Глуховская Дарья Дмитриевна

Студентка Ставропольского колледжа связи им. Героя Советского Союза В.А. Петрова

Безопасность в сети Интернет

**Аннотация:** Одним из ключевых вопросов при работе в Интернете считается защищенность и безопасность . Необученный пользователь может перейти по подозрительной ссылке в Интернете, перейти на зараженный веб-сайт, скачать вирусный файл или потерять персональную информацию и другие данные. Текстовые данные, а также рисунки имеют все шансы быть носителями вредоносного программного кода, что существенно увеличивает угрозу заражения ПК.
Для обеспечения безопасности при работе в Интернете существуют определенные правила, соблюдение которых помогает улучшить защиту персональных данных и программного обеспечения на вашем компьютере.

**Ключевые слова**: вирусы, интернет, ссылка, файл, данные.

Интернет — всемирная система объединённых компьютерных сетей для хранения и передачи информации

Основной особенностью любой сетевой системы, в частности, Интернета является то, что ее компоненты распределены в пространстве и связь между ними физически осуществляется при помощи сетевых соединений и программно при помощи механизма сообщений. При этом все управляющие сообщения и данные, пересылаемые между объектами распределенной вычислительной системы, передаются по сетевым соединениям в виде пакетов (порций данных) обмена.

Со временем сеть становится все сложнее, в ней хранится все больше информации. На определенной ступени этой эволюции организация сталкивается с проблемами:

- защиты самой информационной системы (поскольку ущерб организации наносится в результате воздействия вирусов или атак при наличиии самой простой информационной системы);

- разграничениями и ограничениями доступа пользователей к ресурсам Интернета;

- контролем за действиями пользователей в Интернет.

В качестве модулей защищенного доступа в Интернет используются:

1) Межсетевые экраны

· для пресечения возможности обхода средств контроля

· для регламентирования объемов загружаемой информации

2) Средства контроля содержимого

· для проверки входящих и исходящих почтовых сообщений;

· для проверки данных Web-сайтов и их содержимого.

3) Антивирусные средства - для проверки mail и web-трафика на наличие вредоносного программного обеспечения.

Предлагаемое решение позволяет:

· защититься от утечки секретной и конфиденциальной информации;

· пресечь рассылки рекламных сообщений нецелевого характера;

· бороться с непроизводительным использованием сервисов Интернета;

· пресечь распространения клеветнических сообщений;

· контролировать лояльность персонала;

· повысить эффективности использования информационных технологий;

· обнаруживать в электронных письмах конфиденциальную информацию, вирусы и другие нежелательные объекты, а также реагировать на это заданным образом.

Существует такое понятие как **виртуальные грабли :**

* Вирусная атака.
* Спам и фишинг.
* Раздражающая и потенциально опасная реклама.
* Кибершпионаж.
* Продать или купить в интернете
* Браузерный эксплойт.

ВИРУСНАЯ АТАКА

 Самая распространённая интернет – угроза — это атака вирусов. Из-за неё можно потерять информацию, которую вы годами собирали на компьютере. Вирусные атаки представляет собой более изощрённый метод получения доступа к закрытой информации, так как используются специальные программы для ведения работы на компьютере, а также дальнейшего распространения (это вирусы и черви). Такие программы предназначены для поиска и передачи своему владельцу секретной информации, либо просто для нанесения вреда системе безопасности и работоспособности компьютера. Принципы действия этих программ различны. На данный момент вирусные атаки представляют серьезную угрозу в том числе и для простых пользователей.

СПАМ

 Спамом называют массовую рассылку электронной почты, обычно содержащую навязчивую рекламу, на адреса пользователей, которые не выражали желания ее получать. Спам вреден тем, что нагружает каналы связи и сетевое оборудование провайдеров, что, в свою очередь, увеличивает трафик и снижает пропускную способность передачи полезной информации. Кроме того, спам заставляет пользователя тратить свое время на обработку бесполезной информации. Совет: никогда не отвечайте на спамерское письмо, даже если очень хочется. Ваш ответ будет подтверждением того, что данный почтовый ящик существует в действительности, а подобная информация очень ценится у спамеров. В дальнейшем ваш ящик будет постоянно забит спамом.

ФИШИНГ

Фишинг – это вид мошенничества в глобальной сети Интернет с целью получения персональных данных пользователей. Такие данные злоумышленники могут получить следующим образом: пользователь получает сообщение о том, что ему необходимо обновить конфиденциальную информацию, перейдя по предложенной ссылке. Далее, щелкнув по ссылке, пользователь заходит на поддельный сайт и сам оставляет там свои персональные данные, вплоть до паролей, номера кредитной карты или банковского счета, что приводит к их краже.

КИБЕРШПИОНАЖ

Программы-шпионы проникают в компьютер вместе с подозрительным контентом, который вы скачиваете из сети. Шпионы собирают личные данные, анализируют ваши действия, составляют список часто посещаемых сайтов, просматривают поисковые запросы, а затем отправляют эту информацию поставщикам интернет-услуг. Такие программы работают в фоновом режиме и, как правило, не заметны для обычных пользователей. Вам может показаться, что шпионы безвредны, но это не так. Они способны отключить антивирус, а также передать ваши данные злоумышленникам.

БРАУЗЕРНЫЙ ЭКСПЛОЙТ

 Браузерный эксплойт – это форма вредоносного кода, которая использует уязвимость в браузере или компоненте системы, с целью изменить настройки без Вашего ведома. Вы открываете браузер, и вместо привычной домашней страницы вас ожидает сюрприз — сайт с сомнительным контентом. А при ошибке ввода данных в адресной строке автоматически происходит переадресация на неизвестный сайт. Если вам знакомы эти ситуации, то, скорее всего, вы столкнулись с браузерным эксплойтом, т.е. ваш браузер был атакован.

**Для более безопасного просмотра веб-страниц, Интернет:**

* Используйте безопасный браузер. (Браузеры Opera 28, Firefox 36 и Microsoft Internet Explorer 11 более безопасны, чем их предшественники).
* Установите и активируйте антивирусную программу и при необходимости убедитесь, что антивирусные базы обновлены вовремя. (Качество антивирусных программ часто зависит от их оплаты и частоты обновления).
* Включите брандмауэр и настройте его должным образом.
* Работать под учетной записью с ограниченными привилегиями, а не под учетной записью с правами системного администратора.
* Используйте официальную сборку ОС. (Microsoft Windows 7 более безопасна, чем предыдущие операционные системы рабочих станций Microsoft, включая Microsoft Windows XP, UNIX-подобные операционные системы (включая Linux, BSD), чем другие популярные операционные системы).
* Активируйте обновление операционной системы.

**Советы по безопасности в Интернете:**

* Не заходите на подозрительные сайты и ссылки от неизвестных лиц. Не нажимайте на всплывающие объявления.
* Используйте сложные пароли.
* Не делитесь своей информацией с посторонними.
* Для авторизации используйте экранную клавиатуру.
* Если вы используете браузер, установите специальные дополнения, такие как Adblock Plus. Если вы используете это дополнение, вы не увидите большинство дисплеев, даже вредоносных.
* Проверьте и контролируйте настройки антивируса и брандмауэра.
* Не открывайте сообщения от неизвестных отправителей и не загружайте файлы, прикрепленные к таким сообщениям.
* Не забудьте снизить уровень безопасности при использовании беспроводного подключения в общественных местах.

Список литературы:

* Филимонова, Е.В. Информационные технологии в профессиональной деятельности: учебник. — Ростов н.д.: Феникс, 2003. — — 352 с. (серия «SPO»).
* Автоматизированные информационные технологии в экономике Под ред. Г.А.Титоренко М.: Единица, 2004.
* Грошев С.В., Коцюбинский А.О., Комягин В.Б. Современное самообучение профессиональной работе на компьютере: верно. — М.: Триумф, 2005.
* Автоматизированные информационные технологии в экономике Ред.: Г.А.Титоренко Москва: Юнити, 2006.