Научная статья
УДК:004.056

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ, ОБЕСПЕЧЕНИЕ УСТОЙЧИВОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ НА РЕЖИМНЫХ ОБЪЕКТАХ

Людмила Юрьевна Помыткина[1], Вячеслав Никитич Мачихин[2]
[1, 2] Уральский государственный лесотехнический университет, Екатеринбург, Россия
[1] lypomytkina@yandex.ru
[2] versuvu1@gmail.com

Аннотация. В данной статье анализируются основные методы защиты информации, выявляются наиболее эффективные для режимных предприятий. Проанализированы научные работы и публикации по теме информационной безопасности, а также практический опыт специалистов.

Ключевые слова: Защита информации, режимные предприятия

Для цитирования: Помыткина Л. Ю., Мачихин В. Н. Сравнительный анализ методов защиты информации, обеспечение устойчивости информационных систем на режимных объектах // Эффективный ответ на современные вызовы с учетом взаимодействия человека и природы, человека и технологий = Effective reaction to modern challenges of the interaction between human and nature, human and technologies : материалы XVII Международной научно-технической конференции. Екатеринбург : УГЛТУ, 2026. С. 520–525.

Original article

COMPARATIVE ANALYSIS OF INFORMATION PROTECTION METHODS TO ENSURE THE STABILITY OF INFORMATION SYSTEMS AT HIGH-SECURITY FACILITIES

Lyudmila Yu. Pomytkina[1], Vyacheslav N. Machikhin[2]
[1, 2] Ural State Forest Engineering University, Ekaterinburg, Russia
[1] lypomytkina@yandex.ru
[2] versuvu1@gmail.com

Abstract. This article analyzes the main methods of information protection, and identifies the most effective ones for high-security enterprise. Scientific papers and publications on the topic of information security, as well as the practical experience of specialists, will be analyzed.

Keywords: information protection, high-security enterprises

For citation: Pomytkina L. Yu, Machikhin V. N. (2026) Sravnitel'nyj analiz metodov zashchity informacii obespecheniya ustojchivosti informacionnykh sistem na rezhimnykh ob"ektakh [Comparative analysis of Information protection methods to ensure the stability of information systems at high-security facilities] // Effektivnyi otvet na sovremennye vyzovy s uchetom vzaimodeistviya cheloveka i prirody, cheloveka i tekhnologii [Effective reaction to modern challenges of the interaction between human and nature, human and technologies : materials of the XVII International Scien-tific and Technical Conference]. Ekaterinburg : USFEU, 2026. P. 520–525. (In Russ).

В нынешний период с мгновенной цифровизацией и постоянными киберугрозами защита конфиденциальной информации и создание более безопасного и надежного ПО становятся все сложнее. В то же время, они выполняют важнейшую функцию в обеспечении безопасности и стабильной работы режимных спецобъектов. Они созданы для управления критически важными процессами, для хранения и обработки конфиденциальной информации, обеспечения связи и координации между отделами. Но также они могут повысить риск компрометации со стороны злоумышленников.

Выделяют множество методов защиты, проанализируем те, которые обеспечивают безопасность и устойчивость информационных систем предприятий.

Шифрование — это незаменимый инструмент для защиты личной информации. Оно создает надежный барьер, который не позволяет злоумышленникам воспользоваться данными, даже если они попадут в их руки. Представьте себе: конфиденциальные данные зашифрованы и выглядят как бессмысленный набор символов для любого, кто попытается их расшифровать без специального ключа. Такая защита применяется на предприятиях с повышенными требованиями к безопасности, таких как финансовые учреждения или государственные организации.

Современная криптография AES-256 или RSA представляется фундаментом обеспечения конфиденциальности в соответствии со строгими стандартами по типу GDPR или ФЗ-152, но и она не лишена уязвимостей. Безопасность напрямую зависит от сохранности ключа, его потеря ведет к безвозвратной потере доступа к данным, а компрометация отдает доступ в неблагонадежные руки. Устаревшие методы уязвимы к новым регулярно совершенствующимся атакам, к брутфорсу или приходящим квантовым вычислениям, из чего самое важное – это актуализировать и адаптировать криптографические протоколы к вызовам времени [3].

Еще одним важным методом является **резервное копирование** данных. Компании все чаще используют арендуемые сервера для хранения данных, но большим и специализированным предприятиям это не подходит. Они предпочитают размещать хранилища локально. Это требует дополнительных затрат, но обеспечивает более надежную защиту информации.

Для информационных систем предприятий важно, чтобы данные можно было хранить и обрабатывать без подключения к сети. Такой подход делает их более устойчивыми. Одно из главных преимуществ локального хранения – быстрое восстановление данных после потери. Оно сокращает время простоя и уменьшает риск полной утраты информации.

Резервные копии могут быть созданы с помощью отдельных сервисов, например американских Commvault и Российских Veeam, которые больше подходят для нашего объекта. А также можно использовать штатные инструменты Windows Server, которые позволяют откатить систему до возможной атаки ransomware (программа-вымогатель) или просто случайного удаления, это может быть дешевле, но при том и менее безопасно. Однако все эти средства кратно увеличивают свою эффективность, если соблюдать правило трех расположений копий данных, две – на разных носителях на территории предприятия, и одна – удаленно (офф-сайт) [4].

Контроль доступа – еще один значимый этап в организации системы безопасности. Для этого используются пароли, многофакторная аутентификация и разграничение ролей. Подотчетность внутри предприятия и в его информационных системах считается одним из основных плюсов контроля доступа. Она позволяет отслеживать, к каким данным у сотрудников есть доступ и какие операции они выполняют. Такой контроль помогает обнаружить утечки данных и предотвратить их появление. Помимо этого, он упрощает работу администраторов, автоматизируя управление пользователями.

С другой стороны, при всех преимуществах очень сложно реализовать контроль доступа. Чтобы гарантировать такой высокий уровень защиты, нужно правильно организовать работу систем. Коды доступа или пароли должны быть уникальными и надежными, а для большей безопасности должна использоваться двухфакторная идентификация. Постоянное обновление и тестирование систем контроля доступа. Все это поможет защитить конфиденциальные данные от раскрытия неавторизованным лицам и обеспечить стабильную работу систем.

Внедрение и обслуживание контроля доступа обходятся дорого. Кроме того, важно предоставить пользователям возможность либо изменить свой пароль, либо восстановить его в случае утери [1].

Далее мы рассмотрим **сетевую безопасность** – комплекс мер, направленных на защиту данных в компьютерных сетях. Эти меры включают использование брандмауэров для ограничения доступа извне, систем обнаружения вторжений, а также шифрование данных в сети.

Ее весомый плюс – это способность предостеречь угрозу, охраняя служебные данные от внешних воздействий, и играет важную роль для организаций, позволяя им придерживаться требований законодательства и стандартов в своей отрасли. Активное залатывание дыр в защите сетевой инфраструктуры существенно уменьшает вероятность распространения коммерческих тайн компаний. Присутствуют минусы, мешающие

реализации. Чтоб система работала, необходим найм опытных профессионалов сетевой безопасности. А также со временем стратегии сетевой безопасности должны регулярно обновляться и адаптироваться к современным рискам и методам атак, что требует постоянного внимания и ресурсов [2].

Физическая безопасность – это комплекс мероприятий, контролирующий доступ к помещениям и технике. Она также определяет правила взаимодействия со служебными ИС:

- размещение замков, клеток и иных запирающих объектов;
- использование биометрических данных работников для разблокировки устройств;
- применение токенов, карточек-ключей и иных уникальных переносимых идентификаторов;
- установка систем слежения и сигнализирования о проникновениях.

Главный плюс этого метода защиты безопасности в том, что она обеспечивает полный контроль над физическим доступом к данным для компаний. Меры физической защиты дают организациям уверенность в безопасности их данных. Они играют ключевую роль в защите резервных копий данных, обеспечивая их целостность и доступность. А регистрация всех переносимых устройств, таких как просто носителей информации, средств связи, и ноутбуков, используемых в работе, убирает лишние риски.

Из-за человеческого фактора, а подавляющая масса потерь информации происходят по вине человека, очень важно обеспечивать наибольшее количество уровней физической защиты, что потенциально пресечет утечки, а любое пренебрежение ими потенциально ведет к убыткам. Но это ведет за собой как психологическую, так и физическую повышенную нагрузку на персонал, что нужно учитывать и, по возможности, искать компромиссы [5].

Для обеспечения безопасности на режимных предприятиях важно применять комплексный подход, который включает в себя все перечисленные выше меры, но наиболее подходящими вариантами защиты являются следующие:

– надежные алгоритмы **шифрования** (AES с длиной ключа 256 бит**);**

– **локальное резервное копирование критически важных данных** (с использованием RAID-массивов, позволяющих повысить отказоустойчивость и производительность системы хранения данных за счет использования нескольких дисков);

– **контроль доступа** к ИС (многофакторная аутентификация, регулярные проверки прав доступа пользователей к ресурсам по ролям, обновление паролей, токены и смарт-карты);

– аспекты **сетевой безопасности (**межсетевые экраны NGFW контролируют и фильтруют трафик, блокируя несанкционированный доступ и атаки. VPN IPsec и WireGuard создают зашифрованные туннели для удаленной работы, защищая данные в публичной сети. Системы защиты

от распределенных атак отказа в обслуживании предотвращают перегрузки сети и серверов, обеспечивая непрерывную работу систем. Использование SSL/TLS для шифрования сетевого трафика гарантирует, что данные передаются в зашифрованном виде. Регулярный анализ сетевой активности помогает выявлять подозрительные действия и потенциальные угрозы);

– **физическая безопасность** (электронные замки и системы контроля доступа, регистрация всех носителей информации, которые используются на предприятии, что позволяет вести учет и контролировать доступ к данным).

Эти меры позволяют обеспечить высокий уровень защиты данных, систем и сотрудников на предприятии. Выбор конкретных методов защиты зависит от специфики предприятия, его размеров, структуры и требований к безопасности. Однако стоит помнить, что безопасность – это процесс, требующий постоянного внимания и обновления подходов. Специалисты должны регулярно оценивать состояние безопасности и внедрять новые технологии и методы, чтобы эффективно противостоять возникающим угрозам.

Список источников

1. Укрепление цифрового бастиона: Новаторство кибербезопасности на предприятии благодаря динамическому управлению секретами и объединению CMDB // Журнал информационной безопасности. 2024. № 15. С. 411–418.

2. Optimizing Network Security via Ensemble Learning: A Nexus with Intrusion Detection / A. Baluguri, V. Pasumarthy, I. Roy [et al.] // Journal of Information Security. 2024. № 15. 545–556.

3. Методы защиты данных [Электронный ресурс]. URL: https://www.titanfile.com/blog/5-methods-of-protecting-data (дата обращения: 11.11.2024).

4. План резервного копирования системы – безопасность вашей информации [Электронный ресурс]. URL: https://zscomp.ru/news/Plan_rezervnogo_kopirovaniya_sistemi_text (дата обращения: 11.11.2024).

5. Что такое физическая безопасность [Электронный ресурс]. URL: https://tor-safety.com/ru/chto-takoe-fizicheskaya-bezopasnost/ (дата обращения: 11.11.2024).

References

1. Strengthening the Digital Bastion: Innovating Cybersecurity in the Enterprise through Dynamic Secret Management and CMDB Integration // Information Security Journal. 2024. No. 15. P. 411–418.

2. Optimizing Network Security via Ensemble Learning: A Nexus with Intrusion Detection / A. Baluguri, V. Pasumarthy, I. Roy [et al.] // Journal of Information Security. 2024. № 15. 545–556.

3. Data protection methods [Electronic resource]. URL: https:// www.titanfile.com/blog/5-methods-of-protecting-data (date of accessed: 11.11.2024).

4. System backup plan – security of your information [Electronic resource]. URL: https://zscomp.ru/news/Plan_rezervnogo_kopirovaniya_sistemi_text_ / (date of accessed: 11.11.2024).

5. What is physical security [Electronic resource]. URL: https://tor-safety.com/ru/chto-takoe-fizicheskaya-bezopasnost (date of accessed: 11.11.2024).