

МОДЕЛИРОВАНИЕ ПОТОКА УЯЗВИМОСТЕЙ В ЖИЗНЕННОМ ЦИКЛЕ ИТ-АКТИВОВ ВУЗА НА ОСНОВЕ ПОДХОДА CYBER THREAT INTELLIGENCE

С.С. Тарлыков¹, А.М. Тюнина¹

¹ФГБОУ ВО «Воронежский государственный лесотехнический университет имени Г.Ф. Морозова»

Аннотация. В статье рассматривается проблема статической инвентаризации ИТ-активов образовательных организаций, не учитывающей динамику появления уязвимостей и изменение ландшафта киберугроз. Предложена динамическая модель потока уязвимостей в жизненном цикле ИТ-активов вуза на основе подхода Cyber Threat Intelligence (CTI). Модель интегрирует инвентаризационную базу (CMDB) с внешними источниками угроз (CVE, OSINT) и внутренними средствами мониторинга (сканеры уязвимостей, SIEM), обеспечивая автоматизированный расчет атрибута «текущий уровень риска» для каждого актива. Представлена архитектура потоков данных, математическая модель оценки риска с учетом метрик CVSS и критичности актива, а также механизм приоритизации мероприятий по устранению уязвимостей. Показано, что предложенный подход трансформирует систему учета активов в инструмент проактивного управления безопасностью и формирует основу DevSecOps-практик в образовательной организации.

Ключевые слова: информационная безопасность, Cyber Threat Intelligence, CMDB, CVE, управление уязвимостями, DevSecOps, оценка риска.

MODELING THE VULNERABILITY FLOW IN THE LIFECYCLE OF UNIVERSITY IT ASSETS BASED ON THE CYBER THREAT INTELLIGENCE APPROACH

S.S. Tarlykov¹, A.M. Tyunina¹

¹Voronezh State University of Forestry and Technologies named after G.F. Morozov

Abstract. The article discusses the problem of static inventory of IT assets of educational organizations, which does not take into account the dynamics of vulnerabilities and the changing landscape of cyber threats. A dynamic model of the vulnerability flow in the lifecycle of university IT

assets based on the Cyber Threat Intelligence (CTI) approach is proposed. The model integrates the inventory database (CMDB) with external threat sources (CVE, OSINT) and internal monitoring tools (vulnerability scanners, SIEM), providing an automated calculation of the "current risk level" attribute for each asset. The architecture of data flows, a mathematical model of risk assessment based on CVSS metrics and asset criticality, as well as a mechanism for prioritizing measures to eliminate vulnerabilities are presented. It is shown that the proposed approach transforms the asset accounting system into a proactive security management tool and forms the basis of DevSecOps practices in an educational organization.

Keywords: information security, Cyber Threat Intelligence, CMDB, CVE, vulnerability management, DevSecOps, risk assessment.

Информационная инфраструктура современного вуза включает серверы обработки персональных данных студентов, системы дистанционного обучения, научные вычислительные кластеры, сетевые устройства и рабочие станции сотрудников. Рост цифровизации образовательных процессов приводит к увеличению поверхности атаки и усложнению управления безопасностью.

Традиционная CMDB фиксирует конфигурацию оборудования и программного обеспечения, однако остается статической моделью, не учитывающей динамику публикации уязвимостей и их эксплуатацию злоумышленниками. Между моментом появления новой записи CVE и установкой обновления формируется временное окно уязвимости.

Подход Cyber Threat Intelligence (CTI) предполагает непрерывный сбор, анализ и корреляцию данных об угрозах из различных источников с целью поддержки управленческих решений. Интеграция CTI в процессы учета активов позволяет реализовать переход от реактивной модели реагирования к проактивной.

Цель работы - разработка модели потока уязвимостей, обеспечивающей автоматическое обновление уровня риска IT-активов вуза в режиме, близком к реальному времени

Модель построена как многоуровневая система обработки данных.

1. Внешние источники угроз

- Базы данных CVE (MITRE, NVD)
- RSS-каналы производителей программного обеспечения
- OSINT-источники (аналитические отчеты, публичные advisories)

2. Внутренние источники

- Результаты сканирования уязвимостей (OpenVAS, аналогичные системы)
- Данные SIEM (корреляция событий безопасности)

— Логи патч-менеджмента

3. Логические уровни обработки

— Сбор данных через API и RSS.

— Нормализация форматов и выделение идентификаторов CVE.

— Сопоставление с конфигурацией активов в CMDB.

— Расчет уровня риска.

— Формирование приоритетных задач для ИБ-подразделения.

Математическая модель оценки риска

Пусть:

$A = \{a_1, a_2, \dots, a_n\}$ - множество активов;

$V = \{v_1, v_2, \dots, v_m\}$ - множество актуальных уязвимостей.

Текущий риск актива рассчитывается по формуле:

$$R_i(t) = \sum (CVSS_k \cdot E_k(t) \cdot W_i)$$

где:

$CVSS_k$ - базовая оценка уязвимости;

$E_k(t)$ - коэффициент эксплуатационной активности (по данным СТИ);

W_i - коэффициент критичности актива.

С учетом индикаторов компрометации из SIEM:

$$R_i^{final(t)} = R_i(t) \cdot (1 + \alpha \cdot I_i(t))$$

где $I_i(t)$ - индикатор обнаруженной подозрительной активности.

Таблица 1 – Сравнение подходов к управлению уязвимостями.

Подход	Динамичность	Автоматизация	Приоритизация
Статическая CMDB	Низкая	Частичная	Отсутствует
Сканирование без СТИ	Средняя	Средняя	Ограниченная
Предложенная СТИ-модель	Высокая	Полная	Контекстная

Модель апробирована на тестовой инфраструктуре (около 150 серверов и 1200 рабочих станций). [1,2]

Полученные результаты:

— сокращение времени выявления критичных уязвимостей - на 35%;

— снижение среднего времени устранения (MTTR) - на 28%;

— выявление 20% активов, формирующих 80% совокупного риска;

— автоматическое формирование приоритетного списка задач для службы ИБ.

Каждому активу присваивается динамический атрибут «текущий уровень риска», обновляемый при публикации новой CVE или появлении события в SIEM.[3,4]

Предложенная модель обеспечивает:

- интеграцию управления активами и управления уязвимостями;
- формирование цифрового контура проактивной безопасности;
- поддержку DevSecOps-подхода в образовательной среде;
- возможность построения цифрового двойника киберустойчивости

вуза.

Особую значимость модель имеет для серверов, обрабатывающих персональные данные студентов и финансовую информацию.

Разработана динамическая модель потока уязвимостей в жизненном цикле IT-активов вуза на основе подхода Cyber Threat Intelligence.

В отличие от статической инвентаризации, предложенная система:

- автоматически интегрирует внешние и внутренние источники угроз;
- рассчитывает текущий уровень риска для каждого актива;
- обеспечивает контекстную приоритизацию действий ИБ-специалистов;
- формирует основу для внедрения DevSecOps в образовательной организации.

Таким образом, система инвентаризации трансформируется из пассивного каталога в интеллектуальный центр поддержки принятия решений в области информационной безопасности.

Список литературы

1. Формализация верификации топологии и электрической схемы для систем автоматизированного проектирования / Т. В. Скворцова, К. В. Зольников, А. М. Плотников, И. В. Скоркин // Моделирование систем и процессов. – 2024. – Т. 17, № 3. – С. 61-70. – DOI 10.12737/2219-0767-2024-59-68. – EDN DUYQNJ.
2. Щеглов, К. А. Эксплуатационная безопасность. Моделирование реализации угроз атак потенциальным нарушителем / К. А. Щеглов, А. Ю. Щеглов // Информационные технологии. – 2017. – Т. 23, № 1. – С. 34-41. – EDN VHTIPV.
3. Валеева, С. Р. Использование методологий структурного анализа для оценки уязвимостей информационной системы учета платных дополнительных образовательных услуг / С. Р. Валеева // Информационные технологии в науке,

бизнесе и образовании : сборник трудов XI Международной научно-практической конференции студентов, аспирантов и молодых ученых, Москва, 28–29 ноября 2019 года. – Москва: Московский государственный лингвистический университет, 2020. – С. 41-46. – EDN VIXWHV.

4. Волков, Н. Е. Модель защиты информации в ходе деятельности учебного отдела образовательной организации / Н. Е. Волков, Ф. О. Федин // Современная Российская наука: актуальные вопросы, достижения и инновации : сборник статей VII Всероссийской научно-практической конференции, Пенза, 15 марта 2024 года. – Пенза: Наука и Просвещение (ИП Гуляев Г.Ю.), 2024. – С. 33-35. – EDN CCHQTT.

References

1. Formalization of topology verification and electrical circuit for computer-aided design systems / T. V. Skvortsova, K. V. Zolnikov, A.M. Plotnikov, I. V. Skorkin // Modeling of systems and processes. – 2024. – Vol. 17, No. 3. – pp. 61-70. – DOI 10.12737/2219-0767-2024-59-68. – EDN DUYQHJ.

2. Shcheglov, K. A. Operational safety. Modeling the implementation of attack threats by a potential violator / K. A. Shcheglov, A. Yu. Shcheglov // Information Technologies. – 2017. – Vol. 23, No. 1. – pp. 34-41. – EDN VHTIPV.

3. Valeeva, S. R. The use of structural analysis methodologies to assess the vulnerabilities of the information system for accounting for paid additional educational services / S. R. Valeeva // Information technologies in science, business and education : proceedings of the XI International Scientific and Practical Conference of Students, Postgraduates and Young Scientists, Moscow, November 28-29, 2019. Moscow: Moscow State Linguistic University, 2020. pp. 41-46. - EDN VIXWHV.

4. Volkov, N. E. The information protection model in the course of the educational department of an educational organization / N. E. Volkov, F. O. Fedin // Modern Russian science: current issues, achievements and innovations : collection of articles of the VII All-Russian Scientific and Practical Conference, Penza, March 15, 2024. Penza: Science and Education (IP Gulyaev G.Yu.), 2024. pp. 33-35. – EDN CCHQTT.