**Тип работы:** Реферат

**Предмет:** Информатика



Введение

Большинство пользователей уверены, что компьютерная безопасность — это такое сложное для их понимания комплексное и технически трудное в реализации мероприятие по защите компьютеров от сторонних посягательств, вирусов, хакеров и т.д.

А немного разобравшись в этом вопросе, может оказаться, что наиболее сложные вещи для понимания на самом деле очень просты.

Возьмем например ситуацию, которая происходит с очень многими пользователями, а именно случайную установку ими в комплексе с полезной программой или игрой, различных ненужных надстроек для браузеров, лаунчеров, отдельных окон с рекламой. Не разобравшись в том, откуда это всё взялось у него на компьютере и как исправить ситуацию, месяцами человек терпит такое безобразие, просто привыкая к нему.

А когда обращается за помощью к знающему человеку и после этого, по его совету, простыми способами быстро и эффективно очищает компьютер, то с удивлением замечает, что браузер и устройство работают намного быстрее, не тормозят и т.д. Теперь поговорим о важных вещах, которые вы должны сделать, чтобы обезопасить свой ПК и свою работу в Интернете.

С конца 80-ых начала 90-ых годов проблемы, связанные с защитой информации, беспокоят как специалистов в области компьютерной безопасности так и многочисленных рядовых пользователей персональных компьютеров. Это связано с глубокими изменениями вносимыми компьютерной технологией в нашу жизнь. Изменился сам подход к понятию «информация». Этот термин сейчас больше используется для обозначения специального товара который можно купить, продать, обменять на что-то другое и т.д.

Цель работы состоит в изучении компьютерной безопасности.

Достижение цели предполагает решение ряда задач:

1) определить сущность компьютерной безопасности;

2) рассмотреть способы защиты компьютера;

3) охарактеризовать проблемы безопасности и надежности информации в компьютерных сетях.

Широкое распространение мощных сетевых компьютеров в сфере делового и личного использования привело к появлению целых отраслей компьютерной и сетевой безопасности. Компании нуждаются в знаниях и умениях экспертов по безопасности для проведения аудита и принятия решений, соответствующих их требованиям. А так как многие компании по своей природе динамичны, и их работники обращаются к информационным ресурсам и локально, и удалённо, необходимость в создании защищённого компьютерного окружения возрастает ещё больше.

1.Сущность компьютерной безопасности

Компьютерная безопасность — это «общее понятие, охватывающее широкую область компьютерных и информационных технологий. В областях, где компьютерные системы и сети ежедневно используются для выполнения бизнес-транзакций и обращений к жизненно-важной информации, данные составляют значимую часть всех активов» [6]. Некоторые понятия и оценки прочно вошли в повседневный деловой лексикон, например, полная стоимость владения (TCO) и качество обслуживания (QoS). Эти оценки позволяют оценить целостность данных, высокую степень доступности и другие аспекты с точки зрения затрат на планирование и управление процессами. В некоторых отраслях, например, в электронной коммерции, доступность и доверие к данным может играть решающую роль.

В действительности компьютер подвержен только нескольким рискам, если он по сети не подключен к другим компьютерам. За последнее время процент использования компьютерных сетей (особенно Интернета) значительно вырос, поэтому сегодня термин «компьютерная безопасность» используется для описания проблем, связанных с сетевым использованием компьютеров и их ресурсов.

Основными техническими составляющими компьютерной безопасности являются:

— конфиденциальность;

— целостность;

— аутентификация;

— доступность.

Для понимания сущности компьютерной безопасности необходимо дать определение всем вышеперечисленным её компонентам:

1. Конфиденциальность, также известная как секретность, означает, что у неавторизированных пользователей не будет доступа к вашей информации. Последствия, которые могут быть вызваны пробелами в конфиденциальности, могут варьироваться от незначительных до разрушительных.

2. Целостность означает, что ваша информация защищена от неавторизированных изменений, что не относится к авторизированным пользователям. Угрозу целостности баз данных и ресурсов, как правило, представляет хакерство.

3.Аутентификация — это сервис контроля доступа, осуществляющий проверку регистрационной информации пользователя. Другими словами это означает, что пользователь — это есть на самом деле тот, за кого он себя выдаёт.

4. Доступность означает то, что ресурсы доступны авторизированным пользователям.

4.Другими важными компонентами, которым большое внимание уделяется профессионалами в области компьютерной безопасности, являются контроль над доступом и строгое выполнение обязательств. Контроль над доступом подразумевает не только факт, что пользователь имеет доступ только к имеющимся ресурсам и услугам, но и тот факт, что у него есть право доступа к ресурсам, которые он законно ожидает. Что касается строгого выполнения обязательств, то это подразумевает невозможность отказа пользователям того, что он отправил сообщение и наоборот.

Концепция компьютерной безопасности очень большая, поэтому к данным техническим аспектам есть и другие дополнения. Корни компьютерной безопасности заложены в дисциплине. Основными вопросами, связанными с данным термином, являются компьютерное преступление (попытки предотвратить, обнаружить атаки) и конфиденциальность/анонимность в киберпространстве.

2. Существующие компьютерные угрозы и борьба с ними

2.1.Автоматические обновления.

Большинство приложений и программ, которыми мы пользуемся ежедневно (это если говорим о Windows, интернет-браузерах, плагинах, а не о взломанных программах) зачастую сами беспокоятся о своих обновлениях безопасности.

Сегодня не нужно скачивать отдельный файл, ведь приложения обновляются в фоновом режиме. Чтобы сохранить компьютер в рабочем актуальном состоянии, с точки зрения безопасности, вы ни в коем случае не должны отключать автоматическое обновление (рис.1).

Рис 1. Центр управления Windows

А если уже отключили, то обязательно верните все так как было до этого. Microsoft предоставляет обновления для системы и связанных с ними продуктов регулярно. Таким образом, единственным способом защитить себя от самых последних известных уязвимостей — является активирование функции автообновления (рис.2).

Рис.2. Активирование функции автообновления

Многие организации сегодня управляют устранением уязвимостей и установкой обновлений вручную. Вместо того, чтобы полагаться на автоматизированную установку обновлений, сотрудники ИТ-служб тестируют и проверяют обновления до их разворачивания в продуктовой среде.

Стоит признать, что ручной подход все сложнее и сложнее поддерживать. Вероятно, именно это послужило причиной того, что все больше и больше систем, включая новую Windows 10, переключаются на автоматизированную установку обновлений.

Рассмотрим: действительно ли автоматическое обновление менее опасно, чем ожидание патча?

Согласно Verizon Data Breach Report 2015, 99,9% использованных уязвимостей использовались злоумышленниками через год и более после публикации соответствующих описаний (Common Vulnerabilities and Exposures, CVE).

Более того, более 70% атак использовали известные уязвимости, патчи для которых уже были опубликованы. Это лишний раз подтверждает, насколько сложно сегодня использовать ручной подход.

Неудивительно, что на недавней конференции RSA в Сан-Франциско одним из предметов

1. Грошев, А.С. Информатика: учебник для вузов / А.С. Грошев. — Архангельск: Изд-во Арханг. гос. техн. ун-та, 2010. — 470 с.
2. Информационные технологии в юридической деятельности / под ред. П.У. Кузнецова. — М.: Юрайт, 2011. — 422 с.
3. Информационные технологии в экономике и управлении: учебник / под ред. проф. В.В.Трофимова. — М.: Юрайт, 2011. — 475 с.
4. Костина, А.В. Тенденции развития культуры информационного общества: анализ современных информационных и постиндустриальных концепций / А.В. Костина // Знание. Понимание. Умение. — 2009. — № 4 — С. 12—14.
5. Цветкова, М.С., Модели комплексной информатизации общего образования / М.С. Цветкова, Э.С. Ратобыльская, Г.Д. Дылян; под общ. ред. Г.Д. Дылян. — М.: БИНОМ. Лаборатория знаний. — 119 с.
6. Шендрик, А.И. Информационное общество и его культура: противоречия становления и развития // Информационный гуманитарный портал «Знание. Понимание. Умение». — 2010. — № 4 — Культурологи.