ORES

Научно-практический электронный журнал
Оригинальные исследования (ОРИС), *ISSN 2222-0402*
www.ores.su
original-research.ru

СОВРЕМЕННЫЕ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОРПОРАТИВНЫХ СЕТЕЙ И ПРИЁМЫ БОРЬБЫ С НИМИ

Сагидова Марина Леонидовна,
кандидат технических наук
Филиал ФГАОУ ВО «Мурманский арктический университет»
(Россия, г. Апатиты)
sagidovaml@arcticsu.ru

Аннотация

Данное исследование касается тематики процессов обеспечения надежности и информационной безопасности в рамках функционирования корпоративных сетей и анализа наиболее эффективных приёмов борьбы с угрозами информационной безопасности. Цель статьи – исследование современных угроз информационной безопасности корпоративных сетей и приёмы борьбы с ними. Выделены основные угрозы информационной безопасности корпоративных сетей. Рассмотрены основные пути обеспечения информационной безопасности корпоративных сетей и приёмы борьбы с ее угрозами.

Ключевые слова: информационная безопасность, управление, исследование, угрозы, корпоративные сети, меры борьбы.

MODERN THREATS TO INFORMATION SECURITY OF CORPORATE NETWORKS AND METHODS OF COMBATING THEM

Sagidova M. L.,
Candidate of Technical Sciences
Branch of the Murmansk Arctic University
(Russia, Apatity)

ABSTRACT

This study concerns the topics of processes for ensuring information security of corporate networks and methods of combating its threats. The purpose of the article is to study modern threats to the information security of corporate networks and methods of combating them. The main threats to the information security of corporate networks are identified. The main ways to ensure information security of corporate networks and methods of combating its threats are considered.

Keywords: information security, management, research, threats, corporate networks, countermeasures.

Большинство современных систем управления компаний и предприятий являются по сути системами распределенной информации в аспекте организационных, управленческих, финансовых и прочих данных [1]. Фактически такие системы реализуются по принципу корпоративных систем информации и данных, которые активно используются и обрабатываются в их корпоративных сетях и системах. Обрабатываемая в корпоративных сетях информация содержит целый ряд важнейших данных в отношении, как управленческих и организационных процессах компаний, так и про их финансовые операции и данные. Сохранение безопасности такой информации весьма важно для обеспечения устойчивой и стабильной деятельности компании и предприятий в условиях наличия большого количества угроз и противозаконных действий [3]. Именно поэтому актуальным является исследование локальных корпоративных сетей в аспекте борьбы угроз их информационной безопасности.

Цель статьи – исследование современные угрозы информационной безопасности корпоративных сетей и приёмы борьбы с ними.

Широкое внедрение информационных технологий в управлении деятельности компаний и предприятий вызывает серьезные опасения, связанные с доверием, рисками и безопасностью. С другой стороны, идея доверия к технологиям информационных технологий предполагает уверенность пользователей и вовлеченных сторон в надежности, честности и этичности применения таких систем. С одной стороны, риски технологий информационных технологий включают возможные негативные последствия и неопределенности, связанные с алгоритмами и системами борьбы с угрозами их сохранности.

Современный этап развития процессов обеспечения информационной безопасности связан с реализацией стандартов ее регулирования на мировом уровне и в пределах отдельных стран– рис. 1 [3].

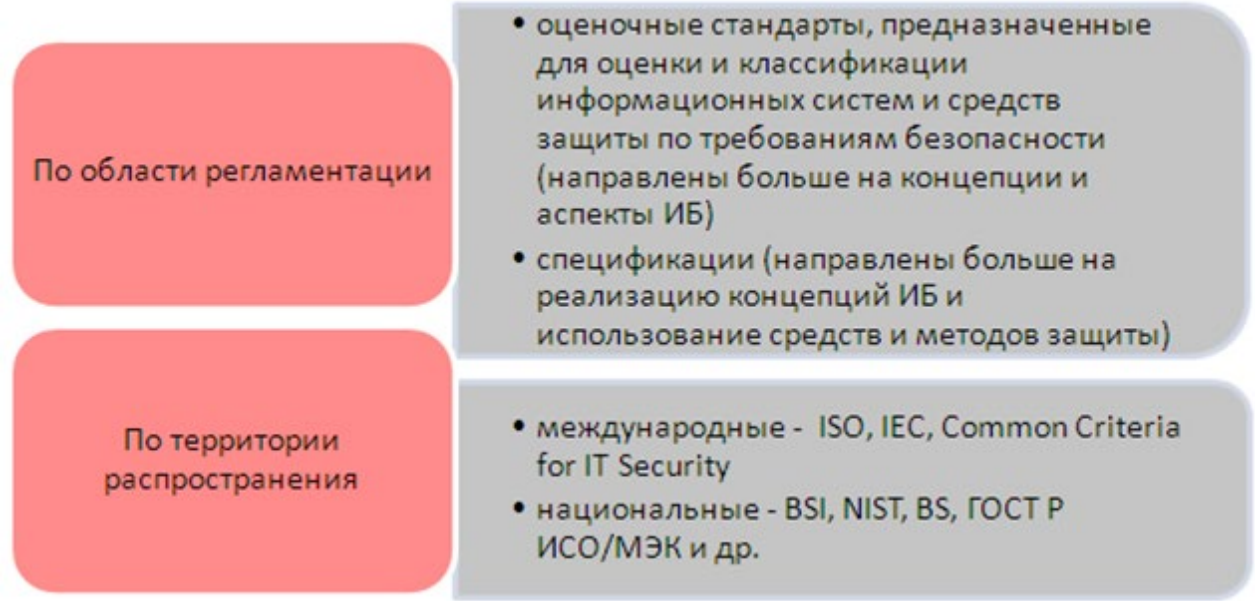

Рис. 1 – Классификация стандартов информационной безопасности корпоративных сетей

Данные стандарты имеют цель активно предотвращать угрозы информационной безопасности корпоративных сетей [4]:

– внешние: вредоносное программное обеспечение, «вымогатели» (шифровальщики, англ. ransomware), руткиты (англ. Root kit), фишинги (англ. Phishing), DDoS-

атаки (аббревиатура от англ. Denial of Service, “отказ в обслуживании”), эксплойты, ботнеты и пр.:

- внутренние: разнообразные уязвимости в ПО и архитектуре систем, бэкдоры и человеческий фактор.

Гарантия высокой информационной безопасности корпоративных сетей, отвечающей современным стандартам на сегодня и на ближайшее будущее связана с созданием на следующем этапе необходимой смоделированной архитектуры с применением эффективных инструментов и программных средств– рис. 2 [1].

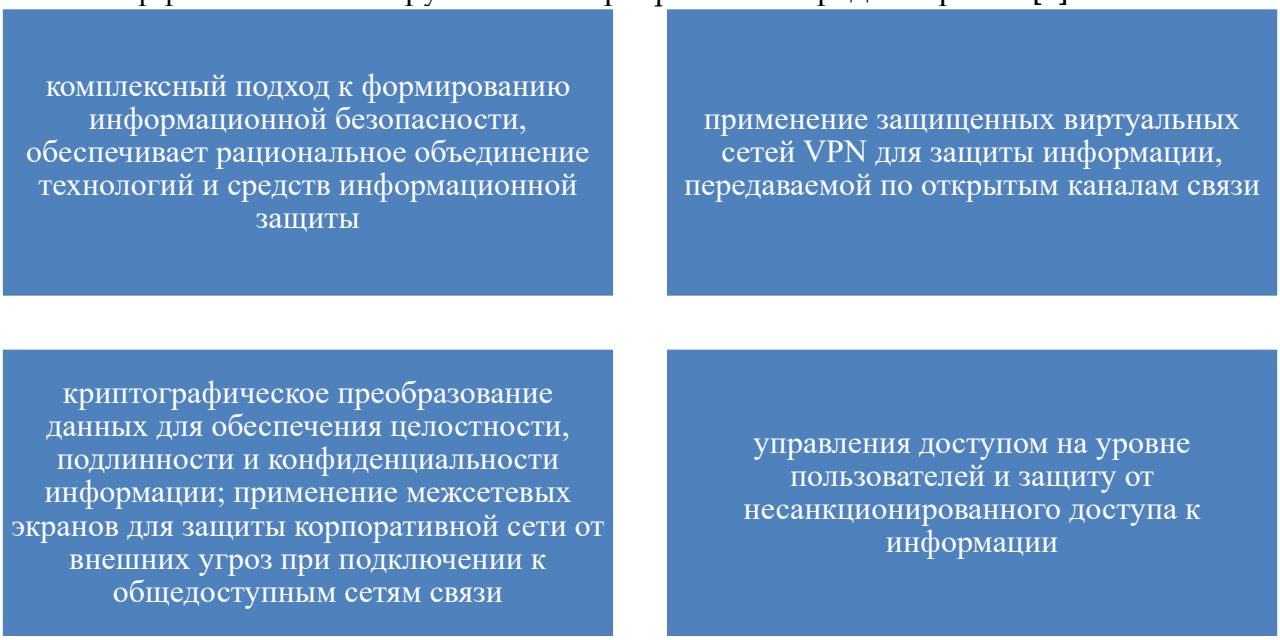

Рис. 2 – Особенности этапа моделирования архитектуры системы информационной безопасности

Этап обеспечения програмно-компонентной реализации должен включать такие направления – рис. 3 [5].

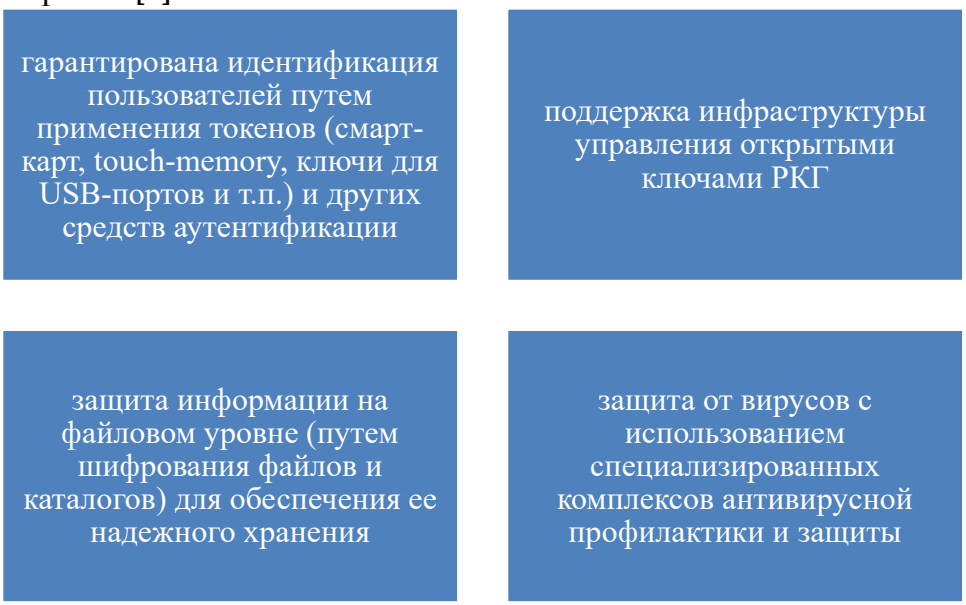

Рис. 3 – Направления этапа программно-компонентной реализации, отвечающие современным стандартам [2]

Оценивая стоимостное выражения услуг на современном рынке продуктов по обеспечению информационной безопасности корпоративных сетей, отвечающей

современным стандартам, можно назвать базовую цену на уровне 100-150 тыс. рублей, однако это в основном касается стандартизированных программных продуктов.

В рамках исследования основных этапов разработки информационной безопасности корпоративных сетей, отвечающей современным стандартам, показана актуальность практической реализации технологии Blockchain. Блокчейн (в переводе с англ. Blockchain - цепочка и блоков) - распределенная база данных, содержащая сведения обо всех операциях, осуществленных участниками системы. Информация хранится в виде цепочки блоков, в каждом из которых записана определенное количество таких операций [3].

Маршрут достижимости информационной безопасности корпоративных сетей с использованием технологии Blockchain может быть описан при помощи логико-математической модели:

$$x_{1s}^{i,j-1,k} = \left(x_{11}^{ijk} \vee x_{12}^{ijk} \vee x_{13}^{ijk} \vee x_{14}^{ijk} \vee \right.$$
$$\left. \vee x_{15}^{ijk} \vee x_{16}^{ijk} \vee x_{r}^{ijk} \right) \cdot \overline{x}_{0}^{ijk} \cdot \overline{q}_{s}^{ijk},$$

где x_{1s}^{ijk} – достижимость блока с информацией (ijk), s=1..6;

q_s^{ijk} – значение первого n- D – триггера блока с информацией (ijk), s=1..6;

x_r^{ijk} – резервный блок с информацией;

x_0^{ijk} – отказавший блок с информацией.

Представленная логико-математическая модель достижимости информационной безопасности корпоративных сетей с использованием технологии Blockchain регулирует движение блоков с информацией в корпоративной системе при их различных статусах: «действенный», «отказавший» и «резервный».

В результате исследования рассмотрены основные угрозы информационной безопасности корпоративных сетей, отвечающей современным стандартам в аспекте разработки системы мониторинга их информационной безопасности. В рамках исследования основных этапов разработки информационной безопасности корпоративных сетей, отвечающей современным стандартам, показана актуальность применения технологии Blockchain. Предложена логико-математическая модель, описывающая маршрут достижимости информационной безопасности на основе технологии Blockchain.

Список литературы:

1. Ланецкая А.Ю., Александрова Е.Н. Современные угрозы информационной безопасности // Международный журнал гуманитарных и естественных наук. 2022. №7-2. URL: https://cyberleninka.ru/article/n/sovremennye-ugrozy-informatsionnoy-bezopasnosti (дата обращения: 22.07.2024).
2. Табилова А.З., Коннов А.Л. Анализ проблем информационной безопасности в корпоративных сетях // Вестник науки и образования. 2019. №17 (71). URL: https://cyberleninka.ru/article/n/analiz-problem-informatsionnoy-bezopasnosti-v-korporativnyh-setyah (дата обращения: 22.07.2024).
3. Карасёв П.А. Информационная безопасность в корпоративных сетях // Таврический научный обозреватель. 2017. №3-1 (20). URL:

https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-v-korporativnyh-setyah (дата обращения: 22.07.2024).
4. Джонс С., Дэвис Дж. Стратегии конфиденциальности и защиты данных в инфобизнесе: лучшие практики и проблемы. Журнал информационной конфиденциальности, (2023), 15(4), 321-336.
5. Иремадзе Э. О., Заремба А. И. Основы информационной безопасности // Скиф. 2022. №5 (69). URL: https://cyberleninka.ru/article/n/osnovy-informatsionnoy-bezopasnosti (дата обращения: 12.07.2024).

References:

1. Lanetskaya A.Yu., Aleksandrova E.N. Modern Information Security Threats // International Journal of Humanities and Natural Sciences. 2022. No7-2. URL: https://cyberleninka.ru/article/n/sovremennye-ugrozy-informatsionnoy-bezopasnosti (date of access: 22.07.2024).
2. Tabilova A.Z., Konnov A.L. Analysis of information security problems in corporate networks // Bulletin of Science and Education. 2019. No17 (71). URL: https://cyberleninka.ru/article/n/analiz-problem-informatsionnoy-bezopasnosti-v-korporativnyh-setyah (date of access: 22.07.2024).
3. Karasev P.A. Information Security in Corporate Networks // Tauric Scientific Reviewer. 2017. No3-1 (20). URL: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-v-korporativnyh-setyah (date of access: 22.07.2024).
4. Jones, S., Davis, J. Data Privacy and Protection Strategies in Infobusiness: Best Practices and Challenges. Journal of Information Privacy, (2023), 15(4), 321-336.
5. Iremadze E. O., Zaremba A. I. Fundamentals of information security // Scythian. 2022. No5 (69). URL: https://cyberleninka.ru/article/n/osnovy-informatsionnoy-bezopasnosti (date of access: 12.07.2024).