Перевертун Д.Р. Угрозы информационной безопасности: всесторонний анализ// Международный журнал информационных технологий и энергоэффективности. - 2024. – Т. 9 № 5(43) с. 104–108

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.056

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ВСЕСТОРОННИЙ АНАЛИЗ

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

Статья представляет всесторонний анализ угроз информационной безопасности, рассматривая их многообразие и динамическое развитие в современном цифровом мире. Основное внимание уделено классификации угроз, включая вредоносное ПО, атаки на уязвимости, социальную инженерию, внутренние угрозы и кибершпионаж. Помимо этого, рассмотрены методы предотвращения и противодействия угрозам, охватывающие как технические, так и организационные аспекты, включая использование искусственного интеллекта, обучение персонала, и разработку комплексных политик безопасности. В заключение представлены будущие тенденции в области информационной безопасности, подчеркивая роль инноваций и международного сотрудничества в адаптации к эволюционирующим угрозам.

Ключевые слова: Информационная безопасность, киберугрозы, вредоносное ПО, атаки на уязвимости, социальная инженерия, внутренние угрозы, кибершпионаж, предотвращение угроз, искусственный интеллект, международное сотрудничество, будущие тенденции.

THREATS TO INFORMATION SECURITY: A COMPREHENSIVE ANALYSIS

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 presents a comprehensive analysis of information security threats, considering their diversity and dynamic development in the modern digital world. The main focus is on the classification of threats, including malware, vulnerability attacks, social engineering, internal threats and cyber espionage. In addition, methods of preventing and countering threats are considered, covering both technical and organizational aspects, including the use of artificial intelligence, personnel training, and the development of comprehensive security policies. In conclusion, future trends in the field of information security are presented, emphasizing the role of innovation and international cooperation in adapting to evolving threats.

Keywords: Information security, cyber threats, malware, vulnerability attacks, social engineering, internal threats, cyber espionage, threat prevention, artificial intelligence, international cooperation, future trends.

Угрозы информационной безопасности можно классифицировать на несколько основных категорий: вредоносные программы, атаки на уязвимости, социальная инженерия, внутренние угрозы и кибершпионаж. Вредоносные программы включают в себя вирусы, трояны, шпионское и рекламное ПО, которые могут привести к утечке конфиденциальной

информации, потере данных или даже полному контролю над системой. Атаки на уязвимости эксплуатируют пробелы в безопасности программного обеспечения и операционных систем. Социальная инженерия направлена на манипулирование людьми для получения доступа к закрытой информации. Внутренние угрозы исходят от сотрудников организации, которые могут нанести ущерб, имея легитимный доступ к ресурсам. Кибершпионаж охватывает деятельность, направленную на незаконное получение секретной информации с целью получения преимущества.

В контексте информационной безопасности современный цифровой ландшафт представляет собой многоуровневую систему, в которой различные угрозы переплетаются и взаимодействуют друг с другом, создавая сложную и постоянно меняющуюся картину рисков. Эти угрозы происходят не изолированно, а формируются в рамках широкого спектра действий и акторов, каждый из которых имеет свои мотивы, цели и методы.

На первом уровне находятся вредоносные программы, которые, будучи разработаны для выполнения нежелательных и часто вредоносных действий, способны внедряться в системы, оставаясь незамеченными. Их цели могут варьироваться от простого раздражения пользователей до кражи конфиденциальных данных и дестабилизации критически важной инфраструктуры.

Далее, атаки на уязвимости представляют собой сознательное использование слабых мест в программном обеспечении и системах для проникновения или нарушения их нормального функционирования. Эти уязвимости могут быть как вновь обнаруженными, так и уже известными, но не устраненными из-за различных причин, включая недостаток ресурсов или знаний.

Социальная инженерия выступает как метод манипулирования людьми для обхода традиционных мер безопасности. Эта тактика основана на использовании психологических приемов для введения в заблуждение и получения несанкционированного доступа к информации или системам.

Внутренние угрозы, исходящие от самих сотрудников организации, могут быть как непреднамеренными, так и умышленными. Непреднамеренные угрозы часто связаны с недостаточным пониманием или игнорированием политик безопасности, в то время как умышленные действия могут включать в себя кражу данных, саботаж или другие вредоносные действия.[4]

Наконец, кибершпионаж, используемый государственными и негосударственными акторами для получения конфиденциальной информации без ведома и согласия владельца, демонстрирует сложность и масштаб угроз в современном мире. Эта деятельность направлена на получение стратегического преимущества в политических, экономических или военных сферах.

Эти угрозы не являются статичными; они развиваются вместе с технологическим прогрессом, становясь всё более изощренными и трудноуловимыми. Борьба с ними требует комплексного подхода, включающего технологические, организационные и образовательные меры, а также постоянное сотрудничество между организациями и государствами.

Для обеспечения информационной безопасности используются комплексные меры, включающие как технические, так и организационные аспекты. К техническим мерам относятся использование антивирусного и антиспамного ПО, файерволов, систем обнаружения и предотвращения вторжений, а также регулярное обновление ПО для

устранения уязвимостей.[2] Организанизационные меры включают разработку и внедрение политик информационной безопасности, обучение персонала принципам безопасного обращения с информацией, регулярные аудиты и проверки безопасности для выявления и устранения потенциальных уязвимостей. Важным элементом является также создание системы реагирования на инциденты, что позволяет оперативно принимать меры при обнаружении угрозы.

В области информационной безопасности методы предотвращения угроз объединяются в комплексный подход, включающий в себя разнообразные стратегии и технологии, направленные на защиту информационных систем от широкого спектра угроз. Этот подход требует интеграции технических средств, организационных мер и образовательных программ для создания эффективной обороны против внешних и внутренних атак.

На техническом уровне внедрение современных антивирусных программ и межсетевых экранов служит первой линией защиты, блокируя вредоносное ПО и нежелательный сетевой трафик. Дополнительно, системы обнаружения и предотвращения вторжений анализируют сетевой трафик в реальном времени, выявляя и нейтрализуя потенциальные угрозы.[7] Регулярное обновление программного обеспечения и операционных систем устраняет известные уязвимости, снижая риск успешных атак.

Организационные меры предполагают разработку и внедрение политик информационной безопасности, которые определяют стандарты поведения и процедуры для защиты информационных ресурсов. Эти политики охватывают такие аспекты, как управление доступом, шифрование данных, физическая безопасность и реагирование на инциденты. Важной частью организационных мер является также разработка плана реагирования на инциденты, который обеспечивает быструю и организованную реакцию на угрозы и атаки, с целью минимизации ущерба и восстановления нормальной работы систем.

Образовательные программы играют ключевую роль в повышении осведомленности сотрудников об угрозах информационной безопасности и методах их предотвращения. Регулярное обучение и тренировки помогают сотрудникам осознать значение безопасного поведения в интернете, правила создания надежных паролей, опасности социальной инженерии и другие аспекты, критически важные для обеспечения безопасности организации.[5]

Таким образом, методы предотвращения угроз в области информационной безопасности представляют собой сложную и многоуровневую систему, требующую не только применения передовых технологий, но и активного участия всех сотрудников организации, а также постоянного обновления знаний и навыков в соответствии с меняющейся средой угроз.

С учетом постоянного развития технологий и изменения ландшафта угроз, прогнозирование будущих тенденций в информационной безопасности становится ключевым для предотвращения потенциальных атак. Ожидается, что в ближайшем будущем увеличится акцент на разработку и внедрение искусственного интеллекта и машинного обучения для обнаружения и нейтрализации киберугроз в реальном времени. Также предвидится рост важности защиты устройств Интернета вещей, которые становятся все более распространенными и, как следствие, могут служить дополнительными точками входа для кибератак.[3] В связи с этим, комплексная защита, включающая усиленное шифрование и аутентификацию, станет еще более важной. Кроме того, важность приобретает разработка

международных стандартов и правил поведения в киберпространстве для снижения риска масштабных киберконфликтов.

В сфере информационной безопасности постоянное развитие технологий и эволюция угроз определяют динамичный характер будущих тенденций. Адаптация к этим изменениям требует от специалистов не только реагирования на существующие вызовы, но и предвидения возможных угроз, что ведет к инновациям в методах защиты и стратегиях обеспечения безопасности.

Одним из ключевых направлений является интеграция искусственного интеллекта (ИИ) и машинного обучения в системы безопасности. Эти технологии обладают потенциалом радикально трансформировать способы обнаружения и нейтрализации киберугроз благодаря их способности анализировать большие объемы данных в реальном времени, выявляя сложные и скрытые паттерны поведения, которые могут указывать на кибератаку.[6] Эта способность делает ИИ мощным инструментом в прогнозировании и предотвращении угроз до того, как они смогут нанести ущерб.

Также значительное внимание уделяется защите устройств Интернета вещей (IoT), число которых стремительно растет. Устройства IoT часто характеризуются недостаточным уровнем безопасности, что делает их уязвимыми для атак. В связи с этим, разработка и внедрение усовершенствованных стандартов безопасности и протоколов аутентификации становятся приоритетом для обеспечения безопасности данных и функционирования этих устройств.

Помимо технологических аспектов, ожидается усиление внимания к правовым и этическим нормам в сфере кибербезопасности. С учетом глобального характера интернета и трансграничной природы киберугроз, международное сотрудничество и разработка универсальных правовых рамок становятся критически важными для эффективного противодействия киберпреступности и защиты прав индивидов в цифровом пространстве.[1]

Наконец, учитывая растущую зависимость общества от цифровых технологий, осознание роли человеческого фактора в обеспечении информационной безопасности становится все более значимым. Это подчеркивает необходимость комплексного подхода, включающего обучение и повышение осведомленности среди пользователей о потенциальных угрозах и методах их предотвращения.

В заключение данной статьи подчеркивается, что информационная безопасность в современном мире остается одной из наиболее критических и динамично развивающихся областей. Многообразие и сложность угроз информационной безопасности требуют комплексного подхода к их предотвращению и нейтрализации, который включает в себя не только применение передовых технологий и разработку надежных технических решений, но и создание эффективной организационной культуры, направленной на защиту информации. Кроме того, особое внимание следует уделить развитию правовых и нормативных основ кибербезопасности на международном уровне, чтобы обеспечить координированное противодействие трансграничным угрозам.

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.