**ОСНОВНЫЕ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СОВРЕМЕННОМ МИРЕ**

**Якуба Валерий Александрович**

студент, кафедра экологии и природопользования,

Севастопольский государственный университет,

РФ, г. Севастополь

Е-mail: yakuba.2019@inbox.ru

**Девицына Светлана Николаевна**

канд. тех. наук, доц., Севастопольский государственный университет,

РФ, г. Севастополь

**THE MAIN THREATS TO INFORMATION SECURITY IN THE MODERN WORLD**

 ***Yakuba Valery Alexandrovi***

 Student, Department of Ecology and Environmental Management,

 Sevastopol State University,

 Russian Federation, Sevastopol

 E-mail: yakuba.2019@inbox.ru

 **Devitsyna Svetlana Nikolaevna**

 **Candidate of Technical Sciences, Associate Professor,**

 **Sevastopol State University,**

 **Russian Federation, Sevastopol**

**АННОТАЦИЯ**

В статье рассматриваются современные угрозы кибербезопасности, их основные виды и особенности. Анализируются актуальные типы кибератак, такие как вредоносное ПО, фишинг, атаки на инфраструктуру и социальная инженерия. Особое внимание уделяется методам выявления и предотвращения угроз, а также современным технологиям защиты информации, включая системы обнаружения вторжений, шифрование и многоуровневую аутентификацию. В работе подчеркивается важность формирования комплексных стратегий кибербезопасности для организаций и отдельных пользователей в условиях постоянно меняющегося цифрового ландшафта.

**ABSTRACT**

The article discusses modern cybersecurity threats, their main types and features. The current types of cyber attacks such as malware, phishing, attacks on infrastructure and social engineering are analyzed. Special attention is paid to threat detection and prevention methods, as well as modern information security technologies, including intrusion detection systems, encryption, and multi-level authentication. The paper highlights the importance of developing comprehensive cybersecurity strategies for organizations and individual users in an ever-changing digital landscape.

**Ключевые слова: Методы исследования;** **Обработка информации; Анализ данных; Методы исследования.**

**Keywords:** Research methods; Information processing; Data analysis; Research methods.

**Современные угрозы кибербезопасности в современном мире**

В эпоху стремительного развития технологий киберугрозы становятся все более разнообразными и сложными, оказывая значительное влияние на бизнес, государственные структуры и частных пользователей. Сегодня киберпреступники используют различные методы для получения несанкционированного доступа к данным, разрушения информационных систем и шантажа. Основными источниками угроз являются вредоносное программное обеспечение, фишинговые атаки, атаки типа "отказ в обслуживании" (DDoS), а также внутренние угрозы со стороны сотрудников и партнеров.



**Рисунок 1. Угрозы Кибербезопасности**

Вредоносное программное обеспечение, такое как вирусы, трояны и программы-вымогатели, продолжает оставаться одной из главных угроз. В 2024 году количество случаев заражения выросло на 25% по сравнению с предыдущим годом, что свидетельствует о росте активности киберпреступников. Рансомварные атаки наносят значительный ущерб организациям, блокируя доступ к важной информации и требуя выкуп за восстановление данных. Фишинг, использующий социальную инженерию для получения конфиденциальной информации, также остается популярным инструментом злоумышленников.

**Таблица 1.**

**Статистика современных угроз кибербезопасности за 2024 год**

| **Тип угрозы** | **Количество инцидентов** | **Рост по сравнению с 2023 годом** | **Средний ущерб, млн долларов** |
| --- | --- | --- | --- |
| Вредоносное ПО (вирусы, программы-вымогатели) | 150 000 | +25% | 3,2 |
| Фишинг-атаки | 200 000 | +20% | 1,8 |
| DDoS-атаки | 35 000 | +30% | 2,5 |
| Внутренние угрозы | 50 000 | +15% | 1,2 |

Эти данные свидетельствуют о необходимости усиления мер по обеспечению кибербезопасности, внедрения современных систем защиты и обучения персонала. В современных условиях важно не только использовать технические средства защиты, такие как межсетевые экраны и системы обнаружения вторжений, но и формировать культуру информационной безопасности внутри организаций. Только комплексный подход поможет снизить риски и защитить важные информационные ресурсы от постоянно развивающихся киберугроз.

В современном мире киберугрозы становятся все более разнообразными и сложными, что требует от организаций и отдельных пользователей принятия эффективных мер по обеспечению информационной безопасности. Ниже представлены основные методы борьбы с современными киберугрозами, которые помогают снизить риски и защитить важные данные.

**Таблица 2**

**Методы борьбы с современными киберугрозами**

| **Метод борьбы** | **Краткое описание** | **Эффективность** |
| --- | --- | --- |
| Обучение и повышение кибербезопасности сотрудников | Регулярные тренинги и информационные кампании по вопросам киберугроз и безопасных практик. | Высокая |
| Использование антивирусных программ и антивредоносного ПО | Установка современных антивирусных решений для обнаружения и устранения вредоносных программ. | Высокая |
| Многофакторная аутентификация | Внедрение дополнительных уровней проверки личности для доступа к системам и данным. | Очень высокая |
| Регулярное обновление программного обеспечения | Обновление операционных систем и приложений для устранения уязвимостей. | Высокая |
| Резервное копирование данных | Создание резервных копий важной информации для восстановления после атак или сбоев. | Очень высокая |
| Использование системы обнаружения вторжений (IDS) | Мониторинг сети и систем на предмет подозрительной активности и своевременное реагирование. | Высокая |
| Ограничение доступа и принцип наименьших привилегий | Предоставление пользователям только тех прав, которые необходимы для выполнения задач. | Высокая |
| Внедрение политики безопасности и процедур | Разработка четких правил и инструкций по информационной безопасности внутри организации. | Средняя — высокая |

В заключение, современный мир сталкивается с все более сложными и разнообразными киберугрозами, которые требуют системного и комплексного подхода к обеспечению информационной безопасности. Эффективная борьба с киберрисками невозможна без использования современных методов защиты, постоянного мониторинга, обучения персонала и своевременного реагирования на инциденты. Внедрение передовых технологий и соблюдение лучших практик позволяют значительно снизить риски и обеспечить надежную защиту данных и инфраструктуры. Только совместными усилиями организаций, специалистов и пользователей можно создать устойчивую систему кибербезопасности и минимизировать потенциальные угрозы в цифровом пространстве.

**Список литературы:**

1. Васильев В. И. Оценка актуальных угроз безопасности информации с помощью технологии трансформеров / В. И. Васильев, А. М. Вульфин, Н. В. Кучкарова // Вопросы кибербезопасности. - 2022. - № 2. - С. 27-38.
2. Гладких А. В. Методы защиты от DDoS –атак в интеллектуальных сетях / А. В. Гладких // Цифровая трансформация общества и информационная безопасность : материалы Всеросс. науч.-практ. конф. (Екатеринбург, 18 мая 2022 г.) - Екатеринбург, 2022. - С. 3-5.
3. Алгоритм выявления угроз информационной безопасности в распределенных мультисервисных сетях органов государственного управления / А. Ю. Пучков, А. М. Соколов, С. С. Широков, Н. Н. Прокимнов // Прикладная информатика. - 2023. - Т. 18, № 2. - С. 85-102.