



УДК 004.056:621.39

МОДЕЛИРОВАНИЕ КИБЕРУГРОЗ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

Овезмырадова Гозель Пендыевна

преподаватель

Атаджанова Огулбагт Какагельдиевна

студентка

Институт Телекоммуникаций и информатики Туркменистана, г. Ашхабад

Аннотация. В статье рассматриваются вопросы моделирования киберугроз в современных телекоммуникационных системах. Анализируются основные типы кибератак, влияющих на функционирование сетевой инфраструктуры, включая атаки типа отказа в обслуживании, перехват данных и несанкционированный доступ к сетевым ресурсам. Особое внимание уделяется методам моделирования угроз и оценке их влияния на устойчивость и безопасность телекоммуникационных сетей. Рассматриваются подходы к построению моделей угроз, позволяющие прогнозировать возможные сценарии атак и разрабатывать эффективные механизмы защиты. Результаты исследования показывают, что применение методов моделирования позволяет повысить уровень кибербезопасности телекоммуникационных систем и обеспечить устойчивость их функционирования в условиях возрастающих угроз информационной безопасности.

Ключевые слова: телекоммуникационные системы, кибербезопасность, киберугрозы, моделирование угроз, сетевые атаки, информационная безопасность, защита сетей.

CYBER THREAT MODELING IN TELECOMMUNICATION SYSTEMS

Ovezmyradova Gozel Pendiyevena

lecturer,

Atajanova Ogulbagt Kakageldiyevna

student,

Institute of Telecommunications and informatics of Turkmenistan, Ashgabat

Abstract. The article examines cyber threat modeling in modern telecommunication systems. The main types of cyberattacks affecting network infrastructure are analyzed, including denial-of-service attacks, data interception, and unauthorized access to network resources. Particular attention is given to threat modeling methods and the assessment of their impact on the reliability and security of telecommunication networks. Approaches to constructing threat models that enable prediction of potential attack scenarios

and development of effective protection mechanisms are considered. The results demonstrate that the use of modeling techniques improves cybersecurity and enhances the stability of telecommunication systems under increasing information security threats.

Keywords: telecommunication systems, cybersecurity, cyber threats, threat modeling, network attacks, information security, network protection.

Развитие телекоммуникационных технологий и широкое распространение цифровых сетей привели к значительному увеличению объёмов передаваемой информации и расширению возможностей сетевого взаимодействия. Современные телекоммуникационные системы обеспечивают функционирование различных информационных сервисов, включая мобильную связь, интернет-коммуникации, облачные вычисления и мультимедийные платформы [1].

Одновременно с развитием сетевых технологий возрастает и количество угроз информационной безопасности. Кибератаки могут приводить к нарушению функционирования сетевых сервисов, утечке конфиденциальных данных и снижению устойчивости телекоммуникационной инфраструктуры. В связи с этим обеспечение кибербезопасности становится одной из ключевых задач при проектировании и эксплуатации сетей связи.

Для эффективного противодействия киберугрозам необходимо не только внедрение технических средств защиты, но и проведение анализа потенциальных угроз и возможных сценариев атак. Одним из наиболее эффективных инструментов для решения этой задачи является моделирование киберугроз, позволяющее исследовать поведение системы в условиях различных видов атак и оценить уровень её защищённости [2].

Моделирование угроз позволяет выявить уязвимые элементы телекоммуникационной инфраструктуры, определить вероятные точки проникновения злоумышленников и разработать эффективные методы предотвращения атак.

Целью работы является анализ методов моделирования киберугроз в телекоммуникационных системах и оценка их влияния на устойчивость и безопасность сетевой инфраструктуры.

Методология исследования

Методологическую основу исследования составляют методы анализа архитектуры телекоммуникационных сетей, математического моделирования киберугроз и сравнительной оценки эффективности механизмов защиты информации.



Анализ сетевой архитектуры включал изучение структуры телекоммуникационных систем, принципов функционирования сетевых протоколов и механизмов передачи данных. Особое внимание уделялось выявлению потенциальных уязвимостей сетевых узлов и каналов связи.

Математическое моделирование применялось для исследования различных сценариев кибератак и оценки их влияния на функционирование телекоммуникационной системы. В ходе моделирования рассматривались такие типы атак, как распределённые атаки отказа в обслуживании (DDoS), перехват сетевого трафика и попытки несанкционированного доступа к сетевым ресурсам.

Сравнительная оценка эффективности проводилась на основе анализа ключевых показателей функционирования системы. В качестве основных критериев рассматривались уровень доступности сетевых сервисов, устойчивость функционирования сети и степень защищённости информационных ресурсов.

Результаты исследования

В ходе исследования были проанализированы основные факторы, влияющие на уровень кибербезопасности телекоммуникационных систем.

К числу ключевых показателей безопасности относятся:

- уровень защищённости сетевой инфраструктуры;
- устойчивость функционирования системы при кибератаках;
- вероятность несанкционированного доступа к ресурсам сети;
- эффективность механизмов обнаружения и предотвращения атак;
- уровень доступности сетевых сервисов.

Результаты моделирования показали, что различные типы кибератак оказывают существенное влияние на функционирование телекоммуникационных систем.

Основные выявленные эффекты:

- снижение доступности сетевых сервисов при проведении атак типа DDoS;
- увеличение задержек передачи данных вследствие перегрузки сетевых узлов;
- вероятность утечки информации при перехвате сетевого трафика;
- нарушение стабильности работы сети при попытках несанкционированного доступа.

Использование методов моделирования угроз позволяет определить наиболее уязвимые элементы сети и разработать эффективные меры защиты.

Дополнительно было установлено, что внедрение современных механизмов обеспечения информационной безопасности, таких как системы обнаружения вторжений, криптографическая



защита данных и интеллектуальные алгоритмы анализа сетевого трафика, существенно повышает устойчивость телекоммуникационных систем к киберугрозам [3].

Заключение

Проведённое исследование позволило определить основные особенности моделирования киберугроз в телекоммуникационных системах.

Основные выводы исследования заключаются в следующем:

1. Киберугрозы представляют серьёзную опасность для устойчивого функционирования современных телекоммуникационных сетей.
2. Моделирование угроз является эффективным инструментом анализа уязвимостей сетевой инфраструктуры.
3. Использование моделей кибератак позволяет прогнозировать возможные сценарии нарушений безопасности и разрабатывать меры их предотвращения.
4. Внедрение комплексных механизмов защиты информации повышает уровень кибербезопасности телекоммуникационных систем.

Практическая значимость работы заключается в возможности использования полученных результатов при проектировании и модернизации телекоммуникационных сетей с целью повышения их защищённости.

Перспективы дальнейших исследований связаны с разработкой интеллектуальных систем обнаружения кибератак и применением методов машинного обучения для анализа сетевого трафика и прогнозирования угроз информационной безопасности.

Список литературы:

1. Таненбаум Э., Уэзеролл Д. Компьютерные сети. — СПб.: Питер, 2020.
2. Stallings W. Network Security Essentials. — Pearson, 2020.
3. Kurose J., Ross K. Computer Networking: A Top-Down Approach. — Pearson, 2021.
4. Cisco Systems. Cybersecurity and Network Protection. — Cisco Press, 2022.