**ДОБРОВОЛЬСКИЙ Е.А.**

**СОВРЕМЕННОЕ ВРЕДОНОСНОЕ ПО И СПОСОБЫ ЕГО ЛЕЧЕНИЯ**

*В данной статье рассматриваются некоторые современные угрозы в Глобальной сети Интернет и способы борьбы с ними.*

*Ключевые слова: вредоносное ПО, информационная безопасность, заражение, Интернет, лечение, антивирус.*

Перед обсуждением темы вредоносного ПО введем термин «Вредоносное ПО».

Вредоносное программное обеспечение (Вредоносное ПО) – это компьютерные программы или скрипты, разработанные с целью нанесения вреда компьютерной системе, пользователю или его данным. Вредоносное ПО может иметь различные формы, такие как вирусы, черви, троянские программы, шпионское ПО и руткиты. Это программы, которые скрываются внутри легитимного программного обеспечения и выполняют свои функции без согласия или знания пользователя. Основные цели вредоносного ПО включают кражу личной информации, вмешательство в работу компьютера или его сети, открывая доступ злоумышленникам к пользовательским данным, управление компьютером издалека для осуществления массовых атак или использование компьютера в качестве части ботнета. Вредоносное ПО представляет серьезную угрозу для информационной безопасности и может иметь разрушительные последствия для отдельных пользователей, предприятий и других организаций.

Теперь, когда вы ознакомились с основным понятием, можно приступать к нашей с вами теме.

Для начала введем перечень современного вредоносного ПО:

* Вредоносные программы-вымогатели (ransomware): это вирусы, которые зашифровывают данные на компьютере жертвы и требуют выкуп за их восстановление. Они часто распространяются через вредоносные ссылки, электронные письма или поддельные загрузки.
* Ботнеты: Ботнеты представляют собой сети зараженных компьютеров, которые контролируются киберпреступниками. Они могут использоваться для отправки спама, совершения DDoS-атак или майнинга криптовалюты.
* Троянские программы: это программа, которая маскируется под полезное приложение или файл, но на самом деле содержит вредоносный код. Они могут использоваться для получения неправомерного доступа к компьютеру, кражи личной информации или установки других вредоносных программ.
* Кейлоггеры: Кейлоггеры следят за нажатиями клавиш на компьютере и записывают введенные данные, такие как пароли, логины или банковские данные. Эти данные могут быть злоупотребены злоумышленниками.
* Фишинговые атаки: Фишинг - это метод, при котором злоумышленники пытаются получить личную информацию, такую как пароли или данные кредитных карт, путем маскировки под надежные организации или сервисы. Это может происходить через электронную почту, социальные сети или вредоносные веб-сайты.
* Adware: Adware (рекламное ПО) это вредоносная программа, которая отображает нежелательную рекламу на компьютере пользователя. Они могут проникать на компьютер через бесплатное программное обеспечение или загрузки с ненадежных источников.
* Спамеры: Спамеры генерируют и отправляют массовые нежелательные электронные письма на адреса получателей. Они могут быть использованы для рассылки рекламы, распространения вирусов или фишинговых атак.
* Банковские трояны: это вредоносный код, который нацелен на банковскую информацию и пытается получить доступ к аккаунтам и паролям пользователей. Они могут использоваться для кражи денег или конфиденциальной информации.