по обработке цифровой информации (утвержден приказом Министерства образования и науки Российской Федерации от 02.08.2013 № 854), из вариативной части.

Организация-разработчик:
Государственное бюджетное профессиональное образовательное учреждение
Республики Саха (Якутия)
«Ленский технологический техникум» филиал «Пеллудуйский»

Разработчик Дубинин К.В. преподаватель

Рассмотрено и рекомендовано
Методическим советом
Протокол № 44 « 03 » октября 2022 г.

Председатель  /Вавилова Е.Ю. /

Пояснительная записка

Методические указания по дисциплине «Информационная безопасность» для выполнения практических работ созданы в помощь студентам для работы на занятиях, подготовки к практическим занятиям и для правильного составления отчетов.

Уважаемые студенты, приступая к выполнению практической работы, Вы должны внимательно прочитать цель и задачи занятия, ознакомиться с требованиями к уровню Вашей подготовки в соответствии с федеральными государственными стандартами (ФГОС), краткими теоретическими и учебно-методическими материалами по теме практической работы, ответить на вопросы для закрепления теоретического материала.

Все задания к практической работе Вы должны выполнять в соответствии с инструкцией, анализировать полученные в ходе занятия результаты по приведенной методике.

Отчет о практической работе Вы должны выполнить по приведенному алгоритму, опираясь на образец.

Наличие положительной оценки по практическим работам необходимо для получения дифференцированного зачета по дисциплине «Информационная безопасность», поэтому в случае отсутствия на уроке по любой причине или получения неудовлетворительной оценки за практическую работу Вы должны найти время для ее выполнения или пересдачи.

Обучающийся, освоивший дисциплину, должен обладать следующими знаниями:

- сущность и понятие информационной безопасности, характеристику ее составляющих;
 - место информационной безопасности в системе национальной безопасности страны;
 - виды, источники и носители защищаемой информации;
 - источники угроз безопасности информации и меры по их предотвращению;
 - факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;
 - жизненные циклы информации
- ограниченного доступа в процессе ее создания, обработки, передачи;
- современные средства и способы обеспечения информационной безопасности;
 - основные методики анализа угроз и рисков информационной безопасности.

Обучающийся, освоивший дисциплину, должен обладать следующими умениями:

- классифицировать защищаемую информацию по видам тайны и степеням секретности;
- классифицировать основные угрозы безопасности информации.

Перечень тем практических работ

Раздел и тема дисциплины	Наименование практических занятий и лабораторных работ	Объем часов
Средства защиты информации		
Антивирусная защита	Практическая работа № 1 Использование встроенных средств защиты системы	2
	Практическая работа № 2 Установка бесплатных антивирусных программ на примере AVG, Avira, Avast.	2
	Практическая работа № 3 Настройка и обновление бесплатных антивирусных программ на примере AVG, Avira, Avast.	2
	Практическая работа № 4 Установка и настройка средств защиты от лаборатории «Касперский»	4
	Практическая работа № 5 Установка и настройка средств защиты от лаборатории «доктор ВЭБ»	2
	Практическая работа № 6 Проверка компьютера на наличие угроз	4
	Практическая работа № 7 Проверка носителей на наличие угроз	4
	Практическая работа № 8 Использование специальных антивирусных утилит, исправляющих последствия вирусной атаки	6
	Практическая работа № 9 Борьба с рекламными и шпионскими программами	2
	Практическая работа № 10 Настройка межсетевоего экрана	2
Сетевая безопасность		
Защита информации в компьютерных сетях	Практическая работа № 11 Парольный доступ и парольная аутентификация	4
	Практическая работа № 12 Создание цифровой подписи	4
ВСЕГО:		38

Практическая работа № 1

Тема:«Использование встроенных средств защиты системы»

Цель:Определить и освоить встроенные средства защиты операционной системы.

Оборудование и необходимые материалы:Компьютер с установленной операционной системой версии не ниже Windows 8.1

Ход работы:При выполнении практической работы, необходимо используя компьютер на своем рабочем месте, определите какие средства защиты имеются у вас. Проверит актуальность обновления операционной системы и средств защиты.

Практическая работа № 2

Тема:«Установка бесплатных антивирусных программ на примере AVG, Avira, Avast.»

Цель:Получения знаний по установке и настройке сторонних бесплатных антивирусных программ.

Оборудование и необходимые материалы:Компьютер с установленной операционной системой версии не ниже Windows 8.1 и доступ к сети интернет.

Ход работы.

При выполнении практической работы, необходимо:

- используя браузер, найти и скачать бесплатную версию предлагаемого антивирусного обеспечения;
- определить наличие ранее установленного антивирусного программного обеспечения и при наличии, произвести ее удаление;
- произвести установку скаченного антивирусного обеспечения.

Практическая работа № 3

Тема:«Настройка и обновление бесплатных антивирусных программ на примере AVG, Avira, Avast.»

Цель:Получения знаний по обновлению сторонних бесплатных антивирусных программ.

Оборудование и необходимые материалы:Компьютер с установленной операционной системой версии не ниже Windows 8.1 и доступ к сети интернет.

Ход работы.

При выполнении практической работы, необходимо:

- определить версию скаченной вирусной базы антивирусного обеспечения и версию самой программы;
- произвести обновлений вирусной базы на актуальную дату и программного обеспечения.

Практическая работа № 4

Тема:«Установка и настройка средств защиты от лаборатории «Касперский»

Цель:Получения знаний по установке и настройке антивирусного обеспечения от лаборатории «Касперский»

Оборудование и необходимые материалы:Компьютер с установленной операционной системой версии не ниже Windows 8.1 и доступ к сети интернет.

Ход работы.

При выполнении практической работы, необходимо:

- используя браузер, найти и скачать антивирусное обеспечение от лаборатории «Касперский»;
- определить наличие ранее установленного антивирусного программного обеспечения и при наличии, произвести ее удаление;
- произвести установку скаченного антивирусного обеспечения;
- произвести обновление вирусной базы;

Практическая работа № 5

Тема:«Установка и настройка средств защиты от лаборатории «доктор ВЭБ»

Цель:Получения знаний по установке и настройке антивирусного обеспечения от лаборатории «доктор ВЭБ»

Оборудование и необходимые материалы:Компьютер с установленной операционной системой версии не ниже Windows 8.1 и доступ к сети интернет.

Ход работы.

При выполнении практической работы, необходимо:

- используя браузер, найти и скачать антивирусное обеспечение от лаборатории «доктор ВЭБ»;
- определить наличие ранее установленного антивирусного программного обеспечения и при наличии, произвести ее удаление;
- произвести установку скаченного антивирусного обеспечения;
- произвести обновление вирусной базы;

Практическая работа № 6

Тема:«Проверка компьютера на наличие угроз»

Цель:Получения знаний по поиску вирусов на компьютере и обезвреживание.

Оборудование и необходимые материалы:Компьютер с установленной операционной системой версии не ниже Windows 8.1 и доступ к сети интернет

Ход работы.

При выполнении практической работы, необходимо:

- используя имеющее антивирусное обеспечение определить актуальность установленной вирусной базы и в случае необходимости, произвести ее обновление;
- произвести полное сканирование вашего компьютера на наличие вирусных угроз и обезвреживание при наличии таковых.

Практическая работа № 7

Тема:«Проверка носителей на наличие угроз»

Цель:Получения знаний по поиску и обезвреживанию вирусов на переносных носителях.

Оборудование и необходимые материалы:Компьютер с установленной операционной системой версии не ниже Windows 8.1 и доступ к сети интернет.

Ход работы.

При выполнении практической работы, необходимо:

- используя имеющееся антивирусное обеспечение определить актуальность установленной вирусной базы и в случае необходимости, произвести ее обновление;
- произвести полное сканирование переносных носителей, выданных преподавателем на наличие вирусных угроз.
- в случае обнаружения вирусных угроз, произвести обезвреживание, используя средства защиты.

Практическая работа № 8

Тема:«Использование специальных антивирусных утилит, исправляющих последствия вирусной атаки»

Цель:Получения знаний по устранению последствий вирусной атаки.

Оборудование и необходимые материалы:Компьютер с установленной операционной системой версии не ниже Windows 8.1 и доступ к сети интернет и переносной носитель.

Ход работы.

При выполнении практической работы, необходимо:

- используя сеть интернет, необходимо на сайте лаборатории «Касперского» произвести скачивание «KasperskyRescueDisk»
- при помощи программы UltraISOпроизвести монтирование образа «KasperskyRescueDisk» на съемный носитель;
- загрузиться со съемного носителя с установленным образом «KasperskyRescueDisk»

- произвести полное сканирование вашей операционной системы из оболочки «KasperskyRescueDisk»
- в случае обнаружения вирусных угроз, произвести обезвреживание, используя средства защиты «KasperskyRescueDisk»

Практическая работа № 9

Тема:«Борьба с рекламными и шпионскими программами»

Цель:С помощью программы удаления рекламных и шпионских программ (например, Ad-Adware) очистить компьютер от adware и spyware программ.

Оборудование и необходимые материалы:Компьютер с установленной операционной системой версии не ниже Windows 8.1 и доступ к сети интернет.

Ход работы.

При выполнении практической работы, необходимо:

- используя сеть интернет, необходимо скачать и установить программу Ad-Adware, которая удаляет рекламные и шпионские программы;
- произвести сканирование и обезвреживания найденных критических и подозрительных объектов.

Практическая работа № 10

Тема:«Настройка межсетевого экрана»

Цель:Познакомиться на практике с особенностями конфигурирования межсетевых экранов и фильтров на примере программ OutpostFirewallPro

Оборудование и необходимые материалы:Компьютер с установленной операционной системой версии не ниже Windows 8.1 и доступ к сети интернет.

Ход работы.

При выполнении практической работы, необходимо:

- Используя сеть интернет, найти и установить OutpostFirewallPro

- Запустить консоль администрирования Outpost («Пуск» – «Все программы» – «Agnitum» – «OutpostFirewall»). Определите, сколько и какие программы обнаружил Outpost, какой уровень доверия им присвоен и какие правила для них (внести в отчет).
- Добавить новое сетевое приложение (например, IExplorer). Создать для него правила на основе предустановок, как для браузера.
- Поэкспериментировать с добавлением и удалением правил для приложений, сменой их уровня доверия.
- Разрешите доступ к Интернет только InternetExplorer, а остальным приложениям запретите.
- Исследуйте правила InternetExplorer. Через какие порты разрешен доступ (внесите в отчет)? Подробно опишите в отчете правило InternetExplorer FTP connection.
- Изучить настройки контроля Anti-Leak. Какие возможности он предоставляет (внести в отчет)?
- Исследовать настройки контроля компонентов. Какие возможности он предоставляет (внести в отчет)?
- Исследовать доступные политики МЭ. Сменить политику на «Блокировать». Попробуйте подключиться к соседнему компьютеру (через «Сетевое окружение»). Удалось ли это сделать? Почему? Сменить политику на «Запрещать». Удалось ли подключиться теперь? Внести в отчет результаты.
- Изучите системные настройки («Параметры» – «Системные»). Какие возможности здесь предоставлены (внести в отчет)? Чем отличается режим невидимости от обычного режима (внести в отчет)?
- Изучить дополнительные подключаемые модули Outpost. Внесите в отчет возможности, которые они предоставляют.
- Отключите службу Outpost и выйдите из этого приложения.

Тема:«Парольный доступ и парольная аутентификация»

Цель:Изучить методы повышения надежности путем практического применения рекомендаций по администрированию парольной системы операционной системы

Оборудование и необходимые материалы:Компьютер с установленной операционной системой версии не ниже Windows 8.1 и доступ к сети интернет.

Ход работы.

Откройте **Панель управления** → **Администрирование** → **Локальная политика безопасности**. Выберите в списке **Политика учетных записей** и **Политика паролей**. Для *Windows Vista* экран консоли управления будет выглядеть так, как представлено на рис. 1.

Значения выбранного параметра можно изменить (рис. 2). Надо понимать, что не все требования политики паролей автоматически подействуют в отношении всех учетных записей. Например, если в свойствах учетной записи стоит "Срок действия пароля не ограничен", установленное политикой требование максимального срока действия пароля будет игнорироваться.

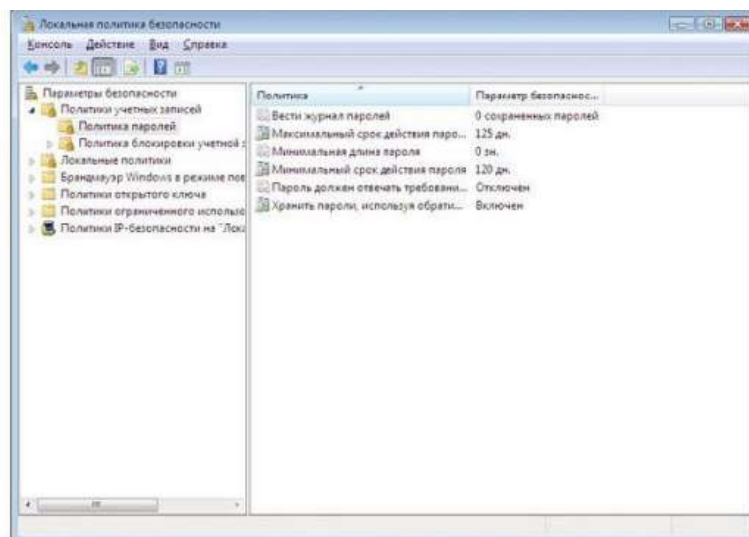


Рис. 1. Настройка политики паролей

Для обычной пользовательской учетной записи, эту настройку лучше не устанавливать. Но в некоторых случаях она рекомендуется. Например, если в учебном

классе нужна "групповая" учетная запись, параметры которой известны всем студентам, лучше поставить для нее "Срок действия пароля не ограничен" и "Запретить смену пароля пользователем".

Свойства учетной записи можно посмотреть **управления** → в **Панель Администрирование** → **Управление компьютером**, там выберите **Локальные пользователи и группы** и **Пользователи** (или запустив эту же оснастку через **Пуск** → **Выполнить** → **lusrmgr.msc**).

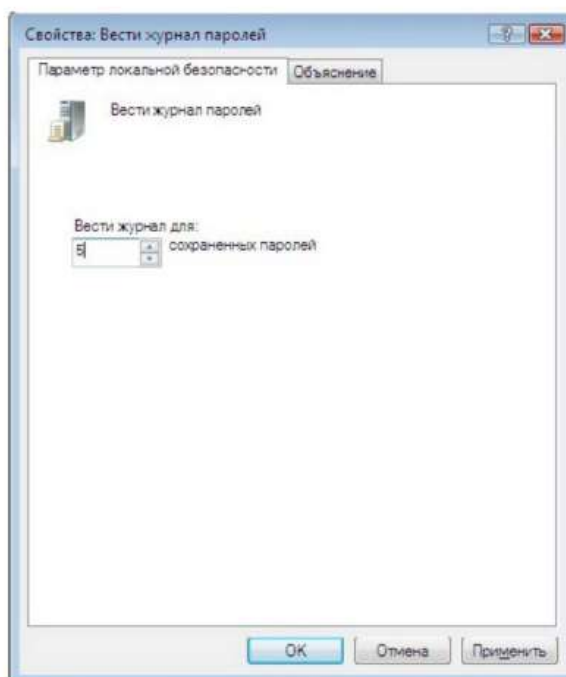


Рис. 2- Установка требования ведения журнала паролей

Практическая работа № 12

Тема: «Создание цифровой подписи»

Цель: На примере программы Kleopatra научиться создавать электронную подпись.

Оборудование и необходимые материалы: Компьютер с установленной операционной системой версии не ниже Windows 8.1 и доступ к сети интернет.

Ход работы.

- Используя сеть интернету скачать приложение Kleopatra;
- Установить приложение Kleopatra;
- Сгенерировать в Kleopatra новую пару ключей (открытый + закрытый) по алгоритму RSA;
- Экспортировать открытый ключ в файл и передать его партнеру (одногруппнику (-це)) по электронной почте
- Получить открытый ключ партнера (файл с расширением .asc) и импортировать его в Kleopatra, заверить своим закрытым ключом.
- Создать файл формата .doc/.docx/.txt с текстом
- Используя открытый ключ партнера, зашифровать для него созданный файл в Kleopatra и передать по его электронной почте
- Расшифровать зашифрованный файл (сначала без подписи, затем с подписью) партнера своим закрытым ключом
- Созданный в п.5 текстовый документ подписать своей электронной подписью и отправить партнеру два файла: сам документ и файл с подписью (***.sig).
- Проверить электронную подпись партнера.
- Изменить содержание документа и проверить электронную подпись повторно.