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

**ВВЕДЕНИЕ**

В последние пять лет мир столкнулся с резким увеличением и эволюцией цифровых технологий, что привело к появлению новых и более сложных угроз безопасности. Киберпреступники, государственные хакеры и другие злоумышленники активно используют этот контекст для разработки и реализации различных атак на организации, правительства и даже обычных граждан. Введение данной статьи представляет собой краткий обзор некоторых из наиболее распространенных угроз безопасности, которые доминировали в мире информационной безопасности за последние пять лет. Эти угрозы охватывают широкий спектр атак, от киберпреступности и социального инжиниринга до угроз, связанных с искусственным интеллектом и интернетом вещей (IoT). Понимание этих угроз и меры по их предотвращению становятся все более важными для обеспечения безопасности в цифровом мире.В последние пять лет мир столкнулся с резким увеличением и эволюцией цифровых технологий, что привело к появлению новых и более сложных угроз безопасности. Киберпреступники, государственные хакеры и другие злоумышленники активно используют этот контекст для разработки и реализации различных атак на организации, правительства и даже обычных граждан. Введение данной статьи представляет собой краткий обзор некоторых из наиболее распространенных угроз безопасности, которые доминировали в мире информационной безопасности за последние пять лет. Эти угрозы охватывают широкий спектр атак, от киберпреступности и социального инжиниринга до угроз, связанных с искусственным интеллектом и интернетом вещей (IoT). Понимание этих угроз и меры по их предотвращению становятся все более важными для обеспечения безопасности в цифровом мире.

**Фишинг (или phishing**) - это мошенническая практика, направленная на получение чувствительной информации или денег от пользователей, путем обмана их, заставляя предоставить такие данные добровольно или через маскировку под официальные запросы. Этот вид атаки может применяться к множеству пользователей, и обычно он осуществляется несколькими способами:

1. **Фишинговые письма (email phishing)**

Нападающие отправляют ложные электронные письма, которые выглядят как официальные уведомления от банков, компаний или сервисов. В письмах содержатся ссылки или вложения, при клике по которым пользователи могут быть перенаправлены на фальшивые веб-сайты, где их просят ввести личную информацию, такую как пароли, номера кредитных карт и т.д.

1. **Социальный фишинг (social engineering)**

Этот метод включает в себя манипуляции и обман, где злоумышленники могут общаться с целью по телефону, через социальные сети или лично, представляясь сотрудниками банка, службы поддержки или даже друзьями. Они могут просить о передаче личной информации или даже денег, используя обман и манипуляции.

1. **Фишинговые веб-сайты (phishing websites)**

Злоумышленники создают фальшивые веб-сайты, которые выглядят как официальные, чтобы заполучить информацию. Пользователи могут случайно попадать на эти сайты через фишинговые письма или поддельные ссылки на социальных сетях.

1. **СМС-фишинг (smishing)**

Злоумышленники отправляют мошеннические текстовые сообщения, выдающие себя за официальные уведомления или акции. Они могут содержать ссылки на вредоносные веб-сайты или просить позвонить по номеру, где ожидаются дополнительные инструкции для мошенничества.

1. **Фишинг через социальные сети (social media phishing)**

Злоумышленники могут создавать фейковые профили в социальных сетях, представляясь друзьями или представителями организаций, чтобы получить доступ к личным данным или деньгам пользователей.

1. **Фишинг через мессенджеры (messaging app phishing)**

Злоумышленники могут использовать мессенджеры для отправки ложных сообщений, в которых они могут просить о передаче денег или конфиденциальной информации.

**Фишинг** - это серьезная угроза для пользователей, и чтобы избежать попадания в ловушку, важно быть внимательными, не отвечать на подозрительные запросы и не предоставлять личную информацию без проверки подлинности источника.

**Вирусы**- это вредоносные программы, которые могут инфицировать компьютеры и выполнять различные действия без согласия пользователя. Вирусы могут привести к краже информации, рассылке спама, организации DDoS атак, или получению полного контроля над компьютером. Они могут попасть на компьютеры через электронные письма, уязвимости операционных систем и другие способы.

**DoS (Denial of Service**)- это атака, которая направлена на вывод компьютерной системы или программы из строя. Злоумышленник создает запросы, которые перегружают систему и приводят к ее отказу от обслуживания. Это может привести к перезагрузке системы или прекращению ее нормальной работы.

**Flood (Флуд или Поток/Затопление)** - это тип атаки, при котором злоумышленник отправляет большое количество запросов или пакетов на цель, перегружая ее и вызывая отказ от обслуживания. Это может включать в себя SYN Flood, ICMP Flood, и другие виды атак.

Рекомендации по защите от вирусов и DoS атак включают использование антивирусного ПО, не открывание подозрительных вложений и программ от неизвестных отправителей, а также правильную настройку межсетевых экранов (брандмауэров) для ограничения количества допустимых пакетов.

Также важно обновлять операционные системы и программное обеспечение, чтобы закрыть уязвимости, которые могут использоваться злоумышленниками для атак.

Наконец, информация о классификации вирусов и типах атак может быть найдена на указанных вами веб-ресурсах для более подробного изучения.

**Smurf (Смурф-атака)** - это атака, которая злоумышленникам позволяет использовать ошибки в реализации TCP-IP протокола для атаки. Этот вид атаки был более распространен в прошлом, когда TCP-IP был новым протоколом, и содержал ошибки, позволяющие подменять IP-адреса. Этот вид атаки включает в себя TCP Smurf, UDP Smurf и ICMP Smurf, в зависимости от типа пакетов, используемых для атаки. Рекомендации по защите от него включают в себя использование коммутаторов Cisco и других средств защиты, а также блокирование широковещательных запросов.

**Ping-of-Death (Jolt, SSPing)** - это атака, при которой злоумышленник отправляет жертве фрагментированный ICMP пакет с очень большим размером (64 кБ), что может вызвать зависание или сбой старых версий операционных систем, таких как Windows 95. Рекомендация по защите - обновление операционных систем до актуальных версий.

**UDP Storm (UDP шторм)** - это атака, при которой злоумышленник использует два открытых UDP порта на жертве, чтобы создать бесконечное взаимодействие между портами и снизить производительность. Рекомендации включают в себя исключение использования сервисов, принимающих UDP пакеты, или их отрывание от внешней сети с помощью межсетевых экранов.

**UDP Bomb** - это атака, при которой злоумышленник отправляет системе UDP пакет с некорректными полями служебных данных, что может вызвать аварийное завершение системы. Рекомендация - обновление программного обеспечения.

**Land** - это атака, при которой злоумышленник отправляет пакет на определенный порт жертвы, но с адресом отправителя, равным адресу жертвы, и портом отправителя, равным порту получателя. Это может вызвать зависание системы. Рекомендация - использовать обновленное ПО и межсетевые экраны.

**Mail Bombing (Почтовая бомбежка)** - это атака, при которой на почтовый сервер жертвы отправляется большое количество почтовых сообщений с целью вывода его из строя. Это может привести к перегрузке сервера, снижению производительности и переполнению жесткого диска. Рекомендация - грамотная настройка почтового сервера.

Обратите внимание, что для обеспечения безопасности компьютерных систем также важно регулярно обновлять программное обеспечение, следить за уязвимостями и использовать средства защиты, такие как межсетевые экраны и антивирусное ПО.