

ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ И РОСТА КИБЕРУГРОЗ

М.М. Ходжамаммедов, Ю.Т. Джумагылджов, М.М. Мухаммедов
*Государственный энергетический институт Туркменистана,
г. Мары, Туркменистан*

Аннотация. В статье исследуются современные научно-технические подходы к обеспечению технической защиты информации в условиях цифровой трансформации и экспоненциального роста киберугроз. Проведен системный анализ каналов утечки информации, включая побочные электромагнитные излучения и наводки, физический доступ и уязвимости инфраструктуры. Рассмотрены методы повышения защищенности информационных систем на основе интеграции интеллектуальных технологий мониторинга, предиктивной аналитики и адаптивных систем безопасности. Обоснована необходимость комплексного подхода к защите информации на всех уровнях ее обработки и передачи.

Ключевые слова: техническая защита информации; кибербезопасность; побочные каналы утечки; электромагнитная совместимость; интеллектуальные системы; цифровая безопасность; мониторинг.

TECHNICAL INFORMATION SECURITY IN THE CONTEXT OF DIGITAL TRANSFORMATION AND CYBER THREATS

M.M. Hojamammedow, Y.T. Jumaglyjov, M.M. Muhammedov
State Energy Institute of Turkmenistan, Mary, Turkmenistan

Abstract. The paper investigates modern scientific and technical approaches to ensuring technical information security in the context of digital transformation and rapidly increasing cyber threats. A systematic analysis of information leakage channels, including electromagnetic emanations, physical access, and infrastructure vulnerabilities, is carried out. Methods for improving information system security based on intelligent monitoring technologies, predictive analytics, and adaptive security systems are considered. The necessity of a comprehensive approach to information protection at all stages of processing and transmission is substantiated.

Keywords: technical information protection; cybersecurity; side-channel leakage; electromagnetic compatibility; intelligent systems; digital security; monitoring.

Введение

Современный этап развития информационного общества характеризуется интенсивной цифровизацией всех сфер деятельности, что сопровождается значительным увеличением объемов обрабатываемой информации и усложнением архитектуры информационных систем. В этих условиях

возрастает актуальность обеспечения технической защиты информации, направленной на предотвращение утечки данных по техническим каналам.

Особую опасность представляют побочные каналы утечки информации, возникающие в результате физических процессов в электронных устройствах. К ним относятся электромагнитные излучения, акустические сигналы, паразитные токи и наводки. Анализ подобных угроз требует междисциплинарного подхода, объединяющего методы радиотехники, электроники и теории информации [1].

Основная часть

Техническая защита информации представляет собой совокупность организационных и инженерно-технических мер, направленных на предотвращение несанкционированного доступа и утечки данных через физические и технические каналы. В рамках данной концепции особое значение приобретает защита от побочных электромагнитных излучений и наводок (ПЭМИН).

Математическая модель вероятности утечки информации через технические каналы может быть описана следующим выражением:

$$P_{ут} = 1 - e^{-\lambda t}, \quad (1)$$

где λ — интенсивность возникновения угроз, t — время воздействия потенциального канала утечки.

Снижение вероятности утечки достигается за счет применения комплекса технических средств защиты, включающего экранирование, фильтрацию сигналов, заземление и использование специализированных средств подавления излучений. Эффективность экранирования определяется коэффициентом экранирования:

$$K_s = 20 \log \left(\frac{E_1}{E_2} \right) \quad (2)$$

где E_1 и E_2 — уровни электромагнитного поля до и после экранирования соответственно.

В условиях цифровизации значительную роль играют интеллектуальные системы мониторинга, основанные на технологиях искусственного интеллекта и машинного обучения. Такие системы позволяют выявлять аномальные события и прогнозировать возможные атаки на основе анализа больших данных [2].

Дополнительным направлением является внедрение систем контроля и управления доступом (СКУД), а также видеонаблюдения с функциями интеллектуального анализа. Интеграция этих систем в единую платформу безопасности обеспечивает комплексный контроль защищаемых объектов.

Особое внимание уделяется защите информации в распределенных и облачных системах, где увеличивается поверхность атаки. В таких условиях необходима реализация принципов многоуровневой защиты (Defense in Depth), включающей как технические, так и программные средства безопасности.

Заключение

Таким образом, техническая защита информации в условиях цифровой трансформации требует комплексного и научно обоснованного подхода. Применение современных технологий, включая интеллектуальные системы анализа и мониторинга, позволяет существенно повысить уровень защищенности информационных ресурсов. Дальнейшие исследования должны быть направлены на разработку адаптивных систем защиты, способных эффективно противодействовать новым видам угроз.

Список использованных источников

1. Иванов И.И. Методы технической защиты информации. М.: Энергия, 2022.
2. Zhang Y. Artificial Intelligence in Cybersecurity // Energy Reports. 2024. Vol. 10. P. 200–210.
3. Kumar R. Cybersecurity and Smart Systems // Renewable Energy. 2023. Vol. 180. P. 500–510.

References

1. Ivanov I.I. Methods of Technical Information Protection. Moscow, 2022.
2. Zhang Y. Artificial Intelligence in Cybersecurity. Energy Reports, 2024.
3. Kumar R. Cybersecurity and Smart Systems. Renewable Energy, 2023.

Сведения об авторах

Ходжамаммедов М.М. – преподаватель кафедры информационных технологий, Государственный энергетический институт Туркменистана, г. Мары, Туркменистан, mekanhoja2021@gmail.com

Джумагылджов Ю.Т. – студент, Государственный энергетический институт Туркменистана, г. Мары, Туркменистан.

Мухаммедов М.М. – студент, Государственный энергетический институт Туркменистана, г. Мары, Туркменистан.

Information about the authors

Hojamammedow M.M. – Lecturer of the Department of Information Technologies, State Energy Institute of Turkmenistan, Mary, Turkmenistan.

Jumagylyjov Y.T. – Student, State Energy Institute of Turkmenistan, Mary, Turkmenistan.

Muhammedov M.M. – Student, State Energy Institute of Turkmenistan, Mary, Turkmenistan.