Министерство образования и науки РД

ГБПОУ «Дорожно – строительный колледж»

**Конспект урока**

**«Хакерские утилиты и защита от них»**

**Для групп № 35 «А», 36 «А», 40М**

Выполнил:

Юсупов Али Зевдиевич

Дата проведения 26.03.2020г.

**Учебник Угринович Н. Д. «Информатика и ИКТ», 11 класс.**

***Тема урока***: «Хакерские утилиты и защита от них».

***Цели урока***

***Образовательная***

* познакомить учащихся с понятием «хакерские утилиты», типами хакерских атак и методами защиты от них;
* формировать практические умения и навыки при обнаружении и обезвреживании руткиты, а также защищать компьютера от хакерских атак.

***Развивающая***

* развивать память, внимание, алгоритмическое мышление.
* способствовать развитию творческой деятельности учащихся и интереса к предмету информатика;

***Воспитательная***

* воспитывать аккуратность, формировать познавательный интерес к информатике;
* воспитывать умение внимательно выслушивать мнение других, воспитание культуры общения.

***Тип урока:*** урок изучения и первичного закрепления нового материала.

***Форма урока:*** урок изучения нового материала.

***Методы обучения:*** наглядный, словесный, практический.

***Оборудование:*** мультимедийный проектор, экран, презентация, компьютеры, доска, маркер.

***План проведения урока:***

1. Организационный момент –1 мин.
2. Подготовительный этап – 1 мин.
3. Изучение нового материала – 36 мин.
4. Подведение итогов уроков – 1 мин.
5. Информация о домашнем задании – 1 мин.

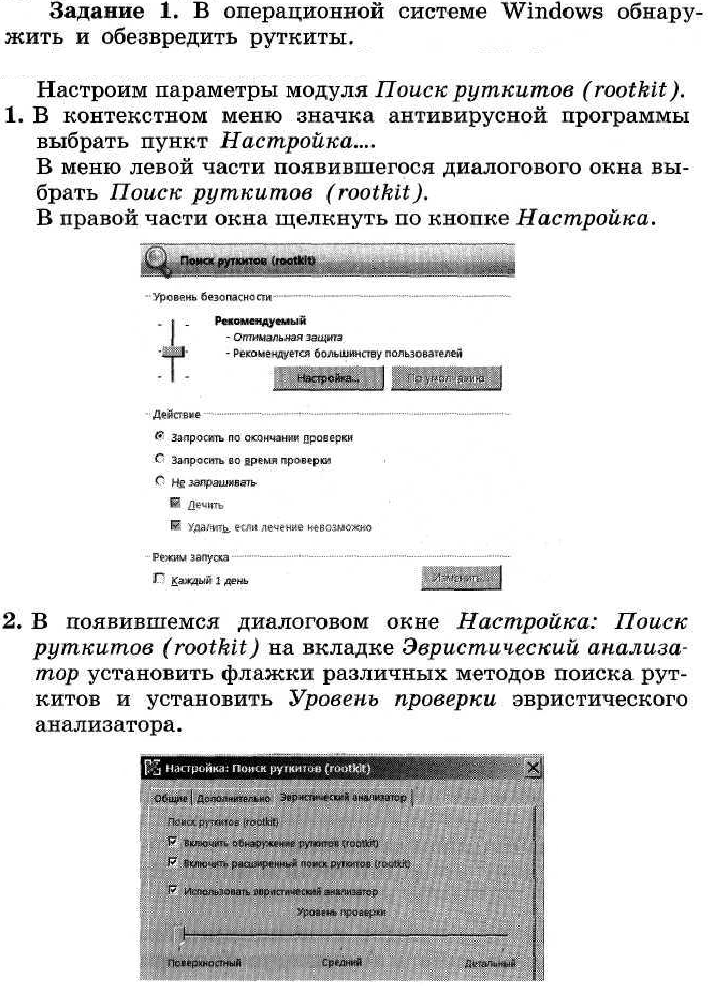
***Ход урока:***

|  |  |
| --- | --- |
| **Деятельность** | |
| **Учителя** | **Учащихся** |
| 1. ***Организационный момент*** | |
| **Цель:** подготовить учащихся и кабинет информатики к уроку. | |
| Здравствуйте | Кол-во приявших участие будет определено по отчётам старостата |
| 1. ***Подготовительный этап.*** | |
| **Цель:** организовать и направить познавательную деятельность обучающихся | |
| На сегодняшнем уроке мы с Вами продолжим знакомиться с видами компьютерных вирусов, способами их распространения, а также будем учиться обнаруживать и обезвреживать руткиты и защищать компьютер от хакерских атак.  Откроем тетради, запишем число и тему урока «Хакерские утилиты и защита от них».  **СЛАЙД 1** | Изучить тему  Открыть тетради и записать число и тему урока. |
| 1. ***Изучение нового материала.*** | |
| **Цель:** обеспечить восприятие, осмысление и первичное запоминание (закрепление) нового материала. | |
| **СЛАЙД 2**    Итак, что такое Сетевые атаки?  Сетевые атаки – это направленные действияна удаленные сервера для  создания затруднений в работе или утери данных.  Запишем это определение в тетрадь.  Сетевые атаки на удаленные серверы реализуются с помощью специальных программ, которые посылают на них специфические запросы.  Это приводит к отказу в обслуживании («зависанию» сервера), если ресурсы атакуемого сервера недостаточны для обработки всех поступающих запросов.  Существуют два типа сетевых атак.  Внимание на слайд!  **СЛАЙД 3**    Первый тип это DoS-программы.  DoS-программы (от англ. Denial of Service – отказ в обслуживании) реализуют атаку с одного компьютера с ведома пользователя.  Запишем это определение в тетрадь.  DoS-программы обычно наносят ущерб удаленным компьютерам и сетям, не нарушая работоспособность зараженного компьютера.  Некоторые сетевые черви содержат в себе DoS-процедуры, атакующие конкретные сайты. Так, червь «Codered» 20 августа 2001 года организовал успешную атаку на официальный сайт президента США, а червь «Mydoom» 1 февраля 2004 года «выключил» сайт компании – производителя дистрибутивов UNIX.  Второй тип сетевых атак - это DDoS-программы.  **СЛАЙД 4**    DDoS-программы *(от англ. Distributed DoS – распределенный DoS)* реализуют распределенные атаки с разных компьютеров, причем без ведома пользователей зараженных компьютеров.  Запишем определение в тетрадь.  Для этого DDoS-программа засылается на компьютеры «жертв-посредников» и после запуска в зависимости от текущей даты или по команде от хакера начинает сетевую атаку на указанный сервер в сети.  Некоторые хакерские утилиты реализуют фатальные сетевые атаки. Такие утилиты используют уязвимости в операционных системах и приложениях и отправляют специально оформленные запросы на атакуемые компьютеры в сети. В результате сетевой запрос специального вида вызывает критическую ошибку в атакуемом приложении, и система прекращает работу.  Для чего же предназначены утилиты «взлома» удаленных компьютеров?  Внимание на слайд!  **СЛАЙД 5**    **Утилиты «взлома» удаленных компьютеров** предназначены для проникновения в удаленные компьютеры с целью дальнейшего управления ими (используя методы троянских программ типа утилит удаленного администрирования) или для внедрения во «взломанную» систему других вредоносных программ.  Утилиты «взлома» удаленных компьютеров обычно используют уязвимости в операционных системах или приложениях, установленных на атакуемом компьютере.  Утилиты «взлома» удаленных компьютеров обычно используют уязвимости в операционных системах или приложениях, установленных на атакуемом компьютере.  **СЛАЙД 6**    Руткит *(от англ. root kit - «набор для получения прав root»)* - программа или набор программ для скрытного взятия под контроль «взломанной» системы.  Запишем это определение в тетрадь.  В операционной системы UNIX под термином «rootkit» понимается набор утилит, которые хакер устанавливает на «взломанном» им компьютере после получения первоначального доступа.  В операционной системе Windows под rootkit принято подразумевать программу, которая внедряется в систему и перехватывает системные функции.  Многие rootkit устанавливают в систему свои драйверы и службы (они также являются «невидимыми»).  А теперь как же защитить компьютерную сеть или отдельно компьютер от хакерских атак?  **СЛАЙД 7**    Защита компьютерных сетей или отдельных компьютеров от несанкционированного доступа может осуществляться с помощью межсетевого экрана, или брандмауэра (от англ. firewall).  Межсетевой экран позволяет:   * блокировать хакерские DoS-атаки, не пропуская на защищаемый компьютер сетевые пакеты с определенных серверов (определенных IP-адресов или доменных имен); * не допускать проникновение на защищаемый компьютер сетевых червей (почтовых, Web и др.); * препятствовать троянским программам отправлять конфиденциальную информацию о пользователе и компьютере.   Межсетевой экран может быть реализован как аппаратно, так и программно.  А теперь мы с вами будем учиться обнаруживать и обезвреживать руткиты и защищать компьютер от хакерских атак.  *(Карточки -ПРИЛОЖЕНИЕ 1).*  **Задание 1.** В операционной системе Windows обнаружить и обезвредить руткиты.  **Задание 2.** В операционной системе Windows включить брандмауэр Windows (межсетевой экран), который предотвращает попытки доступа хакеров или вредоносных программ к локальному компьютеру через локальную сеть или Интернет. | Обратить внимание на слайд.  Записывают определение в тетрадь.  Слушают.  Обратить внимание на слайд.  Записать определениея в тетрадь.  Обратить внимание на слайд.  Записать определение, изучить  Обратить внимание на слайд,  Изучить.  Обращают внимание на слайд.  Слушают.  Записывают определение в тетрадь.  Слушают.  Обращают внимание на слайд.  Слушают.  Получают задание.  Изучают и выполняют  . |
| 1. ***Подведение итогов урока.*** | |
| **Цель:** провести анализ урока и дать оценку успешности достижения цели. | |
| Наш урок подходит к концу. Завершайте выполнение заданий.  Отправить карточки с заданиями адрес группы.  . | Результаты будут оценены по представленным  Каточкам с решениями в адрес преподавателя |
| 1. ***Информация о домашнем задании.*** | |
| **Цель:** обеспечить понимание и принятие цели, содержания и способов выполнения домашнего задания. | |
| Запишите домашнее задание. В учебнике на стр.75-76, а также учить обозначенную тему по угриновичу.  До свидания. Желаю вам успехов. | Делают соответствующие записи по домашнему заданию |

ПРИЛОЖЕНИЕ 1.

**ПРАКТИЧЕСКАЯ РАБОТА**

**ЗАЩИТА ОТ ХАКЕРСКИХ АТАК**

****

