**НАИБОЛЕЕ РАСПРОСТРАНЕННЫХ УГРОЗ БЕЗОПАСНОСТИ ЗА ПОСЛЕДНИЕ 5 ЛЕТ**

**ВВЕДЕНИЕ**

Угроза безопасности информации означает действие или событие, которое может привести к нарушению, искажению или несанкционированному использованию информационных ресурсов, включая хранимую, передаваемую и обрабатываемую информацию, а также программное и аппаратное обеспечение .

Основными видами угроз безопасности информационных технологий и информации (угрозами интересам субъектов информационных отношений) являются:

1. Стихийные бедствия и аварии, такие как наводнение, ураган, землетрясение, пожар и др.

2. Последствия ошибок проектирования и разработки компонентов информационных технологий, включая аппаратное обеспечение, технологии обработки информации, программы, структуры данных и другие.

3. Ошибки эксплуатации, которые могут происходить со стороны пользователей, операторов и другого персонала.

4. Преднамеренные действия нарушителей и злоумышленников, включая обиженных лиц, преступников, шпионов, диверсантов и др.

1. **Характеристика угроз**

**Угрозы безопасности можно классифицировать по различным признакам:**

1. ***По результатам акции:***

- Угроза утечки информации.

- Угроза модификации информации.

- Угроза утраты информации.

2. ***По нарушению свойств информации:***

- Угроза нарушения конфиденциальности обрабатываемой информации.

- Угроза нарушения целостности обрабатываемой информации.

- Угроза нарушения работоспособности системы, также известная как угроза доступности.

3. ***По природе возникновения:***

- Естественные угрозы, вызванные объективными физическими процессами или стихийными природными явлениями.

- Искусственные угрозы, вызванные действиями человека. Искусственные угрозы могут быть непреднамеренными (случайными) или преднамеренными (умышленными). Непреднамеренные угрозы могут быть вызваны ошибками в проектировании системы, программном обеспечении, а также действиями персонала. Преднамеренные угрозы связаны с корыстными мотивами людей, таких как злоумышленники.

Эта информация предоставляет обзор угроз безопасности информации и классификацию этих угроз по различным признакам.

1. **Наиболее распространенными угрозами безопасности информации за последние 5 лет были следующие:**

* ***Кибератаки и хакерские атаки***: За последние годы наблюдается увеличение в числе кибератак, включая атаки на корпорации, правительства и индивидуальных пользователей. Эти атаки могут варьироваться от DDoS-атак (атаки на доступность) до взлома систем и кражи конфиденциальной информации.
* ***Распространение вредоносных программ***: Вирусы, троянские кони и рансомвар стали более сложными и опасными. Они могут заражать компьютеры и сети, шифровать данные и требовать выкуп за их восстановление.
* ***Социальная инженерия***: Злоумышленники все чаще используют методы манипуляции и обмана людей для получения доступа к конфиденциальным данным или системам. Это может включать в себя фишинговые письма, обман сотрудников или другие манипуляции.
* ***Утечки данных***: Утечки конфиденциальных данных стали частым явлением. Компании и организации теряют данные клиентов из-за взломов или ошибок в безопасности.
* ***Недостатки в безопасности оборудования и программного обеспечения:*** Обнаруживаются уязвимости в аппаратных средствах, операционных системах и программном обеспечении, которые могут использоваться злоумышленниками для атак.
* ***Сетевые атаки на Интернет вещей (IoT):*** С увеличением числа устройств, подключенных к Интернету, стали возможными атаки на устройства IoT, что может привести к утечке личной информации или даже к контролю над устройствами.
* Атаки на облачные сервисы: За последние годы множество организаций перешли на облачные хранилища и сервисы, что сделало их объектами интереса для злоумышленников.
* ***Криптовалютные атаки:*** С увеличением популярности криптовалют такие атаки, как криптомайнинг, стали приоритетом для злоумышленников.
* ***Угрозы с целью разрушения:*** В некоторых случаях, атаки на критическую инфраструктуру, такую как энергетические системы и транспортные сети, становятся все более распространенными.
* ***Утечки персональной информации:*** Сбои в безопасности сайтов и приложений могут привести к утечке личных данных пользователей, включая их имена, адреса и данные кредитных карт.

Эти угрозы представляют серьезные вызовы для безопасности информации и требуют постоянного совершенствования мер безопасности и бдительности со стороны организаций и пользователей.

1. **Типы атак**
2. ***Кибератаки и хакерские атаки***

DDoS-атаки: В этом типе атак используются инструменты, такие как ботнеты, для организации множественных запросов к серверам и сетям. Для защиты от DDoS-атак рекомендуется использовать специализированные средства фильтрации трафика и мониторинга сети.

Взлом аккаунтов: Атаки на аккаунты могут быть проведены с помощью брутфорс-атак, когда злоумышленники пытаются перебрать пароли, или через перехват сессий. Для обеспечения безопасности следует использовать множественную аутентификацию (2FA) и сложные пароли.

1. ***Распространение вредоносных программ:***

Вирусы и троянские кони: Злоумышленники могут распространять вирусы и троянские кони через зараженные вложения электронных писем или подделанные загрузки. Антивирусное программное обеспечение и обновления безопасности помогут защитить систему.

Рансомвар: Для защиты от рансомвара рекомендуется регулярно создавать резервные копии данных, избегать непроверенных вложений и использовать антивирусное программное обеспечение.

1. ***Социальная инженерия:***

Фишинговые атаки: Для предотвращения фишинговых атак следует обучать сотрудников распознавать подозрительные сообщения, использовать фильтры спама и дважды проверять ссылки и вложения.

Манипуляции через общение: Важно обучать сотрудников организации правилам безопасного общения и не разглашать конфиденциальную информацию по телефону или электронной почте.

1. ***Утечки данных:***

Уязвимости в программном обеспечении: Постоянное обновление программного обеспечения и регулярное сканирование на наличие уязвимостей помогут уменьшить риски утечки данных.

Недостатки в безопасности оборудования и программного обеспечения:

Эксплуатация уязвимостей: Регулярные патчи и обновления безопасности помогут устранить известные уязвимости и укрепить безопасность системы.

1. ***Сетевые атаки на Интернет вещей (IoT):***

Брутфорс аутентификаци Для защиты устройств IoT следует использовать уникальные и сложные пароли, а также обновлять прошивки для закрытия известных уязвимостей.

1. ***Атаки на облачные сервисы:***

Сетевое перехватывание: Для обеспечения безопасности данных, передаваемых через облачные сервисы, рекомендуется использовать шифрование трафика и сильные пароли.

1. ***Криптовалютные атаки:***

Криптомайнинг-малварь: Защита от криптомайнинг-малвари включает в себя использование антивирусов, брандмауэров и регулярное обновление системы.

1. ***Угрозы с целью разрушения:***

Кибератаки на критическую инфраструктуру: Для защиты критической инфраструктуры необходимо использовать множественные уровни аутентификации и мониторинг сетевой активности.

1. ***Утечки персональной информации:***

Уязвимости в веб-приложениях: Для предотвращения утечек личных данных следует обеспечить безопасность веб-приложений, включая тестирование на проникновение и шифрование данных.

Обеспечение безопасности включает в себя не только технические меры, но и обучение сотрудников, регулярное обновление и мониторинг системы, а также использование лучших практик безопасности.