УДК 343.34

КИБЕРАТАКИ КАК УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
CYBER ATTACKS AS A THREAT TO INFORMATION SECURITY

И.Е. Скоробогатов, Р.А. Грицкевич
Морской государственный университет имени адмирала Г.И. Невельского, Владивосток
Гамс А.В., старший преподаватель кафедры радиоэлектроники и радиосвязи

Аннотация. Киберугрозы и кибератаки напрямую связанны с цифровизацией. Именно поэтому в современном мире данные понятия уже не являются чем-то фантастическим, так как подобные инциденты случаются постоянно. В статье представлен анализ киберугроз, а также рассмотрены цели злоумышленников в таких преступлениях.

Ключевые слова: киберугрозы, кибератаки, цифровизация, кибербезопасность, IT-технологии.

Abstract. Cyber threats and cyber attacks are directly related to digitalization. That is why in the modern world, these concepts are no longer something fantastic, as such incidents happen all the time. The article presents an analysis of cyber threats, as well as the goals of intruders in such crimes.

Keywords: cyber threats, cyber attacks, digitalization, cybersecurity, IT technologies.

В связи со сплошной цифровизацией такой ценный ресурс, как персональные данные, находится под угрозой. Тот факт, что государство в своей деятельности активно использует цифровые технологии, обуславливает повышенный риск кражи данных граждан. В опасности находятся не только те сведения, которые содержатся в документах граждан, но и их банковские счета, так как именно данные, содержащиеся в документах позволяют злоумышленникам безнаказанно списывать безналичные денежные средства, и совершать банковские операции от чужого имени.

Согласно исследованиям «Лаборатории Касперского», одного из самых известных сервисов по защите от киберугроз, 90% организаций регулярно сталкивается со всем многообразием кибератак [1]. Основная опасность атак заключается в том, что они развиваются значительно быстрее, чем системы защиты. К тому моменту, как разрабатывается «противоядие», преступники утрачивают интерес к старому методу взлома, и изобретают новый, куда более изощренный, чем использовался ранее [2].

Под кибербезопасностью понимается многообразие способов и методов защиты от правонарушений, совершаемых в «виртуальном пространстве». Деяния злоумышленников в «виртуальном пространстве» - это злонамеренные действия в отношении различных видов устройств, таких как компьютеры, мобильные телефоны и сетей, серверов, данных.

Существенной преградой к эффективному осуществлению мер по кибербезопасности являются киберугрозы. Киберугроза – это такое незаконное вмешательство в деятельность вышеназванных объектов, которое приводит к угрозе и (или) потере данных, либо к угрозе и (или) нарушению работы вычислительных систем [3].

IT-технологии порождают развитие общества и государства в наиболее прогрессивном русле. Следствием этого является то, что в современном мире наиболее уязвимым звеном являются информационные технологии [4]. Именно информационные технологии позволяют уместить огромный объем информации на различных сервисах и в вычислительных системах. На диаграмме, представленной ниже приведены статистические данные об информации, получение которой становится основной целью киберпреступников. Цели злоумышленников представлены на рисунке 1.

Рисунок 1 – Цели злоумышленников

Из приведенной выше диаграммы мы видим, что основной целью хакеров является получение незаконного доступа к персональным данным других лиц. На втором месте находится коммерческая тайна, в данном случае пострадавшей стороной считаются юридические лица и индивидуальные предприниматели, доступ к данным которых чаще всего получают через рядовых работников. Третье место в этом рейтинге

занимают учётные данные, позволяющие произвести аутентификацию пользователя и успешно получить доступ к личным данным и настройкам пользователя. Следующий вид конфиденциальной информации, на которую покушаются при кибератаках – базы данных клиентов, которые позволяет структурировать предпринимательскую деятельность юридических лиц и индивидуальных предпринимателей. Также атакам подвергаются медицинские данные, представляющие собой охраняемую законом тайну, информация платежных карт, переписки и иная информация.

Список литературы

1. Гуревич, А. Седьмая конференция "Лаборатории Касперского" по промышленной кибербезопасности. [Электронный ресурс]/ А. Гуревич // Релейщик. – 2019. – № 3(35). – С. 4-5. – URL: https://www.elibrary.ru/item.asp?id=41493591 (дата обращения: 03.03.2025)

2. Бураева Людмила Александровна О некоторых вопросах обеспечения кибербезопасности в современных условиях // Теория и практика общественного развития. 2015. №13. URL: https://cyberleninka.ru/article/n/o-nekotoryh-voprosah-obespecheniya-kiberbezopasnosti-v-sovremennyh-usloviyah (дата обращения: 04.03.2025).

3. Валько Д. В. Киберпреступность в России и мире: сопоставительная оценка // Управление в современных системах. 2016. №3 (10). URL: https://cyberleninka.ru/article/n/kiberprestupnost-v-rossii-i-mire-sopostavitelnaya-otsenka (дата обращения: 04.03.2025).

4. Гришин С. Е. Формирование культуры кибербезопасности в обществе актуальная задача современности // Промышленность: экономика, управление, технологии. 2011. №4. URL: https://cyberleninka.ru/article/n/formirovanie-kultury-kiberbezopasnosti-v-obschestve-aktualnaya-zadacha-sovremennosti (дата обращения: 04.03.2025).