УДК 004.492.2

ПРОБЛЕМЫ С БЕЗОПАСНОСТЬЮ И НЕДОСТАТОК КОНФИДЕНЦИАЛЬНОСТИ В СОВРЕМЕННЫХ КОМПЬЮТЕРНЫХ СИСТЕМАХ

Клевец А.А., Резник Н., Василькова А.Н.

Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь

Научный руководитель: Потапенко Н.И. – ст. преподаватель кафедры ИПиЭ

Аннотация. С широким распространением современных компьютерных систем и технологий безопасность и конфиденциальность становятся все более важными проблемами. В этом исследовательском документе мы рассматриваем некоторые из основных проблем безопасности и конфиденциальности в современных компьютерных системах и технологиях. Мы начнем с обсуждения основных концепций безопасности и конфиденциальности и того, как они соотносятся с компьютерными системами. Затем мы исследуем некоторые из наиболее серьезных угроз безопасности и конфиденциальности в современных компьютерных системах, включая вредоносное ПО, утечку данных и кибератаки. Наконец, мы анализируем некоторые методы и технологии, используемые для смягчения этих угроз и повышения безопасности и конфиденциальности компьютерных систем.

Ключевые слова: кибербезопасность, кибератаки, DDoS-атаки, вредоносное ПО, утечка данных, киберпреступники

Введение. Безопасность и конфиденциальность всегда были важными аспектами компьютерных систем и технологий, но с распространением новых технологий и растущей зависимостью от цифровых данных и услуг они стали более важными, чем когда-либо. От персональных компьютеров до корпоративных сетей проблемы безопасности и конфиденциальности возникают на всех уровнях. В этой статье мы стремимся изучить некоторые наиболее важные проблемы безопасности и конфиденциальности в современных компьютерных системах и технологиях, а также оценить некоторые методы и технологии, используемые для их решения.

Основная часть. Термин безопасность относится к мерам, принимаемым для предотвращения несанкционированного доступа к компьютерным системам, приложениям или данным. Он включает в себя ряд методов и технологий, включая брандмауэры, системы обнаружения вторжений, контроль доступа и шифрование. Конфиденциальность, с другой стороны, относится к защите личной информации от несанкционированного доступа, использования или раскрытия. Он включает средства защиты от кражи личных данных, утечки данных и других форм киберпреступлений.

Распространенность проблем безопасности и конфиденциальности резко возросла в последние годы из-за роста киберпреступности, которая включает утечку данных, вредоносное ПО и кибератаки. По данным Ресурсного центра по краже личных данных, только в 2020 году в Соединенных Штатах произошло более 1000 утечек данных, в результате которых было раскрыто более 155 миллионов записей. Кроме того, кибератаки, такие как фишинг, программы-вымогатели и DDoS-атаки, становятся все более изощренными и широко распространенными.

В следующих разделах мы обсудим некоторые наиболее важные проблемы безопасности и конфиденциальности в современных компьютерных системах и технологиях, включая вредоносные программы, утечки данных и кибератаки.

Вредоносное ПО — это тип программного обеспечения, предназначенного для причинения вреда компьютерным системам, сетям или пользователям. Вредоносное ПО может принимать различные формы, включая вирусы, черви, трояны и шпионское ПО.

Вредоносное ПО может использоваться для кражи конфиденциальной информации, нарушения работы компьютерных систем или получения несанкционированного доступа к сетям. Во многих случаях вредоносное ПО распространяется через фишинговые электронные письма или другие методы социальной инженерии. [1]

Чтобы снизить риск вредоносных программ, компьютерные системы должны быть оснащены современным антивирусным программным обеспечением, брандмауэрами и системами обнаружения вторжений. Кроме того, пользователи должны быть обучены тому, как распознавать и избегать подозрительных электронных писем или загрузок.

Утечки данных происходят, когда важные или конфиденциальные данные становятся доступными для неавторизованных лиц. Утечки данных могут быть вызваны взломом, фишингом или внутренними угрозами. Последствия утечек данных могут быть серьезными, включая кражу личных данных, финансовые потери и ущерб репутации организации.

Чтобы снизить риск утечки данных, компьютерные системы должны иметь надежный контроль доступа, надежные механизмы аутентификации и шифрование конфиденциальных данных. Кроме того, организации должны иметь четкие политики и процедуры для обработки и сообщения об утечках данных.

Кибератака — это преднамеренная попытка поставить под угрозу безопасность компьютерных систем, сетей или устройств. Кибератаки могут принимать различные формы, такие как фишинг, вредоносные программы, атаки типа «отказ в обслуживании» или программы-вымогатели, и это лишь некоторые из них. Воздействие кибератаки может быть разрушительным, приводя к утечке данных, финансовым потерям, ущербу для репутации и даже к гибели людей. [2]

Одной из наиболее серьезных проблем в снижении риска кибератак является постоянно меняющийся характер угроз. Киберпреступники постоянно разрабатывают новые методы и способы обхода мер безопасности и получения несанкционированного доступа к компьютерным системам. Поэтому важно реализовать многоуровневую стратегию защиты, включающую различные технологии и методы обеспечения безопасности. Некоторые эффективные меры по предотвращению кибератак включают использование брандмауэров, систем обнаружения и предотвращения вторжений, а также современного антивирусного программного обеспечения. Кроме того, реализация надежных средств контроля доступа, таких как двухфакторная аутентификация, может помочь предотвратить несанкционированный доступ к критически важным системам и данным. Регулярные оценки безопасности и тестирование уязвимостей также могут помочь выявить и устранить потенциальные недостатки в компьютерных системах и сетях.

Хотя профилактические меры необходимы для снижения риска кибератак, также крайне важно иметь план реагирования на случай атаки. Хорошо спланированный и отрепетированный план реагирования на инциденты может значительно свести к минимуму воздействие кибератаки, позволяя организациям быстро и эффективно реагировать, сдерживать атаку, расследовать инцидент и восстанавливать нормальную работу. Планы реагирования на инциденты должны включать этапы коммуникации, сдерживания, анализа и восстановления. Регулярное тестирование и обновление планов реагирования на инциденты может помочь обеспечить их эффективность и актуальность перед лицом развивающихся киберугроз.

Наконец, обучение и осведомленность пользователей имеют решающее значение для предотвращения кибератак. Киберпреступники часто используют методы социальной инженерии, чтобы заставить пользователей разглашать конфиденциальную информацию или переходить по вредоносным ссылкам. Поэтому важно обучать пользователей тому, как распознавать фишинговые атаки и избегать их, как создавать надежные пароли и управлять ими, а также как сообщать о подозрительных действиях.

В целом угроза кибератак является одной из наиболее серьезных проблем безопасности и конфиденциальности, с которыми сталкиваются современные компьютерные системы и технологии. Внедряя комплексную стратегию защиты, включающую сочетание технологий

безопасности, передового опыта и обучения пользователей, организации и отдельные лица могут значительно снизить риск стать жертвой кибератаки.

Заключение. В заключение, вопросы безопасности и конфиденциальности в современных компьютерных системах и технологиях становятся все более важными и сложными. Такие угрозы, как вредоносное ПО, утечка данных и кибератаки, продолжают развиваться и становиться все более изощренными, поэтому организациям и отдельным лицам крайне важно принимать упреждающие меры для снижения этих рисков. Использование современных технологий и методов обеспечения безопасности, таких как антивирусное программное обеспечение, брандмауэры, контроль доступа и шифрование, имеет важное значение для обеспечения безопасности и конфиденциальности компьютерных систем.

В заключение в этом документе представлен обзор некоторых из наиболее важных проблем безопасности и конфиденциальности в современных компьютерных системах и технологиях. Хотя угрозы компьютерной безопасности и конфиденциальности огромны, существует множество методов и технологий, позволяющих снизить эти риски. Понимая природу этих угроз и применяя передовые методы обеспечения безопасности и конфиденциальности, организации и отдельные лица могут обеспечить безопасное и надежное использование компьютерных систем и технологий.

Список литературы

1. *Ричардсон, Крис. Microservices Patterns / Крис Ричардсон. – O'Reilly Media, 2018. – 520 с.*
2. *Ньюман, Сэм. Building Microservices / Сэм Ньюман. – O'Reilly Media, 2015. – 259 с.*

UDC 004.492.2

SECURITY AND PRIVACY ISSUES IN MODERN COMPUTER SYSTEMS AND TECHNOLOGIES

Klevets A.A., Reznik N., Vasilkova A.N.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Potapenko N.I. – senior lecturer of the Department of EPE

Annotation. With the widespread adoption of modern computer systems and technologies, security and privacy have become increasingly important concerns. In this research paper, we examine some of the main security and privacy issues in modern computer systems and technologies. We begin by discussing the fundamental concepts of security and privacy and how they relate to computer systems. We then explore some of the most significant threats to security and privacy in modern computer systems, dealing with cyber-attacks. Finally, we analyze some of the methods and technologies used to mitigate these. Finally, we analyze some of the methods and technologies used to mitigate these threats and enhance the security and privacy of computer systems.

Keywords: cyberattacks, cybersecurity, DDoS-attacks, malware, data breaches, cybercrime.