УДК 005.21:334.012.42

Никитина Т. О.

старший преподаватель кафедры экономической информатики, учёта и коммерции

Гомельский государственный университет имени Франциска Скорины

Республика Беларусь, г. Гомель

РАЗРАБОТКА ЕДИНОЙ ПЛАТФОРМЫ КОНТРОЛЯ ДОСТУПА, ЗАЩИТЫ И ШИФРОВАНИЯ ДЛЯ КОММЕРЧЕСКИХ ОРГАНИЗАЦИЙ

Аннотация:

В статье предложена архитектура интегрированного программного комплекса для обеспечения информационной безопасности в коммерческих организациях, объединяющего управление доступом, антивирусные механизмы и криптографические средства. Описаны ключевые компоненты системы, требования к идентификации и авторизации, особенности поведенческого и сигнатурного обнаружения угроз, а также принципы управления ключами через централизованный KMS/HSM. Предложенные подходы направлены на повышение согласованности мер защиты, оперативности реагирования на инциденты и соответствия регуляторным требованиям.

Ключевые слова: информационная безопасность, управление доступом, шифрование и управление ключами, кибербезопасность, менеджер безопасности.

Nikitina T.

senior lecturer, Department of Economic Informatics, Accounting and Commerce

Gomel State University named after Francis Skorina

Republic of Belarus, Gomel

DEVELOPING A UNIFIED ACCESS CONTROL, SECURITY, AND ENCRYPTION PLATFORM FOR COMMERCIAL ORGANIZATIONS

Abstract:

This article proposes the architecture of an integrated software suite for ensuring information security in commercial organizations, integrating access control, antivirus mechanisms, and cryptographic tools. It describes the key system components, identification and authorization requirements, behavioral and signature-based threat detection features, and key management principles via a centralized KMS/HSM. The proposed approaches are aimed at improving the consistency of security measures, the speed of incident response, and compliance with regulatory requirements.

Keywords: information security, access control, encryption and key management, cybersecurity, security manager.

Защита информации в коммерческой организации — это системная задача, поскольку она включает процессы идентификации и аутентификации, контроля доступа, обнаружения и нейтрализации вредоносного ПО, защиту каналов передачи и хранение данных в зашифрованном виде. При разрозненном использовании независимых средств защиты часто возникают проблемы несовместимости политик, пробелы в журналировании и замедленное реагирование на инциденты; интеграция ключевых функциональных модулей в единую платформу снижает такие операционные риски и повышает согласованность мер безопасности.

При проектировании архитектуры менеджера безопасности использовались следующие принципиальные требования [1]:

- централизованное управление идентификацией и доступом с поддержкой RBAC/ABAC и многофакторной аутентификации;

- сочетание сигнатурного, эвристического и поведенческого анализа в антивирусном/EDR-модуле;

- гибридная криптография с централизованным KMS/HSM для управления жизненным циклом ключей;

- единая система логирования с возможностью интеграции в SIEM для корреляции событий;

поддержка развёртывания как в локальной инфраструктуре, так и в облаке с учётом модели Shared Responsibility и принципов Zero Trust.

Архитектура предусматривает защищённые каналы взаимодействия между компонентами, разграничение привилегий для администраторов и операторов, механизмы аудита и автоматической ротации секретов.

Основной блок управления доступом обеспечивает централизованную идентификацию и аутентификацию пользователей, реализацию политик RBAC и/или ABAC, а также поддержку MFA (TOTP, аппаратные токены, FIDO2) для критичных сервисов. Необходима автоматизация жизненного цикла учётных записей: создание, изменение, временная деактивация и окончательное удаление при увольнении. Для критичных операций рекомендуется двусторонняя авторизация (подтверждение администратора и ответственного за безопасность) и применение принципа наименьших привилегий (least privilege) с обязательным аудитом всех смен прав доступа и всех действий привилегированных аккаунтов. Секреты и пароли следует хранить в защищённом хранилище (KMS/HSM) с политиками ротации и журналированием доступа.

Антивирусный модуль в составе менеджера объединяет традиционные механизмы сигнатурного сканирования и эвристического анализа с возможностями поведенческого мониторинга и EDR-функциями. Это обеспечивает защиту при доступе, регулярное глубокое сканирование, облачную проверку репутации и анализ поведения процессов в рантайме.

При обнаружении угроз модуль выполняет карантин, попытки восстановления, удаление или формирование предупреждений и интеграцию с SIEM/Helpdesk для оперативного реагирования. Для защиты сетевого и почтового трафика реализуется фильтрация вложений и ссылок, TLS-инспекция при необходимости и интеграция с веб-прокси для блокировки фишинговых ресурсов; сочетание локальных и облачных механизмов позволяет быстрее реагировать на новые угрозы и снижает ложные срабатывания через централизованное управление политиками.

Криптографический модуль реализует гибридный подход: симметричное шифрование (рекомендуется использование Authenticated Encryption, например AES-GCM) для объёмных данных и асимметричные схемы для обмена ключами и цифровой подписи. Управление жизненным циклом ключей должно осуществляться через централизованный KMS/HSM с политиками ротации, резервного восстановления и разграничением прав доступа. Для межкорпоративной переписки и почтовых сообщений следует использовать проверенные стандарты (S/MIME или PGP), для каналов передачи — TLS последних версий с отключёнными устаревшими шифрами и корректной конфигурацией сертификатов. Прозрачное шифрование на уровне хранилищ и/или шифрование на уровне приложений должно выбираться согласно сценарию использования и требованиям производительности.

Выбор модели развёртывания (локально или в облаке) должен основываться на оценке регуляторных требований, критичности данных и ресурсных возможностях организации. Локальное развёртывание обеспечивает максимальный контроль и предпочтительно для объектов с высокими требованиями к защите стратегически значимой информации; облачное развёртывание предоставляет масштабируемость и сокращение операционных затрат для малого и среднего бизнеса, но требует внимательной оценки модели Shared Responsibility и дополнительных мер:

шифрование данных в покое и при передаче, управление ключами, резервные планы при потере связи с провайдером и контроль SLA провайдера. При облачном использовании оправдано внедрение принципов Zero Trust: микросегментация, непрерывная проверка контекста доступа и минимизация доверия по умолчанию.

Операционная составляющая менеджера включает централизованное журналирование всех событий безопасности с интеграцией в SIEM для корреляции инцидентов и построения сценариев оповещений, регламентированные процедуры реагирования (детекция, изоляция, форензика, восстановление), регулярное резервное копирование и тестирование планов восстановления (BC/DR). Особое внимание следует уделять политике управления привилегированными учётными записями (PAM), регулярному аудиту прав доступа и обучению персонала, что существенно снижает риски, связанные с человеческим фактором.

Интеграция модулей в единую платформу упрощает операционное управление, уменьшает количество точек администрирования и обеспечивает согласованное логирование, однако создаёт и новые требования по защите административной плоскости: критично разделение обязанностей, использование HSM/KMS для хранения секретов, защита административных интерфейсов и возможность отката изменений в случае компрометации. Поэтому технические меры должны сопровождаться организационными процедурами, политиками и регулярными тренировками команд реагирования на инциденты.

Предложенная архитектура интегрированного менеджера информационной безопасности обеспечивает современный, управляемый и масштабируемый подход к защите коммерческих организаций. Ключевые элементы — централизованное управление доступом с поддержкой MFA и RBAC/ABAC, комбинированная защита endpoint-ов с EDR-возможностями, надёжное управление ключами через KMS/HSM,

централизованное логирование и применение принципов Zero Trust — в комплексе повышают устойчивость организации к актуальным угрозам и упрощают соответствие международным и национальным стандартам безопасности .

Использованные источники

1. Диогенес, Ю. Кибербезопасность: стратегии атак и обороны / Ю. Диогенес, Э. Озкайя - М.: ДМК-Пресс, 2020. – 326 с.