УДК 004.056

ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИОННЫХ РЕСУРСОВ УНИВЕРСИТЕТА

В. Е. МИНИН, С. В. КИСЕЛЕВА, С. С. ТАТУР
Белорусский государственный университет транспорта, г. Гомель

Современные университеты активно используют цифровые технологии в образовательной деятельности. Однако распространенной проблемой является эксплуатация устаревших информационных систем, обновление которых затруднено из-за несовместимости, отсутствия ресурсов или ограничений инфраструктуры.

Примером может служить сервер системы дистанционного обучения (СДО), функционирующий на базе устаревших версий системы управления обучением и операционной системы. Такие системы часто работают без регулярного резервного копирования, не имеют плана восстановления после сбоев и содержат критические уязвимости, что ставит под угрозу доступность и целостность образовательных сервисов.

Эксплуатация устаревших версий программного обеспечения сопровождается рядом рисков:

– наличие известных уязвимостей, для которых уже опубликованы инструменты атаки;

– отсутствие актуальных обновлений безопасности;

– возможные ошибки конфигурации и слабая аутентификация;

– недостаточный контроль событий безопасности;

– риск потери данных из-за отсутствия резервного копирования.

Эти проблемы приводят к снижению уровня защищенности университетской ИТ-инфраструктуры и могут вызвать перебои в предоставлении образовательных услуг.

При невозможности оперативного обновления систем следует внедрить следующие компенсирующие меры, направленные на снижение вероятности инцидентов безопасности.

1 Сегментация сети и размещение сервера в выделенной подсети позволят ограничить сетевой доступ к СДО.

2 Использование межсетевого экрана веб-приложений (WAF) и виртуального патчинга защитит от наиболее распространенных атак на веб-приложения.

3 Централизованный сбор логов и внедрение SIEM-системы обеспечит отслеживание и определение корреляции событий безопасности.

4 Резервное копирование предполагает регулярное создание копий данных с хранением на отдельном сервере.

5 Использование программных решений для динамического блокирования неавторизованного доступа (Fail2Ban, GeoIP-фильтрация) позволит выполнять блокировку несанкционированных попыток входа и ограничение доступа из нежелательных регионов.

6 Контроль целостности файлов осуществляет отслеживание изменений системных компонентов.

7 Усиление аутентификации реализуется применением двухфакторной авторизации и политики надежных паролей.

В совокупности данные меры позволяют существенно снизить риски до завершения обновления инфраструктуры.

Обеспечение защиты информационных ресурсов университета при эксплуатации устаревших систем требует применения многоуровневого подхода. При невозможности немедленного обновления системного и программного обеспечения следует реализовать компенсирующие меры, которые гарантируют приемлемый уровень безопасности и позволят сохранить доступность и надежность образовательных сервисов. При этом информационная безопасность должна рассматриваться как непрерывный процесс, включающий технические, организационные и административные меры, направленные на снижение рисков и повышение устойчивости ИТ-инфраструктуры.

Список литературы

1 **Шаньгин, В. Ф.** Комплексная защита информации в корпоративных системах : учеб. пособие / В. Ф. Шаньгин. – М. : Форум; Инфра-М, 2022. – 592 с.

2 ISO/IEC 27001:2022. Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements.