УДК 004.056

Ельсуков Д.А. студент,

2 курс, Институт математики, физики и информационных технологий,

Тольяттинский Государственный Университет

Тольятти (Россия)

Elsukov D.A. student,

2nd year, Institute of Mathematics, Physics and Information Technology,

Togliatti State University

Togliatti (Russia)

БЕЗОПАСНОСТЬ ДАННЫХ В СЕТИ ИНТЕРНЕТ.

Аннотация: В данной статье описаны цифровая безопасность и меры предосторожности для ее соблюдения.

Ключевые слова: Безопасность, интернет, данные, сеть, информация.

Elements of total quality management.

Annotation: This article describes digital security and precautions to comply with it.

Keywords: Security, Internet, data, network, information.

Современный мир существует в эпоху Интернета, и не один день сегодняшнего человека не проходит без взаимодействия с информационной сетью. Безграничный поток информации, столько знаний хранится в нем, столько всего прекрасного, или же нет.

Интернет, являясь источником огромного количества разнообразной информации, может не только ее вам отдать, но и забрать, можно сказать

даже украсть, без вашего ведома, и вы можете даже спустя годы не узнать об этом. Любая информация, которая попала в сеть, останется там навсегда. И не обладая некоторыми знаниями, можно совершить огромную ошибку, которая может привести к большой проблеме, например утечка личной информации, конфиденциальных данных, паролей от банковских карт, информации с вашего паспорта или важных документов. Если неправильно пользоваться информационной сетью можно попасть в неприятность. Но не стоит паниковать, ведь зная простые принципы безопасности в сети интернета, можно избежать столь страшных последствий.

Информационная безопасность – прежде всего, представляет собой защищенность информационных данных от различного вида угроз, как внутренних, так и внешних. Угроз, которые способны нанести ущерб не только человеку, но и целой стране.

Безопасность информации – защищенность данных (информации) от ее разглашения, утечки, деформации (изменения информационных данных), а также незаконного ее распространения.

Исходя из вышеописанных понятий, можно сделать вывод, что информационная безопасность служит для того, чтобы обеспечить защиту данных, безопасность и конфиденциальность.

Сама защита информации представляет собой комплекс мер, направленных на:

1. Обеспечение безопасности информационных данных от незаконного ее получения сторонними лицами, ее искажения или вовсе уничтожения, утечки, деформации, распространения и других подобных действий.

2. Оберегание информации, ее конфиденциальности, если она имеет ограниченный, к ее получению, доступ.
3. Исполнению права на свободный, защищенный доступ к информационным данным

Безопасность в Интернете не ограничивается вышеуказанными свойствами, поскольку она имеет более широкие понятия, в пример можно привести такие понятия, как: кибербезопасность, компьютерная безопасность, защита сети и браузера. Безопасность достигается за счет правильных действий, соблюдений некоторых правил и правильного поведения в Интернете.

В сети Интернет присутствует множество потенциальных угроз пользователю. Мошенничество, вирусы и различные вредоносные программы скрываются за вполне безобидными ссылками, и они просто выжидают своего часта, чтобы нанести удар по вашей системе, и возможно даже украсть вашу личную информацию для выгоды создателя данных вредоносных программ.

Интернет-безопасность довольно широкое понятие, требующее от пользователя знаний, которые помогут свободно взаимодействовать с информационными просторами.

Они включают в себя:

1. Определение безопасного взаимодействия с сетью.
2. Понимание ценности личных данных персонального пользователя сети.
3. Понимание кода
4. Пользование блокировщиками надоедливой рекламы
5. Использование защищенных сетей
6. Использование сетей (VPN)

Пользуясь следующей информацией, и соблюдая просты правила, можно не только обеспечить свободное и безопасное пользование информационными ресурсами, но и повысить свои знания в понимании того, как правильно работать и взаимодействовать с информационной сетью Интернет.

Правила:

1. Обеспечение безопасного подключения к сети. Не стоит подключаться к неизвестным сетям, особенно которые не имеют пароля, в случае подключения по WI-FI.
2. Не стоит переходить по ссылкам из непроверенных источников.
3. Использование официальных ресурсов. Не стоит пользоваться малоизвестными браузерами, поскольку они не гарантируют безопасное пребывание в сети. Нужно посещать только проверенные официальные сайты, особенно, если на вашем персональном компьютере не установлена система по выявлению вирусов (антивирус).
4. Использование надежного пароля. В различных социальных сетях особенно важно использовать хороший пароль для защиты личной информации. Пароль должен содержать набор из цифр, букв разного регистра и символов. Не стоит создавать пароль, состоящий из вашего имени или даты рождения, ведь так вы просто упрощаете работу злоумышленникам.
5. Использование лицензионного ПО. Нередко бывали случаи, когда при скачивании программы с какого-либо сайта, вместе с программой на компьютер попадает вирус. Лицензионные приложения, надежнее всего обеспечат защиту компьютера. Но это не означает, что в Интернете нельзя ничего скачивать. Можно, но только из проверенных многими людьми источников.

Интернет содержит в себе огромное количество полезных знаний, и зная как обеспечить свою безопасность, можно уверенно пользоваться информационными ресурсами.

Список используемой литературы:

1. Васильков А.В. Безопасность и управление доступом в информационных системах / А.В. Васильков, И.А. Васильков. — Москва: ФОРУМ: ИНФРА-М, 2013.— 368 с.;
2. Теоретические основы компьютерной безопасности / П.Н. Девянин [и др.]. — Москва: Радио и связь, 2000.— 192 с.;
3. Малюк А.А. Введение в защиту информации в автоматизированных системах / А.А. Малюк, С.В. Пазизин, Н.С. Погожин. — Москва: Горячая линия — Телеком, 2001.— 148 с.;
4. Зегжда Д. П. Основы безопасности информационных систем / Д.П. Зегжда, А.М. Ивашко. — Москва: Горячая линяя — Телеком, 2000.— 452 с.