**УДК 004** **Информационные технологии**

***Уруджев Казимагамед Талихович,*** *магистрант,*
*ДГТУ Ростов-на-Дону, РФ*

# АТАКИ С ИСПОЛЬЗОВАНИЕМ ПРОГРАММ-ВЫМОГАТЕЛЕЙ И МЕРЫ ПО ИХ СМЯГЧЕНИЮ

**Аннотация:** В последние годы атаки программ-вымогателей стали одной из наиболее распространенных и разрушительных киберугроз. Эти вредоносные атаки включают шифрование данных или системы жертвы, при этом злоумышленник требует выкуп в обмен на ключ дешифрования. Последствия таких атак для отдельных лиц, предприятий и даже критически важной инфраструктуры были разрушительными. В этом эссе рассматривается сфера атак программ-вымогателей, исследуются их методы, последствия и, самое главное, меры, которые могут быть приняты для смягчения этих угроз.

**Ключевые слова:** атака, шифрование, информационная безопасность, данные, защита

**Annotation:** In recent years, ransomware attacks have become one of the most common and destructive cyber threats. These malicious attacks involve encrypting the victim's data or system, with the attacker demanding a ransom in exchange for the decryption key. The impact of such attacks on individuals, businesses and even critical infrastructure has been devastating. This essay examines the scope of ransomware attacks, examining their methods, consequences and, most importantly, measures that can be taken to mitigate these threats.

**Keywords:** attack, encryption, information security, data, protection.

## Введение

Методы распространения: Атаки программ-вымогателей обычно

начинаются с заражения системы или сети жертвы. Распространенные методы распространения включают фишинговые электронные письма, вредоносные вложения, скомпрометированные веб-сайты и использование уязвимостей программного обеспечения. В некоторых случаях злоумышленники могут использовать методы социальной инженерии, чтобы обманом заставить пользователей загрузить вредоносное программное обеспечение [1].

Шифрование и вымогательство: Оказавшись внутри системы, программа-вымогатель шифрует критически важные файлы и данные, делая их недоступными для жертвы. Затем злоумышленники требуют выкуп, часто в криптовалюте, в обмен на ключ дешифрования. Жертвы сталкиваются с трудным выбором: заплатить выкуп и надеяться на ключ расшифровки или отказаться от оплаты и рискнуть потерять свои данные [2].

Последствия успешной атаки программ-вымогателей серьезны. Предприятия могут понести финансовые потери, нанести ущерб своей репутации и нести юридическую ответственность. Физические лица могут потерять важные личные данные, включая семейные фотографии и документы. Более того, критически важная инфраструктура, такая как больницы, электросети и правительственные учреждения, может быть парализована, что ставит под угрозу жизни и национальную безопасность.

**Основная часть**

Меры по смягчению атак программ-вымогателей, представлены следующим образом:

Регулярное резервное копирование данных: Одной из наиболее эффективных мер по предотвращению атак программ-вымогателей является регулярное резервное копирование данных. Резервное копирование данных в автономное или облачное хранилище гарантирует, что даже если данные зашифрованы, их можно восстановить без уплаты выкупа.

Обучение пользователей: Программы-вымогатели часто проникают в системы по ошибке пользователя или по его неосведомленности. Регулярное информирование сотрудников и отдельных лиц об опасностях фишинговых

писем, подозрительных загрузок и социальной инженерии может значительно снизить риск заражения [1; 2].

Обновление и внесение исправлений: Поддержание программного обеспечения, операционных систем и приложений в актуальном состоянии имеет решающее значение. Многие атаки программ-вымогателей используют известные уязвимости, которые можно было бы исправить. Важно регулярно применять обновления и исправления безопасности.

Внедрение программного обеспечения безопасности: Использование надежного антивирусного и вредоносного программного обеспечения позволяет обнаруживать и блокировать программы-вымогатели до того, как они заразят систему. Системы обнаружения вторжений (IDS) и системы предотвращения вторжений (IPS) также могут быть эффективны при выявлении вредоносной активности.

Сегментация сети: Разделение сети на сегменты с ограниченным доступом может помочь сдержать распространение программ-вымогателей, если одна часть сети скомпрометирована. Это не позволяет злоумышленникам перемещаться в стороны и шифровать всю сеть [3].

План реагирования на инциденты: Наличие четко определенного плана реагирования на инциденты имеет решающее значение. Этот план должен включать шаги по изоляции зараженных систем, обращению в правоохранительные органы и общению с заинтересованными сторонами.

Юридические и этические соображения: Организации и частные лица должны учитывать юридические и этические последствия выплаты выкупа. Выплата выкупа может стимулировать злоумышленников и не может гарантировать безопасный возврат данных.

Сотрудничество и обмен информацией: Обмен информацией об угрозах и сотрудничество с другими организациями и экспертами по безопасности могут помочь в понимании последних угроз программ-вымогателей и разработке эффективных контрмер.

**Заключение**

Атаки программ-вымогателей продолжают становиться все более изощренными и масштабными, представляя значительную угрозу как для отдельных лиц, так и для организаций. Внедрение надежных мер кибербезопасности и формирование культуры осведомленности являются важнейшими шагами в противодействии этим атакам. Регулярно создавая резервные копии данных, обучая пользователей, поддерживая актуальное программное обеспечение и следуя хорошо структурированному плану реагирования на инциденты, отдельные лица и организации могут снизить риск стать жертвами программ-вымогателей. Кроме того, важно, чтобы правительства, правоохранительные органы и эксперты по кибербезопасности работали сообща для отслеживания и задержания злоумышленников-вымогателей, что в конечном итоге сделает киберпространство более безопасной средой для всех.

**Библиографический список:**

1. Галатенко, В.А. Стандарты информационной безопасности. Интернет-университет информационных технологий. ИНТУИТ.ру, 2005.

2. Шаньгин, В.Ф. Защита компьютерной информации. Эффективные методы и средства. М.: ДМК Пресс, 2008.

3. Щербаков, А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. М.: Книжный мир, 2009.