БЕЗОПАСНАЯ ВИРТУАЛЬНАЯ СРЕДА УЧЁБЫ, ДОСУГА, СПОРТА СТУДЕНЧЕСКОЙ МОЛОДЁЖИ. ОБЕСПЕЧЕНИЕ ЛИЧНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А. С. Омелянчук, В. М. Ермалович
A. S. Omelyanchuk, V. M. Ermalovich

Академия Управления при Президенте Республики Беларусь
Минск, Беларусь
Academy of Public Administration under the President of the Republic of Belarus
Minsk, Belarus

e-mail: omelancukangelina@gmail.com, violettaerma@icloud.com,

В статье представлена информация о проблемах обеспечения безопасности в интернете. Рассматриваются основные угрозы личной безопасности в интернете. Авторами подчеркивается важность обеспечения безопасности в интернете и необходимость принятия мер для защиты личных данных и предотвращения различных угроз.

Ключевые слова: кибербезопасность, защита персональных данных, кибербуллинг.

The article deals with information about the problems of Internet security. The main threats to personal security on the Internet are discussed. The authors emphasize the importance of Internet security and the need to take measures to protect personal data and prevent various threats.

Keywords: cybersecurity, personal data protection, cyberbullying.

Обеспечение безопасности в интернете является актуальной темой в современном мире. Интернет стал неотъемлемой частью нашей жизни, однако с появлением новых технологий возникают и новые угрозы безопасности в интернете.

С каждым годом становится все больше и больше устройств, подключенных к интернету – от компьютеров и ноутбуков до мобильных телефонов, планшетов и умных домов. Это означает, что безопасность в интернете становится еще более важной, так как с каждым устройством увеличивается количество потенциальных точек входа для хакеров.

Актуальной задачей становится формирование умений пользоваться информационными ресурсами, критически воспринимать, оценивать,

анализировать полученные сведения и, выделяя главное, превращать их в собственное знание.

Кибербуллинг и *кибербезопасность* – это два тесно связанных аспекта, представленных в интернете.

Кибербуллинг – это форма онлайн-насилия, при которой человек страдает от оскорбительных, унизительных или угрожающих сообщений в интернете. Он может быть осуществлен через социальные сети, форумы, чаты и другие онлайн-платформы.

Кибербезопасность – это процесс обеспечения безопасности данных, информации и пользователей в онлайн-среде. Кибербезопасность включает в себя защиту от хакерских атак, вирусов, фишинговых атак и других киберугроз.

Кибербуллинг может быть одним из аспектов кибербезопасности, так как он может представлять угрозу для личных данных и информации, а также для эмоционального и психологического благополучия человека.

Таким образом, кибербуллинг и кибербезопасность – это важные аспекты безопасности в интернете, которые необходимо учитывать при использовании онлайн-платформ и социальных сетей.

Существует несколько способов, которые могут помочь обезопасить себя в интернете:

1. Использовать сильные пароли без повторения на разных сайтах. Необходимо использовать уникальные и длинные пароли, содержащие комбинацию букв, цифр и символов.
2. Обновлять программное обеспечение своего устройства, включая операционную систему, браузер и антивирусную программу, чтобы быть защищенным от известных уязвимостей.
3. Избегать подключения к открытым и ненадежным Wi-Fi сетям. При необходимости использования открытой сети, пользоваться VPN-сервисами для шифрования вашего трафика.
4. Быть осторожными при открытии электронных писем и приложений, особенно от неизвестных отправителей. Никогда не открывать вложения, не будучи уверенным в их безопасности.
5. Использовать двухфакторную аутентификацию, которая требует ввода кода, отправленного на личный мобильный телефон или другое устройство, помимо пароля, для входа в учетную запись.
6. Избегать использования общих компьютеров или устройств с целью недопущения потенциальной утечки личной конфиденциальной информации.

7. Быть осторожными при совершении онлайн-покупок и использовать только безопасные сайты, проверенные сертификатами безопасности.
8. Обучать себя и своих близких основам безопасности в интернете, информировать их о возможных опасностях и правилах безопасного поведения в интернете.

Невероятной ценностью является информация, несущая в себе данные о личной, индивидуальной или семейной жизни человека. Информация, которая затрагивает частные интересы человека должны уважаться и защищаться государством. На сегодняшний момент сохранность информации человека «о его жизни» зависит только от него самого. Есть и другая ситуация, когда мы обязаны предоставить данные о себе в соответствии с законом третьему лицу, а именно работодателю. Работник в данной ситуации передает конфиденциальную информацию о себе на ответственное хранение. После этого за сохранность данных, способы их защиты, ответственность за невыполнение обязательств по обеспечению сохранности персональных данных отвечает уже работодатель.

Персональные данные состоят из следующих компонентов: состояние здоровья, номер ваших документов, фамилия, имя, дата рождения, номер телефона, отпечатки пальцев, личные фотографии.

Защита персональных данных - безопасное хранение персональных данных от случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от других неправомерных действий в отношении персональных данных.

Существует множество видов киберпреступлений, которые могут быть совершены в интернете.

Киберпреступники могут получить доступ к конфиденциальной информации, включая данные банковских карт, персональные данные и другую конфиденциальную информацию.

Правила, которых необходимо придерживаться для защиты своих персональных данных:

1) не использовать способ разблокировки телефона через отпечаток пальца или FACE ID;
2) установить настройки приватности для своего профиля в социальных сетях;
3) запрещать доступ мобильных приложений к информации, хранящейся в телефоне;

4) при прокладывании маршрута при помощи google-карт, не забывать по прибытию в пункт назначения, отключать передачу геоданных в настройках телефона;
5) не указывать в интернете, мобильных приложениях свою геолокацию.

Несоблюдение вышеперечисленных правил может привести к плачевным последствиям, а именно:

1) краже имущества;
2) созданию фейкового аккаунта;
3) навязчивой рекламе и звонкам;
4) хищению и продаже персональной информации злоумышленниками;
5) копированию личных фото и видео без разрешения;
6) возможности стать объектом слежки.

Обеспечение безопасности в виртуальной среде является общей ответственностью всех пользователей интернета. Поэтому важно не только следовать правилам безопасности, но и принимать активное участие в борьбе с киберугрозами и информировать других о проблемах безопасности в интернете. Только тогда мы сможем создать безопасную и надежную среду для работы, общения и развлечений в интернете.

СПИСОК ЛИТЕРАТУРЫ

1. *Петренко В. И., Мандрица И. В.* Защита персональных данных в информационных системах. [Текст] / В. И. Петренко, И. В. Мандрица. – . – СПб : «Лань», 2019 – 108 с.