**Вызовы и угрозы информационной безопасности в XXI веке**

*Петухова Валерия Владимировна, преподаватель информатики*

*ГБПОУ «Миасский медицинский колледж»*

**Аннотация:** в данной статье рассматриваются вызовы и угрозы информационной безопасности в 21 веке.

**Ключевые слова:** информационная безопасность.

Тема информационной безопасности в последние годы становится более актуальной. Жизнь стремительно переходит в онлайн, отдельные её аспекты частично или полностью автоматизируются. Бизнес и государственные организации повсеместно внедряют современные технологии и «оцифровываются».

Всё это не только ускоряет темпы, меняет саму реальность в корне и создаёт тысячи новых возможностей и перспектив. Масштабное распространение технологий и переход в сеть порождают множество рисков, в том числе – киберугроз. Именно поэтому приоритетным в любой сфере становится обеспечение информационной безопасности.

Информационная безопасность – это практика предотвращения [несанкционированного доступа](https://ru.wikipedia.org/wiki/%D0%9D%D0%B5%D1%81%D0%B0%D0%BD%D0%BA%D1%86%D0%B8%D0%BE%D0%BD%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%BD%D1%8B%D0%B9_%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF), использования, раскрытия, искажения, изменения, исследования, записи или уничтожения [информации](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F). Это универсальное понятие применяется вне зависимости от формы, которую могут принимать [данные](https://ru.wikipedia.org/wiki/%D0%94%D0%B0%D0%BD%D0%BD%D1%8B%D0%B5) (электронная или, например, физическая) [1].

Основная задача информационной безопасности — сбалансированная защита [конфиденциальности](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BD%D1%84%D0%B8%D0%B4%D0%B5%D0%BD%D1%86%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D1%81%D1%82%D1%8C), [целостности](https://ru.wikipedia.org/wiki/%D0%A6%D0%B5%D0%BB%D0%BE%D1%81%D1%82%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8) и [доступности](https://ru.wikipedia.org/wiki/%D0%94%D0%BE%D1%81%D1%82%D1%83%D0%BF%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8) данных, с учётом целесообразности применения и без какого-либо ущерба [производительности](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%B8%D0%B7%D0%B2%D0%BE%D0%B4%D1%81%D1%82%D0%B2%D0%B5%D0%BD%D0%BD%D0%B0%D1%8F_%D0%BC%D0%BE%D1%89%D0%BD%D0%BE%D1%81%D1%82%D1%8C) организации.

Актуальность темы защиты данных в России подтверждена на общегосударственном уровне. Так, в стране реализуется федеральный проект «Информационная безопасность» в рамках национальной программы «Цифровая экономика» [2].

В задачи проекта входит обеспечение информационной безопасности на основе отечественных разработок с целью защиты интересов личности, бизнеса и государства. В качестве приоритетов обозначены целостное, устойчивое и безопасное функционирование российского сегмента интернета, а также усиление защиты государственных информационных систем от хакерских атак.

В XXI веке информационная безопасность сталкивается с рядом вызовов и угроз. Вот самые распространенные:

1. Кибератаки: Это включает в себя различные виды атак, такие как вредоносное ПО, фишинг, DDoS-атаки и т.д. Кибератаки могут привести к утечке конфиденциальной информации, нарушению работы систем и даже к экономическому ущербу.

**Вредоносное ПО:** Хакеры создают и распространяют вредоносные программы, такие как вирусы, троянцы, шпионские программы и руткиты, которые могут заражать компьютеры и украсть информацию.

Один из наиболее распространенных видов атак, который включает в себя отправку фальшивых сообщений или веб-сайтов, которые выглядят как официальные, с целью получить конфиденциальную информацию, такую как пароли и данные банковских карт.

Усиление внешнеполитической нестабильности спровоцировали рост DDoS-атак на российские веб-ресурсы. Распределенные атаки типа «отказ в обслуживании» стали самой распространенной угрозой информационной безопасности России. С начала 2022 года их жертвами стали [3]:

* сайты Центризбиркома РФ, Президента РФ, «Госуслуг», Россельхознадзора, Роспотребнадзора и десятков региональных СМИ;
* сервисы РЖД, «1С», Сбербанка;
* ряд российских систем электронного документооборота (ЭДО);
* платежная система «Мир» и Национальная система платежных карт (НСПК).

При этом DDoS-атаки стали масштабнее не только по охвату, но также по силе и по длительности

2. **Социальная инженерия** — это манипулирование людьми, в том числе психологическое, с целью заставить их совершить определённые действия или сообщить конфиденциальную информацию.

**Основные техники социальной инженерии:**

**– Фишинг.** Мошенники отправляют потенциальным жертвам электронные письма или сообщения в мессенджере, стараются сделать их максимально правдоподобными.

– **Вишинг.** Разновидность фишинга, в данном случае мошенники звонят потенциальным жертвам, представляются сотрудниками банков, полиции и т.д.

**– Приманка.** Мошенники расставляют приманки — это может быть любое устройство, например, флэшка, power bank и т.д. Приманка заражена вирусом.

**– Привлечение внимания.** Чтобы привлечь внимание пользователей, мошенники размещают в интернете безобидные с виду материалы, например, несложные тесты, опросы и т.д.

3. Утечки данных: Это случайное или преднамеренное раскрытие конфиденциальной информации. Утечки данных могут привести к серьезным последствиям, таким как кража личности, финансовые потери и нарушение приватности. Вопросом выявления и предупреждения подобных нарушений кибербезопасности озаботилось само государство. Выполняя президентский указ от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности РФ», Минцифры обязалось до конца года создать открытый реестр с перечнем «недопустимых» ИБ-инцидентов, способных подорвать работу КИИ.

4. Недостатки безопасности: Это может включать в себя слабые пароли, уязвимости в программном обеспечении, отсутствие обновлений безопасности и т.д. Недостатки безопасности могут сделать системы уязвимыми для кибератак.

5. Недостаток осведомленности: Некоторые люди могут не осознавать важность информационной безопасности и не принимать необходимые меры для защиты своих данных и систем.

Чтобы справиться с этими вызовами, необходимо постоянно улучшать механизмы безопасности, обучать пользователей и организации, сотрудничать с другими странами и секторами, а также внедрять новые технологии для обеспечения безопасности.

Список использованных источников

1. https://ru.wikipedia.org/wiki/Информационная\_безопасность

2. https://www.hr.cibit.ru/stati/informacionnaya-bezopasnost-vyzovy-ugrozy-perspektivy/

3. https://apni.ru/article/6280-vizovi-i-ugrozi-informatsionnoj-bezopasnosti