Перевертун Д.Р. Вирусы программного обеспечения и меры обеспечения безопасности // Международный журнал информационных технологий и энергоэффективности.– 2024. – Т. 9 № 4(42) с. 84–88

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

ВИРУСЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Перевертун Д.Р.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: danilaperevertun@gmail.com

В статье рассматриваются современные вызовы в области кибербезопасности, связанные с развитием вирусов программного обеспечения и методов их распространения. Освещаются основные типы вирусов и меры защиты, направленные на обеспечение безопасности информационных систем. Отдельное внимание уделяется современным технологиям и подходам в области обеспечения кибербезопасности, включая использование искусственного интеллекта и машинного обучения для предотвращения кибератак. Анализируются текущие и будущие перспективы развития в контексте международного сотрудничества и стандартизации в сфере кибербезопасности.

Ключевые слова: Кибербезопасность, вирусы программного обеспечения, защита информационных систем, искусственный интеллект, машинное обучение, международное сотрудничество, стандартизация в области кибербезопасности, троянские программы, компьютерные черви, шпионское ПО, рекламное ПО, вирусы-вымогатели.

SOFTWARE VIRUSES AND SECURITY MEASURES

Perevertun D.R.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: danilaperevertun@gmail.com

The article examines modern challenges in the field of cybersecurity related to the development of software viruses and methods of their distribution. The main types of viruses and protection measures aimed at ensuring the security of information systems are highlighted. Special attention is paid to modern technologies and approaches in the field of cybersecurity, including the use of artificial intelligence and machine learning to prevent cyber attacks. The current and future development prospects in the context of international cooperation and standardization in the field of cybersecurity are analyzed.

Keywords: Cybersecurity, software viruses, protection of information systems, artificial intelligence, machine learning, international cooperation, standardization in the field of cybersecurity, Trojans, computer worms, spyware, adware, ransomware.

В современном мире, где цифровые технологии проникают в каждую сферу нашей жизни, вопросы кибербезопасности становятся все более актуальными. Вирусы программного обеспечения – одна из главных угроз, стоящих перед пользователями и организациями. Эти малициозные программы способны не только нарушить нормальную работу компьютерных систем, но и привести к значительным финансовым потерям, утечке конфиденциальной

информации и даже к разрушению критически важной инфраструктуры. В данной статье рассматриваются основные типы вирусов программного обеспечения и современные подходы к обеспечению кибербезопасности, направленные на защиту информационных систем от этих угроз.

Вирусы программного обеспечения могут быть классифицированы по различным признакам, включая способ распространения, тип наносимого вреда, и тактику скрытности. Среди наиболее распространенных типов можно выделить троянские программы, черви, шпионское ПО, рекламное ПО и вирусы-вымогатели. Каждый из этих типов имеет свои особенности и требует применения специфических мер безопасности.

На сегодняшний день каждый аспект нашей жизни все больше зависит от цифровых технологий, вопросы кибербезопасности становятся критически важными. Вирусы программного обеспечения представляют собой одну из самых значимых угроз для пользователей и организаций, способных не только нарушить нормальную работу компьютерных систем, но и привести к значительным финансовым потерям, утечке конфиденциальной информации и даже к разрушению критически важной инфраструктуры.[4]

Вирусы программного обеспечения охватывают широкий спектр малициозных программ, каждая из которых имеет свои уникальные характеристики и методы распространения. Некоторые из них маскируются под легитимное программное обеспечение, тем самым обманывая пользователей и получая доступ к их системам. Другие способны самостоятельно распространяться через сетевые соединения, нанося вред не только отдельным пользователям, но и целым сетям. Также существуют программы, специализирующиеся на сборе информации без ведома пользователя, что представляет серьезную угрозу конфиденциальности данных.

Защита от таких угроз требует комплексного подхода, который включает в себя использование передовых технологий и строгих организационных мер. Современные технологии обеспечения безопасности способны выявлять и блокировать вредоносное ПО, еще до того, как оно сможет нанести ущерб. Вместе с тем, организационные меры, такие как разработка и внедрение политик безопасности, регулярные аудиты и обучение персонала, играют не менее важную роль в обеспечении защиты информационных систем.

Однако с развитием технологий эволюционируют и угрозы кибербезопасности. В ответ на это, разрабатываются новые методы защиты, включая применение машинного обучения для обнаружения и предотвращения атак, усиление защиты облачных и распределенных систем, а также разработку международных стандартов кибербезопасности.

Защита в цифровой среде требует комплексного подхода, который включает в себя как технические средства, так и организационные меры. Среди ключевых технологий – антивирусное ПО, межсетевые экраны, системы обнаружения и предотвращения вторжений, а также средства шифрования данных.[3] Организационные меры включают в себя разработку и внедрение политик информационной безопасности, проведение регулярных аудитов и тренингов для сотрудников.

Обеспечение безопасности в цифровом пространстве — это непрерывный процесс, требующий применения многоуровневых стратегий защиты, включающих в себя как передовые технологии, так и строгие организационные меры. В основе защиты лежит идея создания надежного барьера, который сможет выявлять, предотвращать и минимизировать

вред от малициозных программ, обеспечивая тем самым целостность и конфиденциальность пользовательских данных.

Современные технологии обеспечения безопасности включают в себя разработку и внедрение программного обеспечения, способного анализировать поведение приложений и трафика в реальном времени, выявлять подозрительные действия и блокировать их до того, как они смогут нанести ущерб. Эти технологии постоянно совершенствуются, чтобы противостоять новым и более изощренным угрозам, что требует регулярных обновлений и адаптации к меняющимся условиям киберпространства.

Однако технологические средства защиты не могут обеспечить полную безопасность без должного уровня организационной подготовки. Важным аспектом является разработка и внедрение комплексной политики безопасности, которая включает в себя не только технические аспекты, но и обучение персонала основам кибергигиены, а также проведение регулярных аудитов безопасности. Эти меры позволяют не только своевременно выявлять и устранять уязвимости, но и повышать осведомленность сотрудников о потенциальных угрозах и способах их предотвращения.

В контексте быстро меняющегося цифрового мира, одной из ключевых задач является обеспечение адаптивности и гибкости систем безопасности. Это достигается за счет внедрения новейших технологических решений, таких как искусственный интеллект и машинное обучение, которые способны анализировать большие объемы данных и выявлять сложные угрозы, еще до того как они смогут проявить себя.[2]

Таким образом, обеспечение кибербезопасности требует комплексного подхода, сочетающего в себе использование передовых технологий, строгую организационную дисциплину и постоянное обновление знаний и навыков. Важно понимать, что защита информационных систем — это непрерывный процесс, который требует постоянного внимания и адаптации к постоянно меняющимся условиям и угрозам в киберпространстве.

С развитием технологий эволюционируют и угрозы кибербезопасности. В последние годы особенно актуальными стали атаки с использованием искусственного интеллекта, целенаправленные атаки типа "нулевой день" и атаки на цепочки поставок. В ответ на эти вызовы разрабатываются новые методы защиты, включая применение машинного обучения для обнаружения и предотвращения атак, усиление защиты облачных и распределенных систем, а также разработку стандартов и нормативов кибербезопасности на международном уровне.

В сфере кибербезопасности современные вызовы постоянно эволюционируют, требуя от специалистов не только внимания к текущим угрозам, но и антиципации будущих вызовов. Развитие технологий, таких как искусственный интеллект (ИИ) и машинное обучение, открывает новые горизонты для защиты информационных систем, однако в то же время создает возможности для более изощренных атак. Целенаправленные атаки типа "нулевой день", эксплуатирующие уязвимости, о которых еще не известно производителям программного обеспечения, ставят под угрозу даже самые защищенные системы.[7] Атаки на цепочки поставок, когда злоумышленники используют уязвимости в одном из звеньев для доступа к данным целого ряда организаций, становятся все более распространенными.

В ответ на эти вызовы, область кибербезопасности постоянно развивается, стремясь предвидеть и нейтрализовать потенциальные угрозы. Использование ИИ и машинного обучения для обнаружения и предотвращения атак становится нормой, позволяя

анализировать большие объемы данных в реальном времени и выявлять угрозы, которые могут оставаться незамеченными для традиционных систем безопасности.[6] Разработка и внедрение новых стандартов и нормативов на международном уровне также играет ключевую роль в укреплении общей защищенности цифрового пространства, позволяя координировать усилия различных стран и организаций в борьбе с киберпреступностью.

Важной перспективой в области кибербезопасности является развитие облачных и распределенных систем защиты. Эти технологии обеспечивают гибкость и масштабируемость решений для защиты данных, позволяя быстро адаптироваться к изменяющимся условиям и требованиям безопасности.[1] Также важно уделить внимание укреплению защиты личных данных пользователей, в контексте усиления законодательства в области защиты персональных данных по всему миру.

Однако прогресс в технологиях и методах защиты неизбежно сопровождается развитием новых методов атак. Поэтому в будущем сфера кибербезопасности будет продолжать развиваться, сталкиваясь с новыми вызовами и находя решения для обеспечения безопасности в постоянно меняющемся цифровом мире.[5] Такой подход требует не только технологических инноваций, но и глубокого понимания потенциальных угроз, а также сотрудничества между государствами, частным сектором и международными организациями.

В заключении можно отметить, что кибербезопасность в современном цифровом мире становится все более значимым и сложным аспектом, требующим непрерывного внимания и развития. Угрозы, исходящие от вирусов программного обеспечения, представляют собой серьезный вызов для индивидуальных пользователей, компаний и государственных организаций по всему миру. Многообразие и постоянное эволюционирование малициозных программ требуют от специалистов по кибербезопасности глубоких знаний, умения применять передовые технологии и разрабатывать комплексные стратегии защиты.

Применение современных технологий, таких как искусственный интеллект и машинное обучение, позволяет существенно повысить эффективность систем обнаружения и предотвращения кибератак. Однако технологические решения в одиночку не могут гарантировать полную безопасность. Важную роль играет развитие организационных мер, включая обучение персонала, разработку и внедрение политик информационной безопасности, а также проведение регулярных аудитов и тестирований на проникновение.

Сотрудничество на международном уровне и стандартизация в сфере кибербезопасности также являются ключевыми элементами в борьбе с глобальными киберугрозами. Разработка и внедрение общепризнанных стандартов и практик позволяют координировать усилия различных стран и организаций, способствуя созданию более безопасного цифрового пространства.

В перспективе, обеспечение кибербезопасности потребует от всех заинтересованных сторон адаптации к постоянно меняющейся среде угроз, развития новых подходов и технологий, а также глубокого понимания потенциальных рисков и стратегий их минимизации. Постоянное развитие в этой области не только защитит от текущих угроз, но и подготовит общество к противостоянию будущим вызовам в области кибербезопасности.

Список литературы

1. Krasov A. et al. Using mathematical forecasting methods to estimate the load on the computing power of the IoT network //The 4th International Conference on Future Networks and Distributed Systems (ICFNDS). – 2020. – С. 1-6.

2. Гельфанд А. М. и др. Интернет вещей (IoT): Угрозы безопасности и конфиденциальности//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 215-220.
3. Гельфанд А. М. и др. Исследование распределенного механизма безопасности для устройств интернета вещей с ограниченными ресурсами//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 321-326.
4. Косов Н. А. и др. Анализ методов машинного обучения для детектирования аномалий в сетевом трафике//Цифровизация образования: теоретические и прикладные исследования современной науки. – 2021. – С. 33-37.
5. Косов Н. А., Тимофеев Р. С. Сравнение методов обучения свёрточных нейронных сетей//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 526-530.
6. Косов Н.А., Мазепин П.С., Гришин Н.А. Применение нейронных сетей для автоматизации тестирования программного обеспечения //Наукосфера. – 2020. – №. 6. – С. 152-156.
7. Штеренберг С.И. Методика построения защищенных систем искусственного интеллекта для проведения электроретинографии в офтальмологии //Офтальмохирургия. – 2022. – №. 4s. – С. 51-57.

References

1. Krasov A. et al. Using mathematical forecasting methods to estimate the load on the computing power of the IoT network //The 4th International Conference on Future Networks and Distributed Systems (ICFNDS). – 2020. – pp. 1-6.
2. Gelfand A.M. et al. Internet of things (IoT): security and privacy threats//Actual problems of infotelecommunications in science and education (APINO 2021). – 2021. – pp. 215-220.
3. Gelfand A.M. et al. Investigation of a distributed security mechanism for Internet of Things devices with limited resources //Actual problems of infotelecommunications in science and education (APINO 2020). – 2020. – pp. 321-326.
4. Kosov N. A. et al. Analysis of machine learning methods for detecting anomalies in network traffic //Digitalization of education: theoretical and applied research of modern science. – 2021. – pp. 33-37.
5. Kosov N.A., Timofeev R.S. Comparison of training methods for convolutional neural networks//Actual problems of infotelecommunications in science and education (APINO 2021). – 2021. – pp. 526-530.
6. KOSOV N.A., MAZEPIN P.S., GRISHIN N.A. Application of neural networks for software testing automation //The sciencosphere. - 2020. – No. 6. – pp. 152-156.
7. Shterenberg S. I. Methods of constructing protected artificial intelligence systems for conducting electroretinography in ophthalmology //OPHTHALMOSURGERY. – 2022. – No. 4s. – pp. 51-57.