**ГБПОУ РО «РИПТ»**

**КОНСПЕКТ**

**урока по дисциплине**

**Информатика**

**группа № \_16\_\_**

**ПО ТЕМЕ:**

**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**

**15.11.2021**



**Тема урока: Информационная безопасность**

**Цель:** формирование представления об информационной безопасности.

**Задачи:**

**обучающие:**

- познакомить с понятием информационной безопасности

- рассмотреть различные угрозы информационной безопасности

**развивающие:**

**-**совершенствовать коммуникативные навыки через умение излагать мысли, умение вести диалог

- определить план действий для предотвращения угрозы информационной безопасности

**воспитывающие:**

- воспитывать ответственность за свои действия

**Оборудование и методические материалы:**Мультимедийный проектор + ПК

**Ход урока:**

**Теоретическая часть. Изучение нового материала**

Каковы основные цели и задачи информационной безопасности, что такое информационные угрозы и как они проявляются, что является источником информационных угроз, какие существуют методы защиты информации от информационных угроз. Наиболее актуальным в современном обществе считается вопрос о безопасности в сети Интернет. Все мы или большинство в той или иной мере пользуемся всемирной сетью. Тема урока «Информационная безопасность».

**Информационная безопасность.**

Многие черты информационного общества уже присутствуют в современной жизни развитых стран. Компьютеры контролируют работу атомных реакторов, распределяют электроэнергию, управляют самолётами и космическими кораблями, определяют надёжность систем обороны страны и банковских систем, т.е. используются в областях общественной жизни, обеспечивающих благополучие и даже жизнь множества людей.

Жизненно важной для общества становится проблема информационной безопасности действующих систем хранения, передачи и обработки информации.

**Информационная безопасность – совокупность мер по защите информационной среды общества и человека.**

О важности этой проблемы свидетельствуют многочисленные факты. Более 80% компьютерных преступлений осуществляется через глобальную сеть Интернет, которая обеспечивает широкие возможности злоумышленникам для нарушений в глобальном масштабе.

Какие воздействия могут нанести ущерб информации или владельцу, то есть что представляет угрозу информационной безопасности?

Некоторые виды компьютерных преступлений, когда компьютер является инструментом для совершения преступления, а объектом преступления является информация:

* Вирусы, черви, трояны
* Хакеры
* Спам
* Мошенничество
* Несоблюдение закона об авторском праве, нелицензионное ПО
* Кража личных данных, утечка информации
* Дезинформация

1. Несанкционированный (неправомерный) доступ к информации. Лицо получает доступ к секретной информации, например, путём подбора шифра (пароля).

Хакерами и взломщиками называют людей, которые взламывают защиту систем данных. Они могут вторгнуться на незащищенный компьютер через Интернет и воспользоваться им со злым умыслом, а также украсть или скопировать файлы и использовать их в противозаконной деятельности.

2. Нарушение работоспособности компьютерной системы. В результате преднамеренных действий ресурсы вычислительной системы становятся недоступными, или снижается её работоспособностью. Примером такого рода преступлений является создание и распространение компьютерных вирусов.

Вирус - это программа, которая может проникнуть в компьютер различными путями и вызвать эффекты, начиная от просто раздражающих восприятие до очень разрушительных. Вирусы могут проникать в компьютеры через электронную почту, Интернет, различные виды дисков и т.д., и имеют следующие характеристики:

* они способны размножаться, заражая другие файлы и программы.
* когда они активны, то способны выполнять раздражающие или разрушительные действия на Вашем компьютере.

3. Подделка (искажение или изменение), т.е. нарушение целостности компьютерной информации. Эта деятельность является разновидностью неправомерного доступа к информации. К подобного рода действиям можно отнести подтасовку результатов голосования на выборах, референдумах и т.д. путем внесения изменений в итоговые протоколы.

**Меры обеспечения информационной безопасности.**

Эти меры применяются в основном на этапе эксплуатации информационной системы.

Разработчики системы, предназначенной для обработки важной информации, должны предусмотреть средства защиты уже на этапе её создания. Существует даже специальный термин «защищенная система» - это информационная система, обеспечивающая безопасность обрабатываемой информации и поддерживающая свою работоспособность в условиях воздействия на неё заданного множества угроз (нарушение целостности информации, несанкционированный доступ, попытки нарушения работоспособности).

Средства защиты современных ИС должны учитывать современные формы представления информации (гипертекст, мультимедиа и т.д.). Развитие локальных сетей Internet диктует необходимость эффективной защиты при удаленном доступе к информации. Необходимо осуществлять защиту от автоматических средств нападения: компьютерных вирусов, автоматизированных средств взлома.

Наряду с программно-техническими средствами защиты информации действуют правовые, юридические меры защиты. Перейдите по ссылке познакомьтесь с мерами обеспечения информационной безопасности.

К защите информации также относится и осуществление авторских и имущественных прав на интеллектуальную собственность, каковым является программное обеспечение.

Задачи информационной безопасности сводятся к минимизации ущерба, а также к прогнозированию и предотвращению таких воздействий. Давайте разделимся на группы и установим, какие действия нужно предпринять, чтобы обезопасить себя от таких воздействий.

***Кража личных данных, утечка информации***

* старайтесь не "светить" номер кредитки в Сети;
* совершая онлайновую покупку, обращайте внимание на защищенность канала передачи данных;
* отслеживайте файлы cookies на жестком диске, регулярно проверяйте их принадлежность и удаляйте подозрительные.

***Вирусы, черви, трояны.***

* приобретите хороший антивирусный пакет, установите его в режиме максимальной безопасности, и своевременно обновляйте;

***Спам.***

* не сообщайте посторонним ваш адрес электронной почты, особенно тот, который предоставлен провайдером или особенно важен для вас;
* пользуйтесь почтовыми серверами с установленными фильтрами.

***Хакеры.***

* никогда не храните пароли на винчестере (даже в зашифрованном виде), не ленитесь каждый раз набирать их вручную;
* отсоединяйтесь от Internet при подозрении на хакерскую атаку, запускайте антивирусную программу, изменяйте пароли;
* старайтесь меньше пользоваться общедоступными программами сомнительного происхождения;
* просматривайте чаще системный реестр на предмет подозрительных записей;
* обязательно делайте резервные копии данных на дискеты или CD R/RW;

***Авторское право, нелицензионное ПО***

* укрепление законодательной базы;
* пресекайте попытки воровства вашего творчества;
* используйте только лицензионное ПО.

***Мошенничество (денежное надувательство).***

* просто будьте более скептичными и менее доверчивыми.

***Дезинформация.***

* разумный скептицизм плюс ее проверка в других средствах массовой информации.

Рассмотрим, как можно защитить информацию из своего файла от посторонних глаз, защитить файл от изменений.

***Создание текстового файла, который требует пароль при открытии***

1. Необходимо нажать в строке меню *Сервис / Параметры*
2. Появится окно *Параметры*, выбрать вкладку *Безопасность*
3. В поле *Пароль* для открытия файла ввести пароль, нажать *Ок*
4. Появится окно о подтверждении
5. Внимание !!! Не забудьте свой пароль!

***Создание текстового файла, который не позволяет вносить изменения***

1. Необходимо нажать в строке меню *Сервис / Защитить документ*
2. Появится справой стороны панель *Защита документа*
3. В поле *Ограничение на редактирование* поставить галочку и указать вариант *Только чтение*
4. Нажать кнопку *Да, включить защиту*

**Домашнее задание**

- Сделать конспект в тетради.

- Ответить на контрольные вопросы:

1. ***Что такое "информационная безопасность"?***
2. ***Какие воздействия могут нанести ущерб информации или владельцу, то есть что представляет угрозу информационной безопасности?***
3. ***Перечислить виды компьютерных преступлений***
4. ***Дать определение «защищенная система».***
5. ***Задачи информационной безопасности.***

**Ответы на контрольные вопросы на отдельном листе и сдать для оценивания (подписать Ф.И.О. , № гр., дата).**

**Литература**

1. Цветкова М.С., Хлобыстова Н.Ю. «Информатика»: учебник. – М. «Академия», 2017.
2. Цветкова М.С., Хлобыстова Н.Ю. «Информатика»: практикум. – М. «Академия», 2017.
3. Электронная библиотека Book.ru: Угринович Н.Д. Информатика (для СПО), КноРус, 2018; Угринович Н.Д. Информатика. Практикум (для СПО), КноРус, 2018

**Желаю удачи!**