Практическая работа №15.

Профилактические и антивирусные мероприятия для компьютерного рабочего места в соответствии с его комплектацией для профессиональнойдеятельности.

Тема: *Защита информации, антивирусная защита, безопасность в сети*

Цель:

- выработать навыки работы с антивирусными программами,
- выработать правила безопасной работы в сети

Оборудование: инструкционная карта, ПК с выходом в интернет

Ход работы:

Информационная безопасность

Информационная безопасность государства – состояние сохранностиинформационных ресурсов государства и защищённости законных
прав личности и общества в информационной сфере.

Информационная безопасность - это процесс обеспечения конфиденциальности, целостности и доступности информации.

- Конфиденциальность: Обеспечение доступа к информации толькоавторизованным пользователям.
- Целостность: Обеспечение достоверности и полноты информации иметодов ее обработки.
- Доступность: Обеспечение доступа к информации и связанным с нейактивам авторизованных пользователей по мере необходимости.

Информационная безопасность – все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности,неотказуемости, подотчётности, аутентичности и достоверности информации или средств её обработки.

Безопасность информации (данных) – состояние защищённости информации(данных), при котором обеспечиваются её (их) конфиденциальность,
доступность и целостность.

Безопасность информации (данных) определяется отсутствием недопустимогориска, связанного с утечкой информации по техническим каналам,
несанкционированными и непреднамеренными воздействиями на данные и (или) на другие ресурсы автоматизированной информационной системы,используемые в автоматизированной системе.

Вирусы. Антивирусное программное обеспечение

Компьютерный вирус - программа способная самопроизвольно внедряться ивнедрять свои копии в другие программы, файлы, системные области
компьютера и в вычислительные сети, с целью создания всевозможных помехработе на компьютере.

Признаки заражения:

- прекращение работы или неправильная работа ранее функционировавшихпрограмм
- медленная работа компьютера
- невозможность загрузки ОС
- исчезновение файлов и каталогов или искажение их содержимого
- изменение размеров файлов и их времени модификации
- уменьшение размера оперативной памяти
- непредусмотренные сообщения, изображения и звуковые сигналы
- частые сбои и зависания компьютера и др.

Классификация компьютерных вирусов

По среде обитания:

- *Сетевые* – распространяются по различным компьютерным сетям
- *Файловые* – внедряются в исполняемые модули (COM, EXE)
- *Загрузочные* – внедряются в загрузочные сектора диска или сектора,содержащие программу загрузки диска
- *Файлово-загрузочные* – внедряются и в загрузочные сектора и в исполняемыемодули

По способу заражения:

- *Резидентные* – при заражении оставляет в оперативной памяти компьютерасвою резидентную часть, которая потом перехватывает обращения ОС к объектам заражения
- *Нерезидентные* – не заражают оперативную память и активны ограниченноевремя

По воздействию:

- *Неопасные* – не мешают работе компьютера, но уменьшают объем свободнойоперативной памяти и памяти на дисках
- Опасные – приводят к различным нарушениям в работе компьютера
- Очень опасные – могут приводить к потере программ, данных, стираниюинформации в системных областях дисков

По особенностям алгоритма:

- *Паразиты* – изменяют содержимое файлов и секторов, легко обнаруживаются
- *Черви* – вычисляют адреса сетевых компьютеров и отправляют по ним своикопии
- *Стелсы* – перехватывают обращение ОС к пораженным файлам и секторам иподставляют вместо них чистые области
- *Мутанты* – содержат алгоритм шифровки-дешифровки, ни одна из копий непохожа на другую
- *Трояны* – не способны к самораспространению, но маскируясь под полезную,разрушают загрузочный сектор и файловую систему

Основные меры по защите от вирусов

- оснастите свой компьютер одной из современных антивирусных программ:Doctor Web, Norton Antivirus, AVP, Kaspersky
- постоянно обновляйте антивирусные базы
- делайте архивные копии ценной для Вас информации

Классификация антивирусного программного обеспечения

- **Сканеры (детекторы)**. Принцип работы антивирусных сканеров основан напроверке файлов, секторов и системной памяти и поиске в них известных иновых (неизвестных сканеру) вирусов.
- **Мониторы**. Это целый класс антивирусов, которые постоянно находятся в оперативной памяти компьютера и отслеживают все подозрительные действия, выполняемые другими программами. С помощью монитора можно остановить распостранение вируса на самой ранней стадии.
- **Ревизоры**. Программы-ревизоры первоначально запоминают в специальных файлах образы главной загрузочной записи, загрузочных секторов логическихдисков, информацию о структуре каталогов, иногда - объем установленной оперативной памяти. Программы-ревизоры первоначально запоминают в специальных файлах образы главной загрузочной записи, загрузочных секторов логических дисков, информацию о структуре каталогов, иногда - объем установленной оперативной памяти. Для определения наличия вирусав системе программы-ревизоры проверяют созданные ими образы и производят сравнение с текущим состоянием.

Виды финансового мошенничества в интернете

1. **Социальная инженерия** – это искусство обмана, при котором мошенники используют психологические методы, чтобы убедить жертву довериться им. Они могут выдавать себя за друзей, коллег или службу поддержки, просив доступ к личной информации или паролям.
2. **Фишинг**– вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Это достигается путём проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей. В письме часто содержится прямая ссылка на сайт, внешне неотличимый от настоящего, либо на сайт с редиректом. После того как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приёмами побудить пользователя ввести на поддельной странице свои логин и пароль, которые он использует для доступа к определённому сайту, что позволяет мошенникам получить доступ к аккаунтам и банковским счетам.
3. **Смишинг** – это вид фишинга, где мошенничество происходит через SMS. Злоумышленники отправляют сообщения, маскируясь под авторитетные организации, и используют угрозы или привлекательные предложения, чтобы подтолкнуть жертву к нажатию на вредоносную ссылку. Эта ссылка ведет на поддельный сайт, где от пользователя требуется ввести конфиденциальные данные. Лучший способ защиты – это проверка информации и избегание кликов по ссылкам в SMS от неизвестных номеров.
4. **Вишинг** – это когда мошенники звонят жертвам, выдавая себя за банк или другую организацию, и пытаются получить конфиденциальные данные. Они могут утверждать, что ваш счет был взломан или требуется верификация данных.
5. **Сообщения о чрезвычайных ситуациях** - мошенники отправляют сообщения о якобы чрезвычайных ситуациях, утверждая, что ваш близкий попал в беду и срочно нуждается в финансовой помощи. Обычно просится перевести деньги на указанный счет или номер телефона.

Кибербуллинг или травля в интернете

Кибербуллинг – это намеренное запугивание или травля человека в интернете. Часто травля из онлайн-пространства переходит в реальную жизнь. И если взрослые могут самостоятельно справиться с кибербуллингом, то дети и подростки – нет. Они просто не знают как быть и что делать. В конечном итоге систематические оскорбления в интернете могут привети к печальным последствиям.

Существует несколько форм кибербуллинга, которые могут применяться в отношении жертвы. Все они оказывают равносильное воздействие на человека и могут приводить к трагическим последствиям.

1. **Буллинг.** Под буллингом понимают систематическое насилие одного человека или группы людей над жертвой. В сети он может выражаться в виде отправки сообщений с оскорбительными прозвищами и угрозами, взлома личных страниц в соцсетях и распространения лживых слухов. Чаще всего практикуется такой кибербуллинг в школах.
2. **Троллинг.** При таком кибербуллинге целью становится банальная провокация. Жертву пытаются намеренно вывести из себя, отправляя разные сообщения с неприятным содержанием. Как правило, задиры делают это исключительно для получения собственного удовольствия.
3. **Моббинг.** Главной особенностью кибербуллинга такой формы становится его массовость – над жертвой систематически издеваются сразу несколько человек. Они могут отправлять сообщения с насмешками, указывать на недостатки внешности или просто вести себя враждебно. Такие действия обычно направлены на то, чтобы заставить человека уйти из коллектива.
4. **Флейм.** Главную роль в таком кибербуллинге играют сообщения в формате словесной войны. Жертву оскорбляют и провоцируют, чтобы развивать конфликт еще сильнее даже в том случае, если он уже исчерпан.
5. **Аутинг.** Публикация личных данных человека на всеобщее обозрение без его разрешения. Аутинг очень опасен, потому что агрессоры могут опубликовать как незначительную личную информацию (например, номер телефона жертвы), на разглашение которой можно не обращать внимание, так и сугубо индивидуальные факты из жизни жертвы (его переписки, обнаженные фотографии и проч.).

6. **Фрейпинг.** Форма кибербуллинга, при которой агрессор получает доступ к какому-либо сетевому аккаунту жертвы. От чужого имени он может вести дискуссии, оскорблять кого-либо, публиковать материалы различного характера. Фрейпинг может иметь крайне негативные последствия.
7. **Кибersталкинг.** Чрезвычайно опасная форма кибербуллинга, требующая немедленного вмешательства со стороны взрослых людей. Она может привести к тому, что виртуальный агрессор может стать «реальным», т. е. угрожать жизни вашего ребенка. Жертву могут выслеживать для нападения, избиения, насилия и проч.
8. **Кетфишинг.** От данной разновидности кибербуллинга страдают все знаменитые люди планеты — это намеренное создание подделанной страницы в социальных сетях. Киберагрессоры копируют профиль жертвы, пытаются каким-либо образом ее скомпрометировать.
9. **Хеппислепинг.** Сравнительно недавно появившаяся форма кибербуллинга, характеризующаяся снятием видеороликов, на которых агрессоры избивают жертву или издеваются над ней, а затем «заливают» ролики в Интернет, разумеется, без согласия пострадавшего человека.

Ход работы:

Задание 1. Ответьте на вопросы теста *(вопрос переписать)* **.**

Тест по теме «Защита информации, антивирусная защита»

1. **Информационная безопасность – это …**

1) отсутствие зараженных файлов на компьютере
2) процесс работы антивирусных программ
3) процесс обеспечения конфиденциальности, целостности и доступностиинформации
4) состояние защищённости информации, при котором обеспечиваются её (их) конфиденциальность, доступность и целостность.

2. **Основные угрозы доступности информации:**

1) непреднамеренные ошибки пользователей
2) злонамеренное изменение данных
3) перехват данных
4) хакерская атака.

3. **Один из методов защиты информации на компьютере**

1) полное отключение системного блока
2) отключение жесткого диска
3) защита паролем
4) шифрование информации.

4. **К биометрической системе защиты относятся:**

1) антивирусная защита
2) защита паролем
3) идентификация по отпечаткам пальцев
4) физическая защита данных

5. **Брандмауэр (firewall) – это программа, …**

1) которая следит за сетевыми соединениями и принимает решение о разрешениии или запрещении новых соединений на основании заданного набора правил
2) которая следит за сетевыми соединениями, регистрирует и записывает вотдельный файл подробную статистику сетевой активности
3) на основе которой строится система кэширования загружаемых веб-страниц

4) реализующая простейший антивирус для скриптов и прочих использующихсяв Интернет активных элементов.

6. Положительные моменты в использовании для выхода в Интернет браузера, отличного от Microsoft Internet Explorer, но аналогичного пофункциональности

1) уменьшение вероятности заражения, поскольку использование иного браузера может косвенно свидетельствовать об отсутствии у пользователя достаточныхсредств для покупки Microsoft Internet Explorer
2) уменьшение вероятности заражения, поскольку большинство вредоносных программ пишутся в расчете на самый популярный браузер, коим являетсяMicrosoft Internet Explorer
3) возможность установить отличную от www.msn.com стартовую страницу
4) возможность одновременно работать в нескольких окнах.

7. Что такое "компьютерный вирус"?

1) самостоятельная компьютерная программа или компонент программногокомплекса, предназначенная для создания и изменения текстовых файлов.
2) это совокупность программ, находящиеся на устройствах долговременнойпамяти;
3) это программы, которые могут "размножаться" и скрытно внедрять своикопии в файлы, загрузочные секторы дисков и документы;
4) это сведения об объектах и явлениях окружающей среды, их параметрах,свойствах и состоянии.

8. Назовите основные типы компьютерных вирусов:

1) почтовые, программные
2) аппаратные, программные, загрузочные
3) файловые, макровирусы, загрузочные.

9. Свойство вируса, позволяющее называться ему загрузочным –способность …

1) заражать загрузочные сектора жестких дисков
2) заражать загрузочные дискеты и компакт-диски
3) вызывать перезагрузку компьютера-жертвы
4) подсвечивать кнопку Пуск на системном блоке.

10. Программа, осуществляющая несанкционированные действия по сбору,и передаче информации злоумышленнику, а также ее разрушение или злонамеренную модификацию это:

1) Макровирус
2) Сетевой червь
3) Троян
4) Загрузочный вирус

11. Заражение компьютерными вирусами может произойти в процессе ...

1) работы с файлами
2) форматирования дискеты
3) выключения компьютера
4) печати на принтере

12. Какие файлы заражают макро-вирусы?

1) исполнительные;
2) файлы документов Word и элект. таблиц Excel;
3) графические и звуковые;
4) html документы.

13. К каким вирусам относится "троянский конь"?

1) макро-вирусы
2) скрипт-вирусы
3) интернет-черви
4) загрузочные вирусы.

14. Неопасные компьютерные вирусы могут привести

1) к сбоям и зависаниям при работе компьютера;
2) к потере программ и данных;
3) к форматированию винчестера;
4) к уменьшению свободной памяти компьютера.

15. Опасные компьютерные вирусы могут привести…

1) к сбоям и зависаниям при работе компьютера;
2) к потере программ и данных;
3) к форматированию винчестера;
4) к уменьшению свободной памяти компьютера.

16. Какой вид компьютерных вирусов внедряются и поражают исполнительный файлы с расширением *.exe, *.com и активируются приих запуске?

1) файловые вирусы;
2) загрузочные вирусы;
3) макро-вирусы;
4) сетевые вирусы

17. Какой вид компьютерных вирусов внедряются и поражают файлы срасширением *.txt, *.doc?

1) файловые вирусы;
2) загрузочные вирусы;
3) макро-вирусы;
4) сетевые вирусы.

18. Как происходит заражение почтовыми вирусами?

1) При подключении к web-серверу, зараженному "почтовым" вирусом
2) При открытии зараженного файла, присланного с письмом по e-mail
3) При подключении к почтовому серверу
4) При получении с письма, присланном по e-mail, зараженного файла.

19. Сетевые черви это:

1) Вирусы, которые внедряются в документ под видом макросов
2) Вирусы, которые проникну на компьютер, блокируют работу сети

3) Вредоносные программы, которые проникают на компьютер, используясервисы компьютерных сетей

4) Вредоносные программы, устанавливающие скрытно от пользователя другиепрограммы.

20. Руткит – это:

1) Программа для скрытого взятия под контроль взломанной системы

2) Вредоносная программа, маскирующаяся под макрокоманду

3) Разновидность межсетевого экрана

4) Программа, выполняющая несанкционированные действия по передачеуправления компьютером удаленному пользователю.

21. Какие существуют вспомогательные средства защиты?

1) Аппаратные средства.

2) Программные средства.

3) Аппаратные средства и антивирусные программы.

22. Антивирусные программы - это программы для:

1) Обнаружения вирусов

2) Удаления вирусов

3) Размножения вирусов

23. На чем основано действие антивирусной программы?

1) На ожидании начала вирусной атаки.

2) На сравнении программных кодов с известными вирусами.

3) На удалении зараженных файлов.

24. Какие программы относятся к антивирусным?

1) AVP, MS-DOS, MS Word

2) AVG, DrWeb, Norton AntiVirus

3) Norton Commander, MS Word, MS Excel.

25. Какие программы не относятся к антивирусным?

1) программы-фаги

2) программы сканирования

3) программы-ревизоры

4) программы-детекторы

26. Можно ли обновить антивирусные базы на компьютере, неподключенном к Интернет?

1) да, позвонив в службу технической поддержки компании-производителя антивирусной программы. Специалисты этой службы продиктуют последниебазы, которые нужно сохранить на компьютере воспользовавшись любым текстовым редактором

2) да, это можно сделать с помощью мобильных носителей скопировав антивирусные базы с другого компьютера, на котором настроен выход в Интернет и установлена эта же антивирусная программа или на нем нужновручную скопировать базы с сайта компании-производителя антивирусноййпрограммы

3) нет.

27. Основные меры по защите информации от повреждения вирусами:

1) проверка дисков на вирус
2) создавать архивные копии ценной информации
3) не пользоваться "пиратскими" сборниками программного обеспечения
4) передавать файлы только по сети.

28. Наиболее эффективное средство для защиты от сетевых атак

1) использование антивирусных программ
2) использование сетевых экранов или «firewall»
3) посещение только «надёжных» Интернет-узлов
4) использование только сертифицированных программ-браузеров при доступе ксети Интернет.

29. Основная функция межсетевого экрана

1) управление удаленным пользователем
2) фильтрация входящего и исходящего трафика
3) проверка дисков на вирусы
4) программа для просмотра файлов.

30. Создание компьютерных вирусов является

1) последствием сбоев операционной системы
2) необходимым компонентом подготовки программистов
3) побочным эффектом при разработке программного обеспечения
4) преступлением.

Задание 2. Заполнить таблицу.

Описать 5 антивирусных программ.

Наименование антивирусной программы	**Характеристики**	**Условия использования (платно/бесплатно)**
…	**…**	**…**

Задание 3. Ответьте на вопросы теста (*вопрос переписать****).***

1. В интернете вы увидели новость, что по новому закону каждый гражданин России может получить от государства компенсацию. На специальном сайте нужно ввести номер СНИЛС, чтобы узнать, какая сумма положена именно вам. Ваши действия?

А) Не уверен, что мне положена компенсация. Но почему бы и не попробовать?
Б) Не вижу причин сомневаться! Комментарии от людей, которые уже получили деньги, доказывают, что все безопасно
С) Подозрительно, конечно. Сначала поищу, что за закон такой.

2. Вам звонят из банка и сообщают, что обновляется база клиентов и необходимо подтвердить свои паспортные данные и информацию о карте. Как поступите?

А) Ничего сообщать о себе не буду. По-моему, это аферисты. Сотрудники банков никогда не запрашивают личные и финансовые данные
Б) Это банк – я узнал его номер. Назову все данные, а то вдруг карту заблокируют

3. Вам на почту приходит письмо с электронного адреса известного интернет-магазина с просьбой пройти по ссылке и подтвердить свой аккаунт (вести свои данные и реквизиты карты, включая трехзначный код с обратной стороны карты) для участия в закрытой распродаже. Что делать?

А) Конечно, пройду по ссылке. Я давно жду закрытую распродажу
Б) Сомнительно, конечно, но все же попробую. Данные введу, но на всякий случай сниму все деньги с карты
С) По ссылке заходить не буду. Лучше открою сайт из закладок и проверю сам

4.Какой из этих паролей кажется вам наиболее надежным для онлайн-банка?

А) Дата моего рождения. Такой точно не забудешь
Б) Upgswwk391$
С) qwerty123
D) Солнышко

5. **Вы ждали «черной пятницы», чтобы купить бытовую технику с хорошей скидкой. Нашли интернет-магазин с большим ассортиментом. Однако товары на сайте стоят гораздо дешевле, чем у других продавцов. Что будете делать?**

А) Куплю то, что планировал. Сохраню чек об оплате, чтобы подстраховаться
Б) Если отзывы положительные, тогда и думать нечего. Надо брать, как говорилось в одном фильме
С) Не буду рисковать. А вдруг этот магазин вообще не существует? Ищи потом, кому отправил деньги.

Задание 3. Ответьте на вопросы

1) Где чаще всего происходит Кибербуллинг?
2) Какие есть виды Кибербуллинга? *(опишите 2-3 вида*).
3) Как защитить себя от Кибербуллинга?

Вывод: