Практическая работа № 52

Тема: Средства защиты информации и персональных данных медицинских кадров.

Цель: изучение возможностей защиты информации и персональных данных.

Теоретическая часть.

1. Вредоносное программное обеспечение (ПО)

Вредоносное ПО (malware – сокращение от malicious software) – это различные программы, которые могут наносить вред. Вредоносное ПО – это любая нежелательная программа, которая устанавливается на компьютере без вашего ведома. Вирусы, черви и троянские кони – это примеры вредоносных программ, которые часто совокупно называются вредоносным ПО.

Имеется несколько методов для защиты компьютера от вредоносного ПО:

- убедитесь, что автоматическое обновление операционной системы включено, чтобы получать все последние обновления безопасности;
- включите брандмауэр;
- включите антивирус;
- не открывайте спам-сообщения электронной почты и не переходите по ссылкам на подозрительные веб-сайты;
- постоянно работать на персональном компьютере исключительно под правами пользователя, а не администратора, что не позволит большинству вредоносных программ инсталлироваться на персональном компьютере;
- отключить автозапуск со сменных носителей, что не позволит запускаться кодам, которые находятся на нем без ведома пользователя.

Киберпреступники иногда пытаются побудить вас загрузить мошеннические (ложные) программы безопасности, которые, как они заявляют, защитят вас от вредоносного ПО. Такие мошеннические программы безопасности могут требовать оплаты за фальшивый продукт, устанавливать вредоносное ПО на компьютер или похищать вашу личную информацию.

2. Шпионское программное обеспечение

Шпионское программное обеспечение (spyware, программа-шпион) — программа, которая скрытным образом устанавливается на компьютер с целью сбора информации о конфигурации компьютера, пользователе, пользовательской активности без согласия последнего. Также может производить другие действия: изменение настроек, установка программ без ведома пользователя, перенаправление действий пользователя.

Spyware могут осуществлять широкий круг задач, например:

- собирать информацию о привычках пользования Интернетом и наиболее часто посещаемые сайты (программа отслеживания);
- запоминать нажатия клавиш на клавиатуре (кейлоггеры) и записывать скриншоты экрана и в дальнейшем отправлять информацию создателю spyware;
- несанкционированно и удалённо управлять компьютером;
- инсталлировать на компьютер пользователя дополнительные программы;

- использоваться для несанкционированного анализа состояния систем безопасности — сканеры портов и уязвимостей и взломщики паролей;
- изменять параметры операционной системы — руткиты, перехватчики управления и пр. — результатом чего является снижение скорости соединения с Интернетом или потеря соединения как такового, открывание других домашних страниц или удаление тех или иных программ;
- перенаправлять активность браузеров, что влечёт за собой посещение веб-сайтов вслепую с риском заражения вирусами.

Меры по предотвращению заражения

- Использование браузеров, отличных от Internet Explorer — Opera, Mozilla Firefox и др. Хотя нет совершенно безопасного браузера, Internet Explorer представляет больший риск по части заражения из-за своей обширной пользовательской базы.
- Использование файрволов и прокси-серверы для блокировки доступа к сайтам, известным как распространители spyware.
- Скачивание программ только из доверенных источников (предпочтительно с веб-сайтов производителя), поскольку некоторые spyware могут встраиваться в дистрибутивыпрограмм.
- Использование антивирусных программ с максимально «свежими» вирусными базами.

3. Спам

Спам (spam) — рассылка коммерческой и иной рекламы или иных видов сообщений лицам, не выражавшим желания их получать.

Примечание. Можно дать предварительно задание одному учеников подготовить краткое сообщение о происхождении термина «спам» и о том, как он пришел в электронный мир.

Самый надёжный способ борьбы со спамом — не позволить спамерам узнать электронный адрес. Это трудная задача, но некоторые меры предосторожности можно предпринять.

- Не следует публиковать свой адрес на общедоступных сайтах.
- Если по каким-то причинам адрес электронной почты приходится публиковать, его можно закодировать наподобие «v_a_s_y_a_@_m_a_i_l_._r_u». Спамеры используют специальные программы для сканирования сайтов и сбора почтовых адресов, поэтому даже такая маскировка адреса может помочь. Следует помнить, однако, что в самых простых случаях «закодированный» адрес сможет распознать и программа. К тому же, это создает неудобства не только для спамеров, но и для обычных пользователей.
- Большинство публичных сайтов не публикует адреса электронной почты зарегистрированных пользователей, но даёт возможность отправить сообщение по нику. Реальный адрес подставляется сервером из профиля пользователя, и другим пользователям невидим.
- Адрес можно представить в виде картинки. Существуют онлайн-службы, делающие это автоматически (однако, не следует забывать, что некоторые

из этих служб могут сами собирать и продавать введенные пользователями почтовые адреса). Кроме того, это можно сделать в любом графическом редакторе или просто написать электронный адрес от руки и сфотографировать.

- Можно завести специальный ящик для регистрации в службах, не вызывающих особого доверия, и не использовать его для обычной жизни. Существуют даже службы, выдающие одноразовые адреса электронной почты специально для того, чтобы указывать их в сомнительных случаях. Самая известная из них — mailinator.com.
- Никогда не следует отвечать на спам или переходить по содержащимся в нём ссылкам, в том числе и по ссылкам, предназначенным якобы для отписки от рассылки. Такое действие подтвердит, что электронный адрес реально существует, активно используется, а его получатель читает спам, и приведёт к увеличению количества спама.
- Факт загрузки картинок, включенных в письмо, при прочтении, может использоваться для проверки активности почтового адреса. Поэтому рекомендуется при запросе почтового клиента о разрешении загрузки картинки запрещать действие, если вы не уверены в отправителе.
- Можно время от времени менять свой адрес, но это связано с очевидными трудностями: нужно сообщить новый адрес людям, от которых хотелось бы получать почту.

4. Недостоверная информация

Информация достоверна, если она отражает истинное положение дел. Объективная информация всегда достоверна, но достоверная информация может быть как объективной, так и субъективной. Достоверная информация помогает принять нам правильное решение. Недостоверной информация может быть по следующим причинам:

- преднамеренное искажение (дезинформация) или непреднамеренное искажение субъективного свойства;
- искажение в результате воздействия помех («испорченный телефон») и недостаточно точных средств ее фиксации.

Основной способ различения недостоверной информации — критическое мышление. Прежде чем довериться той или иной информацию, нужно ее проверить, сличить с рядом источников и в результате сделать адекватный вывод о достоверности и возможности практического использования.

5. Интернет-мошенничества (фишинг)

Фишинг (fishing — рыбная ловля, выуживание) — 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.

Фишинг — одна из разновидностей социальной инженерии, основанная на незнании пользователями основ сетевой безопасности: в частности, многие не знают простого факта: сервисы не рассылают писем с просьбами сообщить свои учётные данные, пароль и прочее.

Для защиты от фишинга производители основных интернет-браузеров договорились о применении одинаковых способов информирования пользователей о том, что они открыли подозрительный сайт, который может принадлежать мошенникам. Современные версии браузеров обладают такой возможностью, которая соответственно именуется «антифишинг».

6. Оскорбления и унижения (буллинг)

Кибер-буллинг — это нападения с целью нанесения психологического вреда, которые осуществляются через электронную почту, сервисы мгновенных сообщений, в чатах, социальных сетях, на web-сайтах, а также посредством мобильной связи. Такое многократно повторяемое агрессивное поведение имеет целью навредить человеку и базируется на дисбалансе власти (физической силы, социального статуса в группе).

Рекомендации по противодействию кибер-буллингу

- Не нужно спешить выбрасывать свой негатив в кибер-пространство. Прежде чем писать и отправлять сообщения, следует успокоиться, утолить злость, обиду, гнев.
- Необходимо создавать собственную онлайн-репутацию, не покупаться на иллюзию анонимности. Хотя кибер-пространство и предоставляет дополнительные возможности почувствовать свободу и раскованность благодаря анонимности, существуют способы узнать, кто стоит за определенным никнеймом. И если некорректные действия в виртуальном пространстве приводят к реального вреду, все тайное становится явным. Интернет фиксирует историю, которая состоит из публичных действий участников и определяет онлайн-репутацию каждого — накопленный образ личности в глазах других участников. Запятнать эту репутацию легко, исправить — трудно.
- Необходимо хранить подтверждения фактов нападений. Если вас очень расстроило сообщение, картинка, видео и т.д., следует немедленно обратиться к родителям за советом, сохранить или распечатать страницу самостоятельно, чтобы посоветоваться со взрослыми в удобное время.
- Необходимо игнорировать единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать — часто кибер-буллинг вследствие такого поведения останавливается на начальной стадии. Опытные участники интернет-дискуссий придерживаются правила: «Лучший способ борьбы с неадекватами — игнор».
- Если стал очевидцем кибер-буллинга, правильным поведением будет: а) выступить против агрессора, дать ему понять, что его действия

оцениваются негативно, б) поддержать жертву — лично или в публичном виртуальном пространстве предоставить ей эмоциональную поддержку, в) сообщить взрослым о факте некорректного поведения в кибер-пространстве.

- Нужно блокировать агрессоров. В программах обмена мгновенными сообщениями есть возможность блокировки сообщений с определенных адресов. Пауза в общении часто отбивает у агрессора желание продолжать травлю.
- Не стоит игнорировать агрессивные сообщения, если письма неизвестного вам отправителя систематически содержат угрозы или порнографические сюжеты. В этом случае следует скопировать эти сообщения и обратиться к правоохранителям. Если оскорбительная информация размещена на сайте, следует сделать запрос к администратору для ее удаления.

7. Нежелательное знакомство (контакты с незнакомцами)

В Интернете многие люди рассказывают о себе неправду и выдают себя за других людей. Встреча с Интернет-знакомыми в реальной жизни, бывает опасной: за псевдонимом может скрываться преступник.

8. Интернет-зависимость, игровая зависимость

Интернет-зависимость – это болезнь современного поколения: дети и многие взрослые сутками проводят за компьютером, в частности, во всемирной паутине. Ученые полагают, что в скором времени Интернет-зависимость встанет в один ряд с такими пагубными пристрастиями, как наркотическая зависимость, алкоголизм, курение.

Следует помнить, что жизнь по большому счёту коротка. Поэтому время, потраченное на интернет и игры, восполнить уже невозможно. За время, проведенное вами за компьютером, ваши сверстники уйдут далеко вперед, достигнут новых успехов и результатов. Вы же останетесь далеко позади, без знаний и умений, да ещё и с подорванным здоровьем, т.к. увлечение компьютером его не прибавляет.

Эти нездоровые увлечения в конечном итоге не позволят добиться вам успехов в жизни, занять достойное место в обществе, достойную зарплату и социальный статус. Поэтому всё хорошо в меру. Интернет и игры невозбранимы, но нужно их дозировать, рационально и с пользой распределять свое время.

8 800 25 000 15 — бесплатная всероссийская служба консультирования для детей и взрослых по проблемам безопасного использования Интернета и мобильной связи.

Практическая часть.

Задание 1. Ответить на вопросы.

1. Что такое информационный риск?
2. В чем заключается задача управления информационными рисками?
3. Какие существуют методики оценки рисков и управления ими?
4. Какие формулы используются при количественной оценке информационных рисков?
5. Что такое целостность информации?

6. Какие меры можно предпринять для защиты информации?

Задание №2.

1. Для заданного объекта информатизации изучить нормативно-правовые документы, регламентирующие защиту Пдн(Персональные данные) . Проанализировать какие виды тайн могут содержаться в обрабатываемых ПДн (врачебная тайна, коммерческая тайна, тайна личной жизни граждан). Найти нормативно-правовые документы, защищающие эти виды тайн в ПДн. Оформить результаты в виде таблицы. Составить список всех персональных данных, обрабатываемых в данной организации, указать способ обработки ПДн, определить категорию Пдн.

2. По результатам выполнения пункта составить таблицу по образцу таблицы. Количество строк таблицы варьируется в зависимости от объекта.

Таблица 1 - Нормативно-правовые документы по защите ПДн объекта

Наименование документа	Вид защищаемой информации	Краткие пояснения документа
Федеральные законодательные документы		
Внутренние документы организации		

*В качестве объекта информатизации использовать образовательное учреждение в котором обучаетесь.

Задание 3. Сделать вывод о проделанной работе.