УДК 004.056

РАЗРАБОТКА СТЕНДА ЗАЩИЩЕННОЙ СЕТЕВОЙ ИНФРАСТРУКТУРЫ НА БАЗЕ ОТЕЧЕСТВЕННОГО ПРОГРАММНОГО КОМПЛЕКСА EFROS DEFENCE OPERATIONS

Боговский С. А.[1], Дедков А. В.[1]

Научный руководитель – старший преподаватель кафедры судовой автоматики и измерений Цымай Ю. В.[1]

[1] Санкт-Петербургский государственный морской технический университет

m-walua@yandex.ru

Введение

На современном этапе развития информационных технологий информация стала ключевым ресурсом, обеспечивающим прогресс общества. Однако расширение информационного пространства сопровождается ростом киберугроз, таких как атаки на сетевую инфраструктуру, утечки данных и несанкционированный доступ. Сетевые устройства (серверы, маршрутизаторы, коммутаторы) часто становятся мишенями атак, и их компрометация приводит к нарушению конфиденциальности, целостности и доступности данных[1].

В условиях импортозамещения и роста киберугроз актуальной становится задача внедрения отечественных средств защиты информации и подготовки квалифицированных кадров для работы с ними. В статье представлены результаты исследования, целью которого являлась разработка защищенной сетевой инфраструктуры с использованием программного комплекса Efros Defence Operations (Efros DO), а также создание комплекса лабораторных работ для его практического применения в учебном процессе. Проведен сравнительный анализ зарубежных аналогов с использованием метода QSWOT, подтвердивший преимущества отечественного решения. Описаны процесс развертывания лабораторного стенда, настройка протоколов для централизованного управления доступом, а также структура разработанных лабораторных работ.

Основная часть

Сравнительный анализ программных комплексов методом QSWOT.

Для обоснования выбора Efros DO был проведен анализ рынка программных комплексов, имеющих сходные функциональные характеристики. В качестве конкурентов рассматривались Aruba ClearPass, SolarWinds NCM, ManageEngine, FortiNAC и Cisco ISE.

Системный анализ проводился с использованием метода квалиметрического SWOT-анализа (QSWOT), который позволяет перейти от вербального описания к количественному измерению качества с помощью агрегированных показателей. Оценивание программ проводилось по десятибалльной шкале [3].

Результаты анализа показали, что наивысшую оценку (Q = 8,2) получил отечественный комплекс Efros Defence Operations. Aruba ClearPass занял второе место с оценкой Q = 6,7. Cisco ISE и ManageEngine получили по Q = 6,2, SolarWinds – Q = 6,1, а FortiNAC – Q = 5,9.

Лидерство Efros DO обусловлено его универсальностью, соответствием требованиям национальной безопасности сертификация ФСТЭК (Федеральная служба по техническому и экспортному контролю), поддержка ГОСТ, а также адаптивностью к российским условиям, включая полную совместимость с отечественными операционными системами Astra Linux, Ред ОС, ALT Server. Зарубежные аналоги, напротив, страдают от санкционных ограничений, отсутствия сертификации ФСТЭК и слабой совместимости с российским программным обеспечением.

Разработка и развертывание лабораторного стенда.

В работе подробно описан процесс развертки стенда, а также настройка необходимых протоколов, включая конфигурацию сетевого оборудования и создание необходимых объектов в интерфейсе Efros DO: пользователей локальных и из LDAP (Протокол для доступа и управления распределёнными каталогами информации.)/ Active Directory (службы каталогов), профилей оборудования, списков разрешенных протоколов, профилей авторизации и наборов политик доступа.

Для визуализации инфраструктуры и анализа уязвимостей была построена виртуальная карта сети в модуле «Объект защиты». Карта позволяет отслеживать защищенность объектов и выявлять некорректные настройки, например, прав доступа к критическим файлам в Linux [2,4].

Методическая база лабораторных работ.

Результатом работы стала разработка четырех лабораторных работ для практического освоения Efros DO студентами.

1. Лабораторная работа №1 «Доступ на оборудование с использованием протокола RADIUS»

Цель – освоить настройку аутентификации на сетевом оборудовании с использованием локальных учетных записей Efros DO и протокола RADIUS.

2. Лабораторная работа №2 «Доступ на оборудование с использованием протокола TACACS+»

Работа направлена на изучение интеграции Efros DO с LDAP/Active Directory для аутентификации доменных пользователей.

3. Лабораторная работа № 3. «Организация безопасного гостевого доступа в корпоративной сети»

В ходе работы студенты настраивают гостевой портал в Efros DO для предоставления внешним пользователям доступа к публичной сети с соблюдением требований безопасности. Работа включает создание гостевых пользователей и профилей авторизации.

4. Лабораторная работа № 4. «Построение векторов атак в программном комплексе Efros DO»

Цель – освоить методику анализа уязвимостей сетевой инфраструктуры с использованием моделей нарушителей.

Выводы

В результате выполнения работы был разработан стенд защищенной сетевой инфраструктуры на базе отечественного программного комплекса Efros Defence Operations для демонстрации возможностей комплекса. Проведенный QSWOT-анализ подтвердил его преимущество перед зарубежными аналогами по критериям доступности, соответствия российским стандартам и пригодности для учебных целей.

Литература

1. Защита сетевой инфраструктуры [Электронный ресурс]. – Режим доступа: https://apptask.ru/blog/zashhita-setevoi-infrastruktury (дата обращения 11.02.2026).
2. Программный комплекс по защите системно-технической инфраструктуры «Efros Defence Operations» Описание применения [Электронный ресурс]. – Режим доступа: https://www.gaz-is.ru/component/jdownloads/send/52-efros-defence-operations/358-opisanie-primeneniya-pk-efros-do (дата обращения 12.02.2026).
3. Алексеев А.В., Удодова Е.Н. Квалиметрический SWOT-анализ и его применение в задачах управления развитием критических морских объектов // Морские интеллектуальные технологии. Научный журнал № 1 (31) Т.1 – 2016 – С. 38 – 48.
4. Программный комплекс по защите системно-технической инфраструктуры «Efros Defence Operations» Руководство администратора [Электронный ресурс]. – Режим доступа: https://www.gaz-is.ru/component/jdownloads/send/52-efros-defence-operations/359-rukovodstvo-administratora-pk-efros-do (дата обращения 12.02.2026).