DOI 10.37539/2949-1991.2026.41.6.031

**Инчин Алексей Николаевич,**
студент магистратуры 2 курса гр. ИСТм-41,
ФГОБУ ВО «Поволжский государственный
университет телекоммуникаций и информатики»
Inchin Aleksei Nikolaevich,
2st year master's student gr. ISTm-41,
FGOBU in «Volga State University
of Telecommunications, and Informatics»

**Шакурский Максим Викторович,** д.т.н., зав. каф. ИБ,
ФГОБУ ВО «Поволжский государственный
университет телекоммуникаций и информатики»
Shakursky Maxim Viktorovich,
d.t.n., head of the I.B. department,
FGOBU in «Volga State University
of Telecommunications and Informatics»

# МОДЕЛИРОВАНИЕ И АНАЛИЗ ВЕКТОРОВ АТАК НА ПРИВИЛЕГИРОВАННЫЕ УЧЕТНЫЕ ЗАПИСИ В СОВРЕМЕННЫХ КОРПОРАТИВНЫХ СЕТЯХ
# MODELING AND ANALYSIS OF ATTACK VECTORS ON PRIVILEGED ACCOUNTS IN MODERN CORPORATE NETWORKS

**Аннотация.** В данной статье рассматриваются вопросы математического и имитационного моделирования векторов атак, направленных на компрометацию привилегированного доступа в современных корпоративных информационных системах. Авторами проанализированы основные механизмы бокового перемещения злоумышленников (Lateral Movement) внутри доменной инфраструктуры Active Directory, включая техники перехвата учетных данных и атаку класса Pass-the-Hash. Предложена концепция построения динамических графов атак для оценки уязвимости сетевых узлов. Описаны результаты практического моделирования векторов угроз в изолированной виртуальной лаборатории, позволившие выявить ключевые слабости традиционных превентивных мер защиты и обосновать необходимость перехода к проактивным системам обнаружения аномалий.

**Abstract.** The article describes the methods of simulation and mathematical modeling of cyberattacks aimed at compromising privileged accounts in active directory domains. The mechanisms of unauthorized lateral movement of attackers using credential harvesting and pass-the-hash techniques are analyzed. A concept of dynamic attack graph construction to evaluate infrastructure vulnerability is proposed. The results of simulation modeling of threat vectors in a secure virtual sandbox are presented, proving the critical limitations of traditional rule-based access controls.

**Ключевые слова:** Информационная безопасность, моделирование атак, привилегированный доступ, боковое перемещение, Active Directory, граф атак, имитационный стенд, компрометация учетных записей.

**Keywords:** Privileged access, PAM, machine learning, UEBA, information security, anomaly detection, artificial intelligence.

Обеспечение киберустойчивости современных распределенных информационных систем требует детального понимания механизмов реализации компьютерных угроз. В условиях размытия традиционных защитных барьеров приоритетной целью для внешних

злоумышленников и внутренних нарушителей становятся учетные записи администраторов, обладающие максимальными полномочиями в сети. Моделирование векторов атак позволяет специалистам по информационной безопасности превентивно выявлять уязвимые маршруты внутри инфраструктуры, оценивать риски компрометации критически важных ресурсов и проектировать адекватные механизмы защиты до момента реального проникновения атакующих в сеть.

Наиболее опасным сценарием развития современной кибератаки является несанкционированное боковое перемещение злоумышленника внутри домена Active Directory после первичной компрометации рядовой рабочей станции. Моделирование этого процесса осуществляется с помощью построения направленных графов атак, где вершинами выступают учетные записи и хосты, а ребрами – существующие права доступа и уязвимости конфигурации. В процессе анализа такого графа выявляются цепочки доверия, которые позволяют атакующему последовательно повышать свои привилегии, переходя от одного скомпрометированного узла к другому, вплоть до получения прав администратора всего домена.

Центральным элементом моделирования векторов атак на привилегированный доступ является имитация техник извлечения учетных данных из системной памяти (Credential Harvesting). В рамках экспериментальных исследований детально анализируются механизмы работы утилит класса Mimikatz и сценарии реализации атак типа Pass-the-Hash и Pass-the-Ticket. Моделирование показывает, что использование злоумышленником легитимных хешей паролей и Kerberos-билетов позволяет ему успешно авторизоваться на серверах организации в обход стандартных парольных политик. При этом традиционные превентивные средства безопасности не фиксируют нарушений, поскольку сессия выглядит абсолютно легитимной с точки зрения протоколов авторизации.

Для безопасного исследования и верификации векторов компрометации КИС целесообразно использовать специализированные имитационные стенды на базе изолированных виртуальных машин, функционирующих под управлением современных гипервизоров. Моделирование атак в замкнутой виртуальной песочнице (Sandbox) позволяет детально изучить поведение злоумышленника на каждом этапе жизненного цикла атаки: от первичной разведки и сканирования портов до эксплуатации уязвимостей, повышения привилегий, закрепления в системе и попыток деструктивного воздействия.

Использование виртуальных коммутаторов в режиме полной изоляции трафика (Host-Only) гарантирует безопасность физической инфраструктуры организации, исключая риски выхода вредоносного кода или эксплойтов за пределы тестового контура. Кроме того, такой подход предоставляет исследователям чистую, высокоточную телеметрию и неискаженный поток системных логов событий (включая журналы безопасности Active Directory и шлюзов доступа), полностью лишенный повседневного корпоративного фонового шума.

Полученный в ходе таких симуляций массив данных отражает реальную динамику развития инцидента и является идеальной основой для обучения предиктивных моделей машинного обучения, поскольку содержит четко локализованные во времени маркеры аномального поведения.

Результаты проведенного моделирования доказывают критическую ограниченность классических систем контроля доступа. Традиционный PAM-шлюз, работающий на основе жестких ролевых правил, успешно блокирует попытки прямого несанкционированного входа, но оказывается бессилен перед LotL-атаками, когда скомпрометированная доменная учетная запись используется для выполнения стандартных системных команд PowerShell в нетипичное время. Полученные в ходе анализа графов атак выводы обосновывают необходимость перехода от статического контроля к динамическим моделям поведенческого анализа (UEBA), способным выявлять аномалии непосредственно в процессе активной сессии администратора.

*Список литературы:*

1. Олифер, В. Компьютерные сети. Принципы, технологии, протоколы [Текст]: учебное пособие для вузов / В. Олифер, Н. Олифер. – Юбилейное изд. – СПб.: Питер, 2020. – 1008 с.

2. Васильев, А. В. Методы управления привилегированным доступом в корпоративных сетях [Текст] / А. В. Васильев // Вестник Томского государственного университета. – 2020. – № 345. – с. 34-42.

3. Соколов, А. В. Защита от внутренних угроз в корпоративных информационных системах [Текст] / А. В. Соколов // Безопасность систем. – 2021. – № 2. – с. 34-41.

4. Давыдов, С. В. Анализ сетевых аномалий методами машинного обучения [Текст] / С. В. Давыдов, И. П. Сидоров // Безопасность информационных технологий. – 2023. – Т. 30, № 2. – с. 45-58.

5. Инчин, А. Н. Использование адаптивных моделей для оптимизации управления привилегированным доступом в корпоративных сетях [Текст] / А. Н. Инчин, М. В. Шакурский // Флагман науки: научный журнал. – Май 2026. – СПб.: Изд. ГНИИ "Нацразвитие", 2026. – № 5(40). – с. 12-18.