***ISBN** 978-9975-180-04-7, DOI: https://doi.org/10.53486/sstc.v2*

DOI: https://doi.org/10.53486/sstc.v2.33
CZU: 004.056.57

ИСТОРИЯ РАЗВИТИЯ ПРОГРАММНЫХ ЗЛОУПОТРЕБЛЕНИЙ

NICULIN EGOR, student, Specialitatea: TI
Academia de Studii Economice din Moldova
Str. Bănulescu Bodoni 59, Republica Moldova, mun.Chișinău
Emaill: niculin.egor@ase.md

Abstract. *The report "The history of software malware development" describes how viruses have evolved and analyses the effectiveness of measures to protect against them. Viruses and other malware are a serious problem in today's IT world and pose a threat to users and companies. The study examined various methods of encrypting data. Security measures and measures to prevent the introduction of malicious code were analyzed. The results of the study showed that viruses are constantly evolving, making them more difficult to combat. The report's conclusions and recommendations focus on the use of a set of protection measures.*

Keywords*: software abuse, encryption, ransomware, protection*

JEL CLASSIFICATION: O30

Программные злопотребления, или компьютерные вирусы, являются проблемой, которая существует практически с момента появления первых компьютеров. Некоторые из первых компьютерных вирусов появились в 1970-х годах, но они были довольно простыми и не представляли большой угрозы. С развитием компьютерной технологии в 1980-х годах появились более сложные вирусы, которые могли наносить серьезный вред компьютерным системам. В 1990-х годах появилась новая угроза в виде червей и троянов. С развитием Интернета в начале 2000-х годов появились новые угрозы, такие как фишинг и фарминг. В настоящее время программные злоупотребления остаются серьезной угрозой для компьютерных систем и информационной безопасности в целом. Одной из наиболее опасных форм программных злоупотреблений являются рансомвары, которые захватывают контроль над компьютером или сетью и требуют выкуп за возврат данных или доступа. Целью данного исследования является описание методов развития вирусов и анализ эффективности мер защиты от них.

В ходе исследования были проанализированы данные о развитии вирусов с момента их появления до настоящего времени. Были изучены различные методы шифрования данных, используемые вредоносными программами, а также способы требования выкупа. Были проанализированы средства защиты от вирусов, такие как антивирусные программы, бэкапы данных и меры предотвращения внедрения вредоносного кода.

Программные злоупотребления появились с появлением первых компьютеров и с тех пор развивались и становились все более сложными и опасными. В первые годы компьютеров вирусы были простыми программами, которые просто копировали себя на другие компьютеры. Однако в течение последних десятилетий программные злоупотребления стали гораздо сложнее и могут наносить серьезный ущерб как компьютерам, так и людям. Можно выделить несколько этапов развития компьютерных и программных злоупотреблений:

Этап 1: Эксперименты и игры (1960-е - начало 1980-х)

Первые компьютерные злоупотребления появились в начале 1960-х годов и были созданы для обучения студентов программированию. В этот период программисты создавали зловредные программы и игры, такие как "The Colossal Cave Adventure" и "Eliza". Эти программы были неопасными и не представляли угрозы для безопасности.

Этап 2: Вирусы (середина 1980-х - конец 1990-х)

***ISBN** 978-9975-180-04-7, DOI: https://doi.org/10.53486/sstc.v2*

В середине 1980-х годов был создан первый компьютерный вирус - Brain. Вирусы - это зловредные программы, которые могут копировать себя и распространяться через компьютерные сети. В этот период было создано множество вирусов, которые вызывали сбои в работе компьютеров и повреждали файлы. В ответ на это появилось антивирусное программное обеспечение.

Этап 3: Интернет-черви (1990-е - начало 2000-х)

В конце 1990-х годов появился первый интернет-червь - "Morris worm". Эти зловредные программы использовали уязвимости в операционных системах и программном обеспечении, чтобы распространяться через интернет и заражать компьютеры. Этот период также характеризовался появлением первых троянских программ - зловредных программ, которые скрываются внутри полезного программного обеспечения и выполняют вредоносные функции без ведома пользователя.

Этап 4: Фишинг и шпионское ПО (2000-е годы)

В начале 2000-х годов появились новые типы злоупотреблений, такие как фишинг - попытки получить личную информацию пользователя (такую как пароли и номера кредитных карт) путем мошенничества, и шпионское ПО - зловредные программы, которые шпионят за пользователем и могут перехватывать его личные данные.

Этап 5: Распространение вредоносного ПО через социальные сети (с 2010-х годов)

С развитием социальных сетей появилась новая возможность для распространения вредоносных программ. Киберпреступники могут использовать социальные сети для отправки спама, распространения фишинговых сообщений, а также для заражения компьютеров пользователей вредоносными программами. В этот период также появилась новая форма компьютерных злоупотреблений - рансомвары (вымогательство информации).

Существует множество различных типов программных злоупотреблений и каждый из этих типов имеет свои характеристики и методы работы, которые могут быть использованы для атак на компьютеры и сети.

Бывают несколько методов защиты от программных злоупотреблений. Некоторые из них включают:

1. Антивирусное программное обеспечение - это программное обеспечение, которое защищает компьютеры от вирусов и других типов программных злоупотреблений. Они могут быть установлены на компьютер или использоваться в виде облачного сервиса.
2. Файрволы - это программное обеспечение или аппаратное обеспечение, которое защищает компьютеры и сети от несанкционированного доступа. Файрволы могут использоваться как отдельно, так и вместе с антивирусным программным обеспечением.
3. Обновления программного обеспечения - обновления программного обеспечения могут исправлять уязвимости, которые могут быть использованы для атак на компьютеры и сети.
4. Бэкапы данных - создание регулярных копий важных данных является хорошей мерой защиты от программных злоупотреблений, особенно от вымогателей (ransomware), которые могут заблокировать доступ к данным и требовать выкупа.
5. Обучение пользователей - одним из ключевых методов защиты от программных злоупотреблений является обучение пользователей, как избегать небезопасных действий, например, открытие подозрительных вложений в электронной почте или установка ненадежного программного обеспечения.

Программные злопотребления, такие как вирусы, черви, троянские программы, рекламное ПО (adware), шпионское ПО (spyware), вымогательство (ransomware) и другие, стали серьезной угрозой для безопасности в информационных технологиях. Они развивались с появлением первых компьютеров и стали более сложными и опасными. Для защиты от программных злопотреблений могут использоваться различные методы, включая антивирусное программное обеспечение, файрволы, обновления программного обеспечения, бэкапы данных и обучение пользователей. Однако в связи с быстрым развитием программных

***ISBN** 978-9975-180-04-7, DOI: https://doi.org/10.53486/sstc.v2*

злопотреблений и появлением новых методов атак, защита от них остается актуальной и требует постоянного совершенствования и обновления.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

1. **K. Monappa (2019).** Анализ вредоносных программ. ISBN: 978-5-97060-700-8
2. **Jason Andress (2019).** FOUNDATIONS OF INFORMATION SECURITY A Straightforward Introduction. No starch press. ISBN-10: 1-7185-0004-1 ISBN-13: 978-1-7185-0004-4.
3. **T. Minarik (2019).** 11th International Conference on Cyber Conflict: Silent Battle. ISBN: 978-9949-9904-5-0.
4. **Bruce Middleton (2017).** A History of Cyber Attacks. ISBN: 978-1498785860
5. **Paul Rosenzweig (2013).** Thinking about Cybersecurity: From Cyber Crime to Cyber Warfare. The Great Courses. ISBN: 9781470381844.

Coordonator ştiinţific:OHRIMENCO Serghei, dr. hab., prof. univ.
Academia de Studii Economice din Moldova
Str. Bănulescu Bodoni 59, Republica Moldova, mun.Chișinău
e-mail: osa@ase.md