Клепиковский Алексей Александрович, преподаватель,
Филиал Военного учебно-научного центра
Военно-воздушных сил «Военно-воздушная академия
имени профессора Н.Е. Жуковского и Ю.А. Гагарина»,
г. Челябинск

Букин Роман Владимирович, курсант,
Филиал Военного учебно-научного центра
Военно-воздушных сил «Военно-воздушная академия
имени профессора Н.Е. Жуковского и Ю.А. Гагарина»,
г. Челябинск

ЗАЩИТА ИНФОРМАЦИИ
INFORMATION PROTECTION

Аннотация: В эпоху цифровых технологий и повсеместного использования интернета вопрос информационной безопасности становится особенно актуальным. Обучение основам кибербезопасности и осведомленность о текущих угрозах помогут пользователям защитить свои данные и создать более безопасную цифровую среду. Статья нацелена на то, чтобы повысить уровень информированности и ответственности пользователей в вопросах безопасности в интернете.

Abstract: In the era of digital technologies and the widespread use of the Internet, the issue of information security is becoming particularly relevant. Learning the basics of cybersecurity and awareness of current threats will help users protect their data and create a more secure digital environment. The article aims to raise the level of awareness and responsibility of users in Internet security issues.

Ключевые слова: информация, безопасность, угрозы, социальные сети, кибербулинг, фишинг.

Keywords: information, security, threats, social networks, cyberbullying, phishing.

Информация – сведения (сообщения, данные) независимо от формы их представления [1]

Информационная безопасность, в свою очередь, представляет собой комплекс мер, направленных на защиту информации от несанкционированного доступа, изменения, распространения или уничтожения.

Информационная безопасность охватывает в себя ключевые направлений в области:

Кибербезопасность. Это защита компьютерных систем, сетей, программного обеспечения и данных от цифровых атак, киберпреступников и других угроз в интернете. Она включает в себя как профилактические меры, так и реагирование на инциденты.

Физическая безопасность. Охрана серверов, компьютеров, устройств хранения данных и других элементов инфраструктуры. Это важный аспект, который обеспечивает защиту информации от физических угроз, таких как кража или повреждение оборудования.

Информационная безопасность данных. Направлена на защиту самих данных и предотвращение их утечек. Это может включать шифрование данных, управление доступом и мониторинг активности.

Сетевая безопасность. Обеспечивает защиту компьютерных сетей от атак, таких как вирусы, вредоносные программы и несанкционированный доступ. Это включает в себя использование межсетевых экранов, систем обнаружения вторжений и других технологий.

Основная цель информационной безопасности обеспечить защиту от любого несанкционированного доступа, утечек и изменения данных. Это достигается с помощью

различных технических, программных, аппаратных и организационных мер, которые направлены на предотвращение, своевременное обнаружение и реагирование на кибератаки.

Воздействие на информационную безопасность – это угрозы, которые могут привести к несанкционированному доступу, уничтожению, изменению или утечке данных, а также вызвать сбои в работе информационных систем и сетей. Эти угрозы могут иметь серьезные последствия как для организаций, так и для частных лиц.

Данные – это информация, предоставленная в формализованном виде и предназначенная для обработки ее техническими средствами [3, ст. 12].

Некоторые виды воздействия на информационную безопасность:

Кибератаки и хакерство. Это включает в себя фишинг, DDoS-атаки, внедрение вредоносного программного обеспечения и целевые атаки. Хакеры используют уязвимости в системах безопасности для получения доступа к конфиденциальной информации, шпионажа или саботажа.

Отказ в обслуживании (DoS/DDoS). Атаки, осуществляемые с сотен компьютеров, направлены на перегрузку сервера, что приводит к его неработоспособности и невозможности ответить на запросы пользователей.

Утечки данных. Потеря конфиденциальной информации, которая может произойти в результате хакерской атаки или случайного раскрытия данных.

Сетевые угрозы. Это возможность перехвата данных, подмена точек доступа и другие манипуляции в сети, связывающей устройства с интернетом.

Уязвимости программного обеспечения. "Дыры" в программном обеспечении, которые могут быть использованы злоумышленниками для взлома устройств и получения к ним доступа.

Чтобы обеспечить информационную безопасность, необходимо:

Использование надежных паролей. Создавайте уникальные сложные пароли для каждого сайта и сервиса, включая буквы верхнего и нижнего регистра, цифры и специальные символы.

Регулярные обновления программного обеспечения. Обновления помогают исправить уязвимости, которые могут быть использованы злоумышленниками.

Внимательность в сети. Не открывайте подозрительные ссылки и вложения в электронной почте, будьте осторожны с фишинговыми атаками.

Защита мобильных устройств. Используйте PIN-код или графический ключ для блокировки экрана телефона, устанавливайте приложения безопасности и избегайте загрузки из ненадежных источников.

Информационная безопасность в социальных сетях – это защита личной информации и данных пользователей, а также предотвращение угроз и рисков, связанных с их использованием.

Вот некоторые угрозы информационной безопасности в социальных сетях:

Фишинг. Злоумышленники пытаются получить доступ к личной информации, выдавая себя за надежные источники.

Вредоносные программы. Вирусы, трояны и шпионское ПО могут распространяться через социальные сети.

Нарушение конфиденциальности. Пользователи могут неосознанно раскрывать личные данные, которые могут быть использованы злонамеренно.

Кибербуллинг. Пользователи могут стать жертвами оскорблений, угроз или шантажа.

Социальная инженерия. Метод манипуляции людьми для получения доступа к их личной информации или системам.

Основная цель информационной безопасности в социальных сетях – создать безопасную среду для пользователей, предотвратить утечку личной информации и минимизировать риски, связанные с их использованием.

Меры обеспечивающие информационную безопасность социальных сетей:

Настройка конфиденциальности. Убедитесь, что ваши публикации и профиль доступны только друзьям, а доступ для незнакомцев отключен.

Использование надежных паролей. Применяйте уникальные пароли для разных аккаунтов, содержащие комбинацию букв, цифр и символов. Рекомендуется использовать менеджер паролей.

Осторожность с запросами на добавление в друзья. Принимайте запросы только от людей, которых вы знаете лично.

Внимательность к ссылкам и сообщениям. Не переходите по подозрительным ссылкам и не открывайте неожиданные вложения. Даже если сообщение пришло от друга, уточните, действительно ли он отправил ссылку или файл.

Ограничение публикации личной информации. Избегайте делиться слишком многими личными данными, такими как адрес, номер телефона или информация о местоположении.

Решение проблемы информационной безопасности, как правило, начинается с выявления субъектов информационных отношений и интересов этих субъектов [2, ст. 9].

В заключение, информационная безопасность является критически важным аспектом нашей цифровой жизни, особенно в условиях стремительного развития технологий и увеличения числа пользователей социальных сетей. Защита личной информации и данных требует от нас осознанного подхода и применения эффективных мер безопасности.

Список литературы:

1. Российская Федерация. Законы. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 01.01.2025) // Собрание законодательства РФ. – 2006. – № 31. – Ст. 3448. – ISSN 1560-0580.

2. Баранова, Е. К. Информационная безопасность и защита информации: учебное пособие / Е.К. Баранова, А.В. Бабаш. – 4-е изд., перераб. и доп. – Москва: РИОР: ИНФРА-М, 2024. – 336 с. – (Высшее образование). – DOI: https://doi.org/10.29039/1761-6. – ISBN 978-5-369-01761-6.

3. Баранова, Е. К. Основы информационней безопасности: учебник / Е.К. Баранова, А.В. Бабаш. – Москва: РИОР: ИНФРА-М, 2025. – 202 с. – (Среднее профессиональное образование). – DOI: https://doi.org/10.29039/01806-4. – ISBN 978-5-369-01806-4.

4. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В.Ф. Шаньгин. – Москва: ФОРУМ: ИНФРА-М, 2024. – 416 с. – (Среднее профессиональное образование). – ISBN 978-5-8199-0754-2.