

## **КИБЕРУГРОЗЫ. ИХ ВИДЫ И СПОСОБЫ БОРЬБЫ С НИМИ**

### **Кулишова Диана Васильевна**

студент, ЧОУ ВО Южный университет (ИУБиП), РФ, г. Ростов-на-Дону

### **Мазманян Софи Аргамовна**

студент, ЧОУ ВО Южный университет (ИУБиП), РФ, г. Ростов-на-Дону

### **Исабаева Екатерина Андреевна**

студент, ЧОУ ВО Южный университет (ИУБиП), РФ, г. Ростов-на-Дону

**Кибербезопасность** — совокупность мер, приемов и методов защиты от взломов, атак хакеров для компьютеров, планшетов, мобильных устройств, серверов, электронных серверов, приложений, сетей и использования информации в корыстных целях.

Данная система имеет популярность и используется в разных областях: бизнес-сфера, IT-сфера, юриспруденция и многих других.

Масштаб распространения угроз в сети Интернет повышается с каждым годом. Так, согласно отчетам RiskBased в период с 01.01.2019 по 01.09.2019 было обнаружено 7,9 миллиардов случаев утечки данных из киберсистемы. Данные значения превышают показатели 2018 года в два раза. За 2019 год Cybersecurity Ventures сообщает о частоте атак хакеров. Их число доходит до взломов каждые 14 секунд, а к 2025 их быстрота достигнет 11 секунд.

Данные были опубликованы в официальном регулярном и ежегодном отчете о кибератаках за 2019 год.

Большинство компаний, служб сталкиваются с киберпроблемами. Многие остаются безвозвратно без важной информации, денежные средства из-за отсутствия должной информационной безопасности.

Бывали случаи, когда секретные материалы становились доступны в сети Интернет и ими могли пользоваться разные люди.

Не менее распространенная ситуация, когда обычные юзеры всемирной паутины не могли сохранить личные сведения и ими злоумышленники пользовались в корыстных целях, выпрашивая денежные средства или шантажируя по-иному.

Многими учеными и анализаторами были составлены элементарные меры по защите от киберугроз, соблюдение которых поможет оставлять свои данные в безопасности.

Две трети использующих сеть Интернет имеют одно незащищенное устройство, которое может быть раскрыто злоумышленниками. Также, используя незащищенные сети Wi-Fi, переходя на непроверенные сайты люди подвергают риску утечки данных.

Соблюдение простых правил кибербезопасности позволят сохранить личную защиту. Соблюдение кибергигиены является потребностью каждого пользователя сети Интернет.

Аналитик рассказывает о новом популярном способе программы с мошенническими

программами это троянцы-шифровальщики, требующие выкуп за расшифровку информации.

Также, он рекомендует не пользоваться неизвестными сайтами, не подключаться к неизвестным бесплатным сетевым подключениям.

### **Различные способы борьбы с хакерством:**

- Установление антивирусной защиты (антивирусные программы);
- Установление программ, обеспечивающих своевременное обновление
- Установление оборудования, оснащенного защитой от киберугроз;
- Резервное копирование информации;

### **Способы сохранения личных данных пользователям сети Интернет:**

- Не посещать сомнительные сайты;
- Не переходить по ссылкам в неизвестные источники;
- Не распространять и не вводить свои персональные данные (номер телефона, паспортные данные, адрес места жительства и так далее) на неизвестных сайтах и так далее;
- Устанавливать антивирусные программы;
- Регулярно проверять и обновлять программы безопасности.

Пользователи сети Интернет должны приобрести базовые знания о информационной безопасности, угрозах, методах защиты от них. Так же, статья позволяет сформировать и использовать полученные знания по использованию сети Интернет и защите от злоумышленников от разных видов информационных угроз.

Целью данной статьи является оснащение населения о базовых способах защиты от угроз злоумышленников в сети Интернет, о способах разоблачения взлома, слива персональных данных. В результате будут выделены наиболее важные знания, обобщены различные положения информационной безопасности и будет знакомство с понятиями кибергигиена, киберугроза, кибербезопасность

### **Список литературы:**

1. «Мой-сервис-гид Кибербезопасность» - путеводитель в области ремонта техники. «Кибербезопасность». [Электронный ресурс]. URL:<https://www.my-cervice-guide.ru/press-center/articles/advice-and-instructions/235>
2. «Cyberlininka» - научная электронная библиотека. «Кибербезопасность». [Электронный ресурс]. URL: <https://cyberleninka.ru/article/n/primeneniye-metodov-glubokogo-obucheniya-v-zadachah-kiberbezopasnosti-chast-2>
3. «Cisco» - мировой лидер в области информационных технологий и сетей. [Электронный ресурс]. URL:[https://www.cisco.com/c/ru\\_ru/products/security/what-is-cybersecurity.html](https://www.cisco.com/c/ru_ru/products/security/what-is-cybersecurity.html)
4. «Сервисы» - сервер, анализирующий выводы учёных. [Электронный ресурс]. URL:<https://vc.ru/services/103616-utechki-dannyh-2019-statistika-tendencii-kiberbezopasnosti-i-mery-po-snizheniyu-riskov-vzloma>