Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.056.5

Смалько
Валерий Петрович

Система мониторинга событий информационной безопасности в Active Directory

АВТОРЕФЕРАТ
на соискание ученой степени магистра технических наук
по специальности 7-06-0611-02 Иинформационная безопасность

Научный руководитель

Борботько Тимофей Валентинович

доктор технических наук, профессор

Минск 2026

ВВЕДЕНИЕ

Актуальность темы исследования обусловлена критической ролью служб каталога, в частности Microsoft Active Directory, в обеспечении непрерывности бизнес-процессов современных организаций. Являясь центральным элементом инфраструктуры аутентификации и управления доступом, Active Directory становится приоритетной целью для целенаправленных кибератак. Компрометация данного компонента неизбежно ведет к полной потере контроля над информационной системой предприятия, утечке конфиденциальных данных и нарушению целостности критически важных сервисов. Несмотря на широкое распространение средств защиты информации, статистика инцидентов последних лет демонстрирует устойчивый рост успешных атак на инфраструктуру доменов, что свидетельствует о недостаточности применяемых защитных мер.

Одной из ключевых проблем обеспечения безопасности является кризис традиционной концепции эшелонированной защиты. Практика показывает, что экстенсивное наращивание разнородных средств защиты периметра и конечных точек часто создает ложное чувство защищенности. При таком подходе основное внимание уделяется предотвращению проникновения, тогда как возможности по обнаружению злоумышленника, уже преодолевшего внешний периметр, остаются ограниченными. В результате внутри корпоративной сети формируются «слепые зоны», позволяющие атакующим длительное время скрытно развивать атаку, повышать привилегии и осуществлять горизонтальное перемещение, оставаясь незамеченными для стандартных средств мониторинга.

Существенным недостатком текущих подходов к проектированию систем защиты является нерациональное использование ресурсов в отрыве от статистики актуальных угроз. Зачастую внедрение дорогостоящих технических решений осуществляется без привязки к тактикам и техникам, реально используемым хакерскими группировками. Отсутствие научно обоснованной модели угроз приводит к тому, что системы мониторинга генерируют избыточное количество событий, не имеющих практической ценности, в то время как критически важные индикаторы компрометации игнорируются. Это создает дисбаланс, при котором ресурсы тратятся на защиту от теоретических рисков, а реальные векторы атак остаются без должного противодействия.

Особую техническую сложность представляет организация эффективного мониторинга непосредственно внутри инфраструктуры Active Directory. Стандартные настройки журналов аудита операционных систем не обеспечивают достаточной гранулярности для выявления сложных атак,

направленных на протоколы аутентификации и репликации (таких как DCSync или Golden Ticket). Более того, значительная часть вредоносной активности, связанная с разведкой и эксплуатацией уязвимостей, происходит на уровне сетевого взаимодействия между сегментами, которое зачастую не анализируется существующими средствами защиты. Необходимость глубокого анализа трафика на коммутационном оборудовании и корреляции этих данных с событиями журналов безопасности является критическим условием для своевременного обнаружения инцидентов.

Решение описанных проблем требует перехода к методологии защиты, основанной на данных. В качестве фундаментальной базы для построения адаптивной системы мониторинга целесообразно использовать матрицы MITRE ATT&CK и MITRE Engage. Данные фреймворки систематизируют знания о реальном поведении злоумышленников и позволяют трансформировать абстрактные требования безопасности в конкретные правила обнаружения и сценарии активного противодействия. Использование этих баз знаний позволяет настроить средства защиты на выявление специфических паттернов поведения, характерных для современных целевых атак, и реализовать стратегию активного обнаружения с применением технологий, описанных в соответствующих матрицах.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с приоритетными направлениями научной, научно-технической и инновационной деятельности

Тема диссертационной работы соответствует разделу 6 «Обеспечение безопасности человека, общества и государства» приоритетных направлений научной, научно-технической и инновационной деятельности в Республики Беларусь на 2021–2025 гг., утверждённых Указом Президента Республики Беларусь 7 мая 2020 г., № 156. Работа выполнялась в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники».

Цель и задачи исследования

Цель диссертационной работы заключается в разработке системы мониторинга событий информационной безопасности в Active Directory.

Для достижения поставленной цели необходимо было выполнить следующие задачи:

1. Проанализировать архитектуру и принципы работы Active Directory.
2. Проанализировать кибератаки на Active Directory.
3. Разработать систему мониторинга событий ИБ в Active Directory, которая бы учитывала современную модель угроз в отношении организации с использованием общедоступных баз MITRE и внедрения соответствующих систем защит.

Апробация результатов диссертации

Основные положения и результаты диссертации обсуждались на 60-й научной конференции аспирантов, магистрантов и студентов учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», 12-26 апреля 2024 г (г. Минск).

Опубликование результатов диссертации

По результатам исследований, представленных в диссертации, опубликовано 2 работы, в том числе 2 статьи в сборниках материалов конференций.

Личный вклад соискателя

Все основные результаты, изложенные в диссертационной работе, получены соискателем самостоятельно. Разработанная система мониторинга событий ИБ в Active Directory, является полностью достаточной для решения актуальных задач определённых и сформулированных с использованием баз знаний MITRE и актуальных угроз в отношении Active Directory. В то же время, ее можно модифицировать и менять настройки по собственному усмотрению. Применяться система может в любой организации,

использующей Active Directory для управления внутренними ресурсами организации.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Диссертация состоит из введения, трех глав, заключения и библиографического списка. Общий объем диссертации 75 страницы, 32 наименования в библиографическом списке.

Во введение приводится обоснование актуальности работы.

Первая глава носит обзорный характер. В ней приводится общее описание архитектуры Active Directory, ее назначение и основные компоненты, а также принципы функционирования и особенности взаимодействия пользователя с Active Directory.

Вторая глава посвящена анализу кибератак на Active Directory. Затрагиваются основные этапы кибератаки на Active Directory в соответствии с базой знаний MITRE ATT&CK. Рассматриваются основные техники, используемые нарушителем, а также виды кибератак на Active Directory.

В третьей главе описывается методика формулирования стратегической цели организации с точки зрения защиты, а также определяется и формулируются конкретные задачи для решения определенны цели - обнаружение. Определяются конкретные мероприятия для решения выделенных задач с учетом актуальной модели угроз нарушителя.

Как результат представляется и обосновывается разработанная система мониторинга, которая решает задачи, определенные в третей главе. Дается обоснование использования выбранных систем защиты информации и их использование в сети организации. Кроме того, предлагается и демонстрируется использование базы знаний MITRE ATT&CK, для настройки правил корреляции в системе AlienVault OSSIM.

Разработанная система может быть модернизирована, путем добавления дополнительных средств защиты по собственному усмотрению. Применяться система может в любой организации, использующей Active Directory для управления внутренними ресурсами организации.

В заключении сформулированы основные результаты диссертации.

ЗАКЛЮЧЕНИЕ

В ходе выполнения диссертационного исследования была решена научно-техническая задача по проектированию системы мониторинга событий информационной безопасности в инфраструктуре службы каталога Active Directory. Проектирование системы потребовало перехода от экстенсивного наращивания средств защиты к методологии, ориентированной на конкретные цели и модели угроз. Было обосновано, что традиционный подход, сфокусированный исключительно на эшелонированной обороне и внедрении широкого спектра технологий для предотвращения доступа, зачастую приводит к неэффективному расходованию ресурсов. Вместо хаотичного внедрения разрозненных решений, предложено выстраивание системы мониторинга как итеративного процесса, направленного на повышение стоимости реализации атаки для нарушителя и снижение ценности полученных им результатов.

Методологической базой для стратегического планирования послужил фреймворк взаимодействия с нарушителем MITRE Engage, послуживший связующим звеном между анализом операций и тактическими действиями по обнаружению и нейтрализации угроз. В рамках проектирования были выявлены «слепые зоны» внутри периметра сети, возникающие при использовании стандартных настроек аудита, которые не позволяют детально выявлять сложные векторы атак, такие как несанкционированная репликация (DCSync), подделка билетов (Golden Ticket) и распыление паролей (Password Spraying).

Для реализации предложенной концепции использован комплекс программных средств защиты, включающий систему управления событиями информационной безопасности (AlienVault OSSIM) и платформу имитации угроз (T-Pot). В составе AlienVault OSSIM задействованы модули сбора событий (Sensor) для первичной обработки журналов и серверы управления (Server) для корреляции и поведенческого анализа. Постоянный аудит защищенности хостов обеспечен интеграцией встроенного средства сканирования уязвимостей (OpenVAS). Активная часть мониторинга представлена децентрализованной сетью средств имитации (ловушек), функционирующих в изолированных контейнерах, что исключает возможность горизонтального перемещения нарушителя внутри сети при компрометации отдельной приманки.

Научная обоснованность проектных решений подкреплена разработкой алгоритмов обнаружения, базирующихся на разделе «Стратегия обнаружения» (Detection Strategy) базы знаний MITRE ATT&CK. Для каждой из критических техник (T1110.003, T1558.001, T1003.006) определены

параметры правил корреляции, включающие использование изменяемых элементов, таких как временные окна (Time Window) и пороговые значения (Thresholds). Это позволило перевести теоретические индикаторы компрометации в плоскость конкретных идентификаторов событий журналов безопасности (Event ID 4625, 4771, 4662, 4672) и анализа сетевого трафика протокола репликации (DRSUAPI), обеспечивая возможность своевременной фиксации аномальной активности.

Проектируемая архитектура обладает встроенными механизмами масштабирования и позволяет внедрять дополнительные узлы сбора данных во все сегменты сети (администрация, бухгалтерия, ИТ-служба) без изменения логики центрального аналитического ядра. Возможности дальнейшего расширения системы связаны с внедрением модулей автоматизированного реагирования на инциденты (SOAR), интеграцией внешних потоков разведывательных данных об угрозах и применением методов машинного обучения для глубокого поведенческого анализа активности пользователей и сущностей (UEBA) в среде Active Directory.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

1 – А. Смалько В. П. Система мониторинга событий ИБ в Active Directory // Информационная безопасность: сборник материалов 60-й научной конференции аспирантов, магистрантов и студентов БГУИР, Минск, 22–26 апреля 2024 г. / Белорусский государственный университет информатики и радиоэлектроники. – Минск, 2024. – С. 88–91.

2 – А Смалько В. П. Проектирование системы мониторинга событий информационной безопасности в Active Directory на основе MITRE ATT&CK и MITRE Engage // Вестник науки. – Тольятти, 2026. – Т. 2, № 1 (94). – С. 589-596