УДК 004.056.5

Интеграция технических и организационных мер защиты домена Active Directory: от сетевой сегментации до системы мониторинга инцидентов

Митрофанов М. И., Лаута О. С., Крамской Н. Н., Куракин А. С.

Постановка задачи: *в условиях высокой зависимости корпоративных инфраструктур от доменной архитектуры Active Directory (AD) защита домена рассматривается как ключевой элемент обеспечения устойчивости всей информационной системы организации. Однако практика эксплуатации демонстрирует, что даже при наличии множества технических средств защиты компрометация AD остается возможной вследствие отсутствия системной интеграции технических и организационных мер. Наблюдается фрагментарность внедрения защитных решений, несогласованность процедур администрирования и мониторинга, а также разрыв между архитектурой безопасности и процессами ее сопровождения.* ***Целью работы*** *является разработка интегрированной модели защиты домена Active Directory, объединяющей технические и организационные меры на всех уровнях инфраструктуры — от сетевой сегментации до системы мониторинга инцидентов — с формализацией критериев их критичности и взаимосвязей.* ***Используемые методы****: методология базируется на системном анализе доменной инфраструктуры, декомпозиции уровней защиты, анализе матрицы MITRE ATT&CK, методе экспертных оценок критичности мер, а также анализе журналов событий Windows для построения модели мониторинга и корреляции инцидентов.* ***Новизна:*** *предложена пятиуровневая интегрированная модель защиты Active Directory, рассматривающая систему мониторинга (SIEM–EDR) как интеграционный слой, объединяющий технические и организационные контрмеры в единую эшелонированную архитектуру. Введена классификация мер по уровню критичности в зависимости от их положения в цепочке атаки.* ***Результат.*** *Разработана структурированная модель интеграции технических и организационных мер защиты AD, сформированы таблицы соответствия векторов атак и контрмер, определены приоритеты мониторинга событий Windows и критерии критичности защитных мероприятий.* ***Практическая значимость:*** *предложенная модель позволяет выстраивать архитектуру защиты доменной инфраструктуры с учетом ограничений реальных организаций, обосновывать приоритетность внедрения мер, повышать эффективность процессов реагирования на инциденты и рационально распределять бюджет информационной безопасности.*

Ключевые слова: *Active Directory, доменная инфраструктура, информационная безопасность, сетевая сегментация, SIEM, EDR, защита в глубину, мониторинг инцидентов, MITRE ATT&CK, управление привилегированным доступом.*

Актуальность

Рассматривая современное состояние корпоративной информационной безопасности (ИБ), невозможно не отметить, что развертывание службы ката-

Библиографическая ссылка на статью:
Митрофанов М. И., Лаута О. С., Крамской Н. Н., Куракин А. С. Интеграция технических и организационных мер защиты домена Active Directory: от сетевой сегментации до системы мониторинга инцидентов // Системы управления, связи и безопасности. 2026. № 1. С. 219-247. DOI: 10.24412/2410-9916-2026-1-219-247

Reference for citation:
Mitrofanov M. I., Lauta O. S., Kramskoy N. N., Kurakin A. S. Integration of technical and organizational measures to protect the Active Directory domain: from network segmentation to incident monitoring system. *Systems of Control, Communication and Security*, 2026, no. 1, pp. 219-247 (in Russian). DOI: 10.24412/2410-9916-2026-1-219-247

логов Active Directory (AD) в корпоративных средах представляет собой дефакто стандарт для администрирования аппаратных, программных и сетевых систем, используемых для организации единого информационного и рабочего пространства (ИТ-инфраструктуры) организации на платформе Windows. Это утверждение остается справедливым даже в условиях активной тенденции импортозамещения и постепенного перехода на отечественные решения типа Astra Linux и другие, наблюдаемой в Российской Федерации.

Анализируя текущую ситуацию, следует признать, что Windows и AD попрежнему широко используются, и защита AD-домена остается стратегической задачей для подавляющего большинства организаций. Более того, процесс импортозамещения AD в организациях часто сталкивается с непреодолимыми препятствиями, когда полный отказ от связки Windows и AD становится невозможным по ряду технических причин. Особенно критичной эта ситуация становится на этапе после того, как техническое решение уже составлено и согласовано со всеми необходимыми инстанциями и регуляторами. Нередко внезапно выясняется, что существует критическое программное обеспечение (ПО), применяемое исключительно на платформе Windows и корректно функционирующее только в условиях AD-домена [1-5].

Следовательно, часть инфраструктуры продолжает функционировать по «неимпортозамещенной» схеме, при этом ежедневные задачи по администрированию и защите этого сегмента не исчезают. Даже если организация избегает подобных «подводных камней» при миграции на отечественные решения, необходимо согласиться, что такой переезд представляет собой продолжительный процесс, который в крупных инфраструктурах с большим количеством унаследованных систем вполне может занять годы. Атаки на AD, согласно практическому опыту, происходят ежедневно, и факт миграции организации на альтернативное решение не послужит оправданием в случае компрометации системы в настоящий момент. Таким образом, если AD используется в организации здесь и сейчас, нельзя пренебрегать мероприятиями по защите, несмотря ни на какие обстоятельства.

Защита корпоративной ИТ-инфраструктуры организации всегда представляет собой комплексный процесс, который можно концептуализировать как эшелонированную многоуровневую оборону. В организациях среднего и крупного масштаба практически всегда присутствуют периметровые межсетевые экраны, системы защиты веб-приложений (Web Application Firewall (WAF)), шлюзы для защиты почтового трафика, системы обнаружения вторжений (Intrusion Detection System (IDS)) и системы предотвращения вторжений (Intrusion Prevention System (IPS)), защита конечных точек посредством антивирусных решений и систем класса кибербезопасности, которые обнаруживают и реагируют на угрозы на конечных устройствах (Endpoint Detection and Response (EDR), сегментирование по виртуальным локальным сетям и подсетям, различные политики безопасности, виртуальные частные сети для удаленных сотрудников, процедуры управления обновлениями и множество других защитных механизмов. Все эти компоненты являются составными частями единой страте-

гии, и все защитные решения с их администраторами работают ради достижения одной цели [3, 6-11].

Однако проблема многих существующих материалов и руководств по защите AD заключается в том, что их разрабатывают администраторы домена для администраторов домена. Это представляется закономерным, но не всегда эффективным подходом. На первый взгляд логика очевидна – один специалист по AD создает руководство об AD для других специалистов в этой области. Но в действительности такие рекомендации часто охватывают исключительно архитектуру и настройку, тогда как защита AD как ключевого элемента инфраструктуры организации требует комплексного междисциплинарного подхода.

Размышляя о структуре команды безопасности, необходимо понимать, что сетевые инженеры обеспечивают сегментацию сети, настройку межсетевых экранов и систем IDS/IPS. Инженеры по управлению уязвимостями следят за своевременным обновлением и установкой исправлений в системах. Команда центра операций безопасности (Security Operations Center (SOC)) анализирует журналы и события безопасности, а также реагирует на инциденты для предотвращения атак. Системные инженеры и администраторы поддерживают серверы и рабочие станции, производят их замену или модернизацию, настраивают резервное копирование. Инженеры по информационной безопасности проводят аудиты, тесты на проникновение, следят за соответствием нормативным требованиям. Руководители служб информационной безопасности (Chief Information Security Officer (CISO)) отвечают за управление ИБ в организации, включая выработку организационных мер защиты. И наконец, администраторы домена отвечают за управление доменной инфраструктурой, настройку политик безопасности, контроль учетных записей и групп [10, 11, 13].

В случае небольшой инфраструктуры описанные функции распределяются на меньшее количество специалистов, однако общая картина от этого не изменяется. AD является ключевым элементом корпоративной инфраструктуры, и поэтому подход к ее защите обязан быть комплексным. Администратор домена в большинстве случаев не обязан знать, что такое EDR, какие политики следует настроить на межсетевом экране (МЭ) и каково состояние средств антивирусной защиты (САВЗ) и закрытия уязвимостей на конечных точках в определенный момент времени. Таким образом, советы по этим мероприятиям не будут включены в рекомендации по повышению уровня защиты AD. Но при этом всё это очень важно для безопасности домена.

Согласно исследованиям, около 40% атак на AD заканчиваются успехом для злоумышленников. Анализируя процесс развития атаки, необходимо признать, что для злоумышленников, чтобы начать какие-либо вредоносные действия, направленные на AD, требуется первоначальный доступ в сеть организации. Имея такой доступ, нарушители уже могут выполнить доставку вредоносного ПО на хосты для подготовки плацдарма внутри сети и дальнейшего продолжения атаки. Сложность получения первоначального доступа атакующими напрямую зависит от количества точек входа – систем, по той или иной причине имеющих существенные пробелы в безопасности. Совокупность точек входа называется поверхностью атаки (Attack Surface (AS)). Чем меньше по-

верхность атаки, тем сложнее злоумышленнику скомпрометировать систему, а если проникновение все же произойдет, это поможет замедлить его продвижение внутри сети. В роли точек входа могут выступать открытые в интернет порты, незащищенные протоколы, неполное покрытие конечных устройств САВЗ, устаревшие версии операционных систем, ПО и многое другое [10-14].

Анализ релевантных работ

В отечественной и зарубежной научной литературе проблематика защиты доменных инфраструктур, функционирующих на базе технологии AD, получила значительный исследовательский интерес, особенно усилившийся в период с 2018 по 2025 годов на фоне роста числа целевых атак на привилегированные учётные данные и контроллеры домена [15]. Однако, детальный анализ научных публикаций свидетельствует о том, что сложившаяся исследовательская традиция изучения данной проблематики исторически развивалась по двум самостоятельным, практически не пересекающимся векторам: технико-инженерному и организационно-управленческому. Ни один из них, взятый в отдельности, не предоставляет инструментария, достаточного для построения комплексной системы защиты доменной среды.

Значительный вклад в разработку технико-инженерного вектора обеспечения безопасности доменных сред внесли исследования, посвящённые анализу векторов атак на протоколы аутентификации Kerberos и NTLM (New Technology LAN Manager), механизмам компрометации привилегированных учётных записей, а также средствам обнаружения и предотвращения вторжений [16]. В рамках данного направления разрабатываются технические механизмы защиты: микросегментация сети, применение криптографических протоколов, конфигурирование объектов групповой политики (Group Policy Object (GPO)), внедрение систем класса SIEM (Security Information and Event Management) и EDR, а также реализация модели привилегированного доступа (Privileged Access Management) [17]. Работы таких исследователей, как [15], предлагают алгоритмические подходы к обнаружению аномалий в AD с применением методов машинного обучения, достигая показателей сбалансированной метрики для оценки моделей классификации в машинном обучении до 0,91 (F-мера) при выявлении наиболее распространённых атак на AD.

В обзорном исследовании [18], охватившем 35 работ по защите AD за период 2021–2024 годов, установлено, что более 90% публикаций технического профиля концентрируются на конкретных классах атак и соответствующих контрмерах – в ущерб системному взгляду на всю инфраструктуру защиты. Вместе с тем следует констатировать существенную методологическую ограниченность данного направления. В подавляющем большинстве технических исследований субъект управления ИБ – администратор, оператор SOC, сотрудник службы ИБ – фигурирует лишь в качестве пассивного технического агента, обслуживающего систему защиты, но не как полноправный элемент социотехнической системы. Человеческий фактор, организационные процессы и управленческие решения, непосредственно определяющие эффективность применяемых технических мер, остаются за пределами рассмотрения [19].

Параллельно развивается иная исследовательская традиция, в рамках которой обеспечение ИБ рассматривается сквозь призму менеджмента и организационных процессов. Труды в области управления рисками ИБ (ISO/IEC 27001, NIST SP 800-53) [20], построения моделей нарушителя, разработки политик безопасности, обучения персонала и аудита соответствия нормативным требованиям формируют самостоятельную научную школу, акцентирующую внимание на процессных и поведенческих аспектах защиты информации [21]. Концепция социотехнической системы, восходящая к работам [22] и развитая применительно к кибербезопасности в исследованиях [19], убедительно демонстрирует, что устойчивость организации к киберугрозам определяется не техническими средствами в отрыве от контекста, а системой взаимодействия людей, процессов и технологий.

Однако и данное направление несёт в себе принципиальное ограничение. При всей концептуальной глубине организационного подхода его авторы, как правило, оперируют обобщёнными моделями информационных систем, не учитывая специфику архитектуры AD – её иерархическую доменно-лесную структуру, механизмы делегирования административных полномочий, особенности Kerberos и протокола быстрого доступа к каталогам (Lightweight Directory Access Protocol (LDAP)), а также процессы репликации между контроллерами домена. Рекомендации в области политик безопасности зачастую формулируются на уровне общих принципов – разделения обязанностей, минимизации привилегий – без их операционализации применительно к конкретным объектам AD: организационным единицам, группам безопасности, объектам GPO и схемам делегирования прав [23].

Таким образом, проведённый анализ обнаруживает устойчивое противопоставление двух взаимосвязанных понятий в научном освоении проблемы защиты доменных инфраструктур. Технически ориентированные исследования разрабатывают высокоэффективные контрмеры против конкретных паттернов атак, однако абстрагируются от организационного контекста их применения. Организационно ориентированные исследования формируют концептуальный аппарат управления ИБ, но не обладают необходимой технической детализацией для его адаптации к специфике среды AD.

Описанный концептуальный разрыв имеет непосредственные практические последствия. По данным ряда исследований [16], более 40% компрометаций доменной инфраструктуры происходит в организациях, располагающих формально достаточным набором технических средств защиты. Причиной подобных инцидентов, как правило, является отсутствие организационных процессов, обеспечивающих жизненный цикл этих средств: своевременное обновление конфигураций, разграничение ролей администрирования, проведение регулярного аудита и отработку процедур реагирования на инциденты. Применение передовых SIEM-систем оказывается нерезультативным при отсутствии регламентов анализа оповещений; внедрение сегментации сети не достигает цели без чётко формализованных политик межсегментного взаимодействия.

Учитывая вышеизложенное, формулируется противоречие в практике защиты AD. С одной стороны, существует широкий спектр технических

средств защиты: МЭ, IDS, САВЗ, системы управления привилегированным доступом и многие другие решения. С другой стороны, практика показывает, что даже при наличии всех этих технических средств организации продолжают становиться жертвами успешных атак на AD.

А противоречие в теории заключается в фрагментарном подходе к проблеме защиты AD, когда технические решения разрабатываются изолированно от организационных мер, а исследования фокусируются либо на технических аспектах, либо на организационных процессах, но редко рассматривают их интеграцию как единую систему. Это теоретическое противоречие порождает практические проблемы, когда наличие передовых технических средств защиты не приводит к желаемому уровню безопасности из-за отсутствия соответствующих организационных процессов их поддержки [1-6].

На основе выявленного противоречия сформулирована гипотеза исследования: эффективная защита доменной инфраструктуры AD достигается не только через внедрение технических средств защиты на различных уровнях (сетевой периметр, сетевая инфраструктура, доменная архитектура, конечные точки), но через системную интеграцию этих технических средств с организационными мерами (политиками, процедурами, регламентами), создающую многоуровневую эшелонированную систему защиты с централизованным мониторингом и реагированием на инциденты.

Интеграция технических и организационных мер защиты домена Active Directory

Интеграция технических и организационных мер защиты домена AD основывается на комплексном подходе (рис. 1), включающем: анализ структурированной базы знаний, описывающей тактики, техники и методы, используемые киберпреступниками при атаках на информационные системы (матрицы MITRE ATT&CK (Adversarial Tactics, Techniques & Common Knowledge)) для систематизации векторов атак на; декомпозицию защитных мер по уровням инфраструктуры; метод экспертных оценок для определения критичности мер; анализ событий безопасности Windows для построения системы мониторинга инцидентов [10, 11, 13, 18].

Рис. 1. Комплексный подход к защите

В основе модели лежит принцип эшелонированной защиты (Defense in Depth), предполагающей создание множественных барьеров на пути атакующего (рис. 2).

Рис. 2. Пятиуровневая модель защиты Active Directory

Рассматривая первый уровень защиты – сетевой периметр – необходимо начать с базовых мероприятий по сокращению поверхности атаки (рис. 3).

Рис. 3. Первый уровень защиты

На все системы организации, не только в домене, а вообще везде, необходимо установить антивирусы с централизованным управлением, а также регулярно обновлять антивирусные базы не менее одного раза в сутки. Это поможет обнаружить и удалить известные вредоносные программы, попавшие в систему. Провести аудит политик антивируса, убедиться, что компоненты антивируса включены на всех системах, а централизованные политики запрещают отключение защиты, завершение работы и удаление САВЗ без ввода пароля администратора защиты, который должен быть достаточно сложным.

Обновление операционных систем представляется невероятно важным мероприятием. Минимальное требование, которое необходимо соблюдать: система должна быть поддерживаемой производителем, то есть для нее должны выходить обновления безопасности. Использование устаревших операционных систем, снятых с поддержки, приводит к тому, что новые уязвимости обнаруживаются, но не закрываются. Соответственно, поверхность атаки на таких системах будет только расти.

Помимо закрытия уязвимостей, в новых системах могут появляться новые функции безопасности, которые разрабатываются в ответ на изменение ландшафта угроз. Аналогичная ситуация с программным обеспечением: в старых версиях могут быть уязвимости, которые будут эксплуатироваться злоумышленниками в различных вредоносных целях: вызов отказа в обслуживании, раскрытие и перехват данных, повышение привилегий. Необходимо заметить, что в любой крупной корпоративной инфраструктуре есть унаследованные системы, миграция которых на новое решение невозможна по тем или иным причинам. В этом случае требуется принять компенсирующие меры: установить все доступные исправления безопасности, вывести хост из домена, поместить в отдельную подсеть и ограничить использование минимально необходимыми задачами.

Усиление фильтрации контента, передаваемого по электронной почте, представляет собой критически важную меру, поскольку наиболее часто применяемый способ получить первоначальный доступ – это фишинговые электронные письма, классифицируемые как T1566 в матрице MITRE ATT&CK. На корпоративную почту направляется письмо с вредоносной нагрузкой, в роли которой может быть исполняемый файл, ссылка на недоверенный сайт или текстовый документ с макросом, который активирует вредоносный код при открытии. Для фильтрации электронной почты прежде всего требуется реализовывать технологии проверки подписей, чтобы быть уверенным, что адрес отправителя не был подменен (рис. 4). К таким технологиям относятся Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), Domain-based Message Authentication, Reporting and Conformance (DMARC). Также целесообразно использовать решения типа «песочница» для динамического анализа ссылок и исполняемых файлов или вовсе ограничить прием писем с файлами расширений .exe (исполняемый файл), .ps1 (скрипт PowerShell), .bat (пакетный файл) и так далее, которые могут быть потенциально вредоносными. «Песочница» (sandbox) – изолированная среда, где можно безопасно запускать и анализировать неизвестные файлы, не рискуя повредить рабочие системы. Она помогает выявлять вредоносное поведение, которое не всегда замечают антивирусы или другие средства защиты.

Блокировка подключения недоверенных флеш-накопителей также относится к мерам получения первоначального доступа. Первоначальный доступ может быть достигнут через зараженные USB-накопители, и ущерб может быть катастрофическим. Яркий пример – вирус Stuxnet, который вывел из строя 20% иранских центрифуг для обогащения урана. Для защиты можно применять по-

литику «белых списков», разрешая запуск на конечных устройствах только для доверенных флеш-накопителей.

Рис. 4. Предотвращение первоначального доступа

Переходя ко второму уровню защиты – сетевой инфраструктуре – необходимо вынести контроллеры домена в отдельный сегмент (рис. 5).

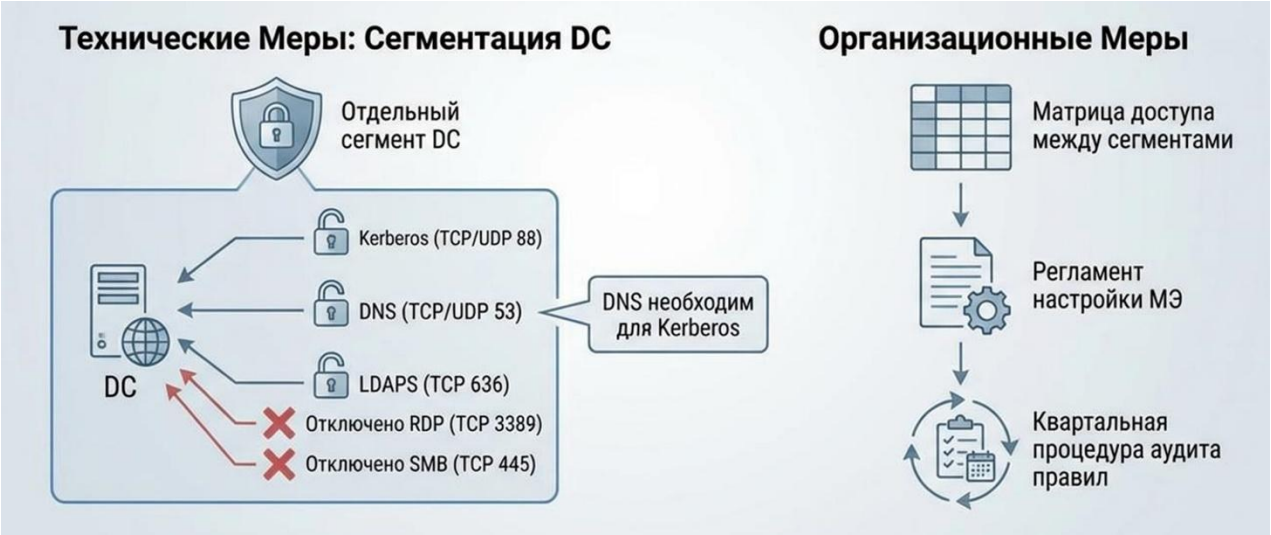

Рис. 5. Изоляция и сегментация

Изоляция контроллеров домена (Domain Controller (DC)) в отдельный сегмент сети позволяет минимизировать риски бокового перемещения. Боковое перемещение – процесс, при котором злоумышленник, получив доступ к одной системе в сети, пытается расширить свою активность, перемещаясь к другим системам. Вынесение DC в отдельный сегмент позволяет уменьшить вероятность такого перемещения. На контроллерах домена должны быть доступны только необходимые сервисы (например, Kerberos); распределённая иерархическая система, преобразующая доменные имена в IP-адреса (Domain Name System (DNS); сетевой протокол для доступа, поиска и управления данными в

службе каталогов с использованием технологии шифрования (Lightweight Directory Access Protocol over SSL (LDAPS)). Это снизит вероятность успешной эксплуатации злоумышленником уязвимостей в других сервисах. Протоколы удалённого рабочего стола (Remote Desktop Protocol (RDP)) и удалённого доступа к файлам, принтерам и другим сетевым ресурсам (Server Message Block (SMB)), которые часто используются для бокового перемещения, должны быть отключены или ограничены. В этом случае злоумышленнику необходимо сначала скомпрометировать систему в сегменте, которая имеет доступ к DC, что усложняет задачу и дает время для реагирования. Важно отметить, что DNS отключать нельзя, так как Kerberos использует его для создания билетов.

Ограничение выхода в интернет для административных учетных записей является критической мерой. Доступ должен быть запрещен как из-под доменных административных учетных записей, так и из-под локальных администраторов. Если администраторам требуется выйти в интернет, они должны делать это из-под обычных, непривилегированных учетных записей. Ограничения такого рода можно настроить, например, на МЭ нового поколения (Next-Generation Firewall (NGFW)) с помощью интеграции с LDAP. Эта мера уменьшит риски несанкционированной сетевой активности привилегированных учетных записей.

Усиление сетевой сегментации рекомендуется реализовывать путем выделения сетей различных подразделений организации в отдельные сегменты (рис. 6).

Рис. 6. Сетевая сегментация

Передачу данных между сегментами сети необходимо ограничить лишь минимально необходимым перечнем портов и протоколов для осуществления рабочих процессов организации. Это замедлит продвижение злоумышленников по инфраструктуре в случае проникновения. Медленнее продвижение означает больше времени на реагирование. Анализ показывают, что сетевая сегментация значительно усиливает защиту, предотвращая атакующим легкое перемещение

через сеть, ограничивая нарушения в пределах одного сегмента и защищая чувствительные данные через изоляцию критических активов.

Усиление конфигураций сетевых устройств требует административного отключения незанятых портов, запрета трафика по незащищенным протоколам передачи файлов (например, File Transfer Protocol (FTP)) и отказа от использования виртуальных локальных компьютерных сетей (Virtual Local Area Network (VLAN)) по умолчанию. Доступ к управлению сетевыми устройствами должен осуществляться с доверенных адресов администраторов. Также в корпоративных средах предпочтительнее применять протоколы для сетевой аутентификации, авторизации и учёта через AAA-сервер (Authentication, Authorization, Accounting) типа RADIUS (Remote Authentication Dial-In User Service) или TACACS+ (Terminal Access Controller Access-Control System Plus). Обязательно обновлять прошивку (рис. 7).

Мониторинг трафика через системы IPS/IDS в контексте предотвращения атак на AD должен отслеживать подозрительный трафик SMB. Если хост соединяется с двадцатью другими за минуту по порту 445, это аномально и может указывать на вредоносную активность. Сетевой инженер может настроить правила для детекции такого поведения. Изоляция сервисов информационной безопасности в отдельный сегмент является хорошей практикой, когда сервисы, относящиеся к обеспечению ИБ организации, выносятся в отдельный сетевой сегмент. Передачу данных между этим сегментом и остальной сетью необходимо ограничить лишь минимально необходимым перечнем портов и протоколов, необходимых для работы защитных решений и выполнения мониторинга.

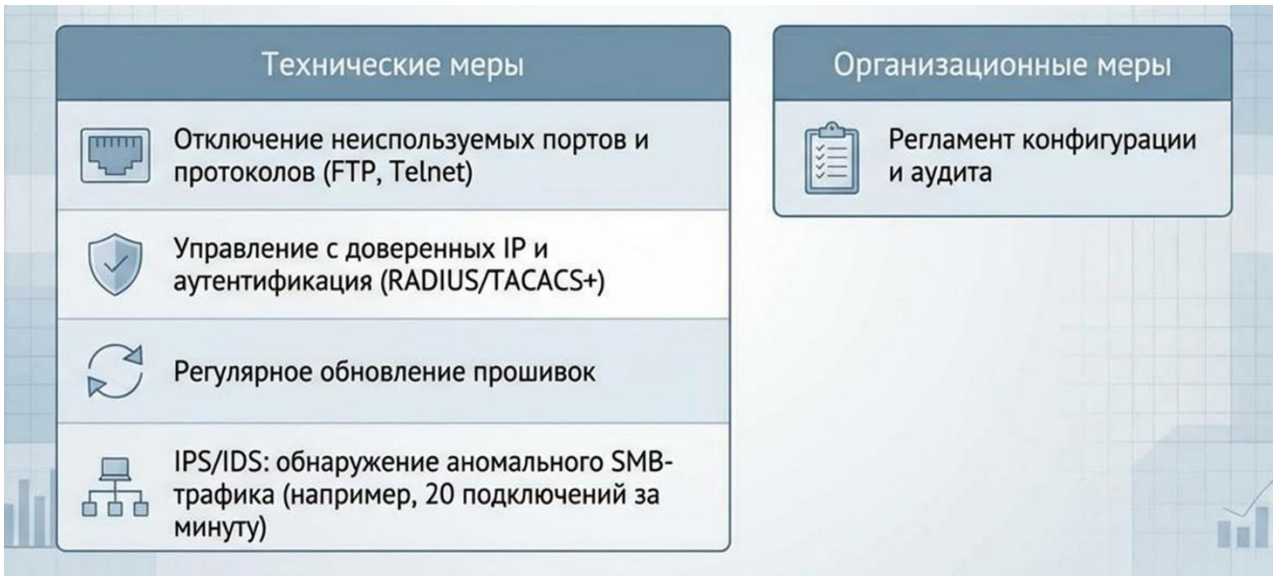

Рис. 7. Усиление конфигураций сетевых устройств

Третий уровень защиты – доменная архитектура – требует ограничения привилегий администраторов. Лучше избегать неограниченных или избыточных привилегий. Например, в организации есть несколько администраторов, при этом их обязанности различаются. Кто-то отвечает за один отдел или департамент, кто-то за другой, кто-то за серверы, кто-то за управление контрол-

лерами домена и политики групповой политики. Зачем назначать им права, не требующиеся для выполнения конкретных обязанностей? Целесообразно руководствоваться принципом наименьших привилегий (Principle of Least Privilege, PoLP) (рис. 8).

Рис. 8. Ролевая модель и делегирование

Отключение протокола сетевой аутентификации NTLM, где это возможно, должно быть выполнено полностью в пользу Kerberos. Это исключает атаки, которые используют недостатки протокола NTLM, для аутентификации в средах Windows, а также кражу хэшей паролей. Если критичные приложения нарушают работу, то можно добавить через групповую политику исключения для конкретных серверов. В процессе перехода на Kerberos нужно убедиться, что для всех сервисов корректно настроены уникальные имена, которые идентифицируют экземпляр службы в домене AD (Service Principal Name (SPN)), присутствует синхронизация времени по протоколу NTP (Network Time Protocol) (расхождение по времени более 5 минут может нарушить работу протокола), и настроено делегирование для многоуровневых приложений.

Однако полное отключение NTLM нежелательно в сложных или гибридных средах. Там могут возникать ситуации, когда поддержка Kerberos затруднена из-за отсутствия служб DNS и аутентификации пользователей, компьютеров и служб в домене AD (Netlogon). Если отказаться от NTLM не получается, можно включить подпись SMB как способ митигации атаки NTLM Relay. Отключение протокола разрешения имён в сетях, в которых отсутствует DNS-сервер (Link-Local Multicast Name Resolution (LLMNR)) также необходимо, поскольку это устаревший протокол, используемый для разрешения имен в случаях, когда DNS недоступен (рис. 9). Он уязвим к атакам «человек посередине» – злоумышленник может принимать запросы на свой компьютер и перехватывать пароли. Если DNS присутствует, протокол можно отключить через групповую политику.

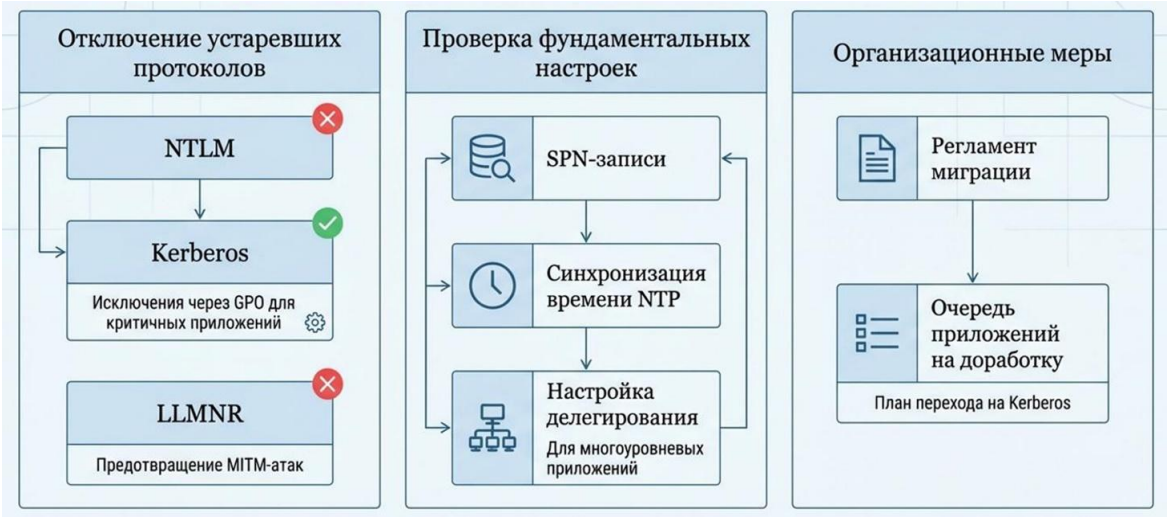

Рис. 9. Усиление протоколов и конфигурации

Ограничение попыток входа через политики AD необходимо включить, чтобы предотвращать атаки подбора паролей или распыления пароля (Brute Force/Password Spraying). Это делается через редактор групповых политик в разделе «Политика блокирования учетной записи». Здесь можно задать порог блокировки (через какое количество неудачных вводов учетная запись будет заблокирована) и сброс счетчика (через какое время счетчик неудачных попыток сбрасывается). Эти значения необходимо задавать разумно, чтобы не вызвать атаку отказа в обслуживании с целью блокировки учетных записей и сократить число обращений в техническую поддержку (рис. 10).

Рис. 10. Управление доступом: политики и процедуры

Также в этом контексте нелишне упомянуть, что в рамках организации может быть целесообразно задать ограничение входов на компьютеры в пределах одного департамента.

Сложность паролей определяется политикой паролей в AD, расположенной по соседству с политикой блокирования. Она определяет требования к сложности пароля и сроку его действия. Необходимо задать адекватный срок действия пароля (30-40 дней), длину от 12 символов и включить историю хра-

нения паролей, чтобы пользователь не смог изменять пароль на использовавшийся ранее. Имеет смысл применять отдельную парольную политику для учетных записей администраторов с более строгими правилами.

Внедрение системы, которая автоматически генерирует, управляет и защищает пароли локальной учётной записи администратора на компьютерах в домене LAPS (Windows Local Administrator Password Solution) решает проблему единообразных паролей локальных администраторов (рис. 11).

Рис. 11. Парольная политика и LAPS

Учетной записи локального администратора на каждой системе следует присвоить уникальный случайно сгенерированный пароль. Если при настройке каждого компьютера в сети на нем создается одна и та же учетная запись локального администратора с одним и тем же паролем, это открывает серьезную брешь в безопасности. После компрометации одного устройства злоумышленник получит административный доступ на всех остальных устройствах в сети. LAPS решает эту проблему, автоматически генерируя уникальные пароли для локальной учетной записи администратора на каждом компьютере. Это означает, что даже если злоумышленник получит доступ к одному устройству, он не сможет использовать этот пароль для доступа к другим. Кроме того, LAPS предоставляет возможность смены пароля через заданный интервал времени, что также повышает безопасность. Проблема LAPS заключается в том, что для развертывания решения требуется функциональный уровень домена (Domain Functional Level) 2016 и выше, а хосты должны быть под управлением Windows 10 21H2 для стационарных персональных компьютеров и Windows Server 2019 для серверов или новее. Здесь встает задача по обновлению операционных систем, упоминавшаяся выше.

Пароль служебной учётной записи для службы распределения ключей (Kerberos Ticket-Granting Ticket (KRBTGT)) представляет особую важность (рис. 12). KRBTGT – сервисная учетная запись, пароль которой применяется для шифрования билетов Kerberos с помощью центра распространения ключей Kerberos (Kerberos Distribution Center, KDC). Компрометация пароля может привести к серьезным последствиям, включая реализацию атаки «золотой би-

лет» (Golden Ticket). Эта атака ведет к полной компрометации домена позволяя злоумышленнику имитировать любую учетную запись, включая администратора домена. Менять пароль KRBTGT рекомендуется не менее одного раза в год и немедленно при подозрении на компрометацию. Это небыстрая процедура, занимающая не менее 10 часов, причем требуется сменить пароль дважды для обеспечения сброса зашифрованной структуры данных, которая служит цифровым пропуском для доступа к различным сервисам (билетом) в протоколе Kerberos.

Рис. 12. Политика безопасности и регламенты

Ограничение доступа к базе данных учётных записей безопасности в операционной системе Windows (Security Account Manager (SAM)) следует реализовать для анонимных пользователей, а также запретить удаленный доступ. База SAM хранит хэши паролей всех локальных учетных записей. Если анонимные пользователи или злоумышленники получат к ней доступ они могут украсть эти хэши и взломать пароли. Количество предыдущих подключений к кэшу базы данных SAM должно быть ограничено. Если у злоумышленника будет возможность подключиться к кэшу SAM много раз подряд, он может подобрать пароли методом грубой силы.

Ограничения времени хранения кэша в lsass.exe (Local Security Authority Process) необходимы, поскольку процесс lsass.exe хранит в памяти токены (ключи доступа) пользователей. Если токены остаются там слишком долго, это повышает риск кражи. За настройку времени очистки памяти процесса lsass.exe от учётных записей пользователей, завершивших сеанс отвечает ключ TokenLeakDetectDelaySecs типа DWORD. Рекомендуемое значение – не более 10 с. Аудит lsass.exe для контроля несанкционированных подключений целесообразно включить для всех операций с lsass.exe. Это позволит оперативно узнавать о попытках сохранения информации о текущем состоянии (дампе) памяти.

Ограничения на доступ пользователей к резервной копии AD базы данных NTDS (NT Directory Services), хранящейся в файле NTDS.DIT (Directory Information Tree (DIT)) критически важны. Файл NTDS.DIT содержит все дан-

ные домена, включая пароли. Если злоумышленник получит к нему доступ, например, через резервную копию, он сможет взломать пароли в офлайн-режиме. Требуется открыть доступ к файлу только для тех администраторов домена, которым такой доступ нужен для работы.

Четвертый уровень защиты – конечные точки – требует комплексного подхода. Под конечными точками понимаются компьютеры, ноутбуки, смартфоны, планшеты, серверы и другие устройства, через которые пользователи могут получить доступ к корпоративным ресурсам. Пароль BIOS на конечной точке может быть надежным с точки зрения политики безопасности, антивируса, EDR и осведомленности пользователя. Но это мало поможет против внутреннего нарушителя, который загрузит автономную операционную систему непосредственно с внешнего носителя (например, LiveCD Kali Linux) и украдет хэши паролей локальных или доменных учетных записей из файла SAM или вовсе сделает побитовую копию диска. Установленный пароль BIOS заблокирует загрузку с внешних носителей и защитит от несанкционированного изменения настроек (рис. 13).

Рис. 13. Политики BIOS и загрузки

Контроль запуска программ и исполняемых файлов на самом деле является несложной задачей. Если в организации не используется большое количество различных программ и специалисты по безопасности точно знают, какое именно программное обеспечение требуется для работы, можно реализовать политику «белых списков» для программного обеспечения, то есть «запрещено все, что явно не разрешено». Другой хороший вариант – реализовать блокировку запуска неподписанных исполняемых файлов и скриптов (например, PowerShell, Visual Basic Script). Это существенно облегчит работу по реагированию на инциденты безопасности, потому что в условиях такого «зачищенного» ландшафта нелегитимная активность будет видна очень хорошо.

Резервное копирование необходимо настроить таким образом, чтобы резервные копии хранились на отдельном сервере, не входящем в домен, а права на удаление и изменение резервных копий имелись только у специально выделенной учетной записи, также не входящей в домен (рис. 14). Такая мера помо-

жет сохранить резервные копии в случае компрометации домена и попытки удалить или зашифровать информацию на атакованных системах.

Рис. 14. Политики BIOS и загрузки

Частота резервных копий должна быть такова, чтобы отказ какого-либо хоста не приводил к потере критического объема информации. Исходя из этого же соображения, для критических систем лучше обеспечить создание и хранение как минимум двух экземпляров каждой резервной копии. Делать копии хорошо, но еще лучше быть уверенным, что восстановление произойдет штатно. Для этого необходимо внедрить процедуру проверки целостности резервных копий и периодически проводить тестовые восстановления из резервной копии.

Настройка логирования имеет решающее значение. Если или когда система будет скомпрометирована и начнется расследование, для восстановления картины произошедшего качество и глубина логов будет иметь решающее значение. Лучшая практика по хранению логов – их отправка на удаленный сервер. Если по каким-либо причинам реализовать это не представляется возможным, следует как минимум позаботиться об увеличении объёма хранимых записей о действиях в системе, чтобы история событий сохранялась дольше и была доступна для последующего анализа. Так, для журнала Security.evtx можно рекомендовать объем не менее 200 Мбайт.

Пятый уровень защиты – система мониторинга и реагирования – представляет собой интеграционный слой, объединяющий все предыдущие уровни. Защитные решения это хорошо и правильно, но все же, по крайней мере пока, для эффективного противодействия угрозам требуется участие аналитиков. И здесь появляется две проблемы:

1. Первая – система защиты домена состоит из множества решений по ИБ, которые генерируют тысячи событий в секунду. Хуже того, эти события надо сопоставлять между собой, потому что сообщение о подозрительном файле в письме от почтового шлюза, событие исходящего соединения на неизвестный IP с МЭ, скачивание неизвестного скрипта и поступившая следом заявка

пользователя с формулировкой «у меня тут ничего не работает» могут быть звеньями одной цепи.

2. Вторая проблема заключается в том, что для эффективной работы аналитикам необходимо использовать минимум две разные технологии мониторинга, обнаружения и реагирования на угрозы (рис 15).

Рис. 15. Роль SIEM и EDR в комплексной защите

Первая – слабого приближения, которая позволяет видеть картину в инфраструктуре в целом. Она собирает данные из разных защитных решений, приводит к виду, понятному человеку, обогащает контекстом и сопоставляет друг с другом. Это система управления информацией и событиями безопасности (SIEM), которая предоставляет интерфейс для аналитиков угроз для запроса, объединения связанных событий и анализа достоверности этих предупреждений. SIEM показывает общую картину и занимается автоматизацией анализа событий.

Вторая – это инструмент для тонкой работы (EDR). Он нужен, когда SIEM уже просигнализировал о подозрительной активности, но ее специфика и происхождение понятны не полностью. EDR позволяет эффективно противостоять сложным угрозам, которые не детектируются обычными антивирусными решениями. Решение такого класса позволяет действовать точечно: изолировать узел; убить процесс; собрать цифровые доказательства о киберпреступлении.

Системы SIEM в большинстве случаях являются примерами централизованных серверов, которые собирают и анализируют данные от систем EDR. Без EDR аналитик может узнать об атаке из SIEM, но не может быстро остановить ее на конечной точке. Без SIEM EDR найдет вредоносное ПО на одном компьютере, но не даст быстро увидеть масштаб проблемы.

Пример применения

Злоумышленник отправляет поддельные письма или создаёт фальшивые сайты, чтобы выманить у пользователей пароли или банковские данные. SIEM замечает подозрительное письмо с вложением от почтового шлюза, исходящие обращения на подозрительный уникальный адрес ресурса (Uniform Resource Locator (URL)) от МЭ, система безопасности компьютера зафиксировала множество неудачных попыток входа (множественные события 4625 от журнала Security хоста). И дает возможность быстро связать эти события в один инцидент. EDR на зараженном компьютере обнаруживает запуск скрипта из вложения, видит попытку кражи учетных данных через LSASS, и дает возможность быстро принудительно закрыть процесс, получить файл на анализ и запустить подозрительный файл в изолированной виртуальной среде. В бюджете ИБ не прописаны расходы на приобретение таких решений? Можно использовать бесплатные открытые решения.

Отслеживание характерных событий в контексте защиты домена у аналитика, работающего с SIEM-EDR, будет достаточно информации для анализа. Для примера приведем несколько важных индикаторов из журнала событий Windows, которые надо отслеживать:

– события 4624 (успешный вход) и 4625 (неудачный вход) позволяют выявлять атаки методом перебора и подбор учетных данных (особенно важно, если фигурируют административные учетные записи и еще важнее, если события происходят в нехарактерное время или месте);

– события 4768-4769 ((запрос билета TGT (Ticket Granting Ticket) от учётной записи в протоколе аутентификации Kerberos и запрос билета обслуживания в службе предоставления билетов (Ticket GrantingService (TGS)) для доступа к сервису)) являются маркерами для обнаружения атак Golden Ticket и Silver Ticket;

– событие 4648 (выполнена попытка входа с использованием явных учетных данных) помогают выявить горизонтальное перемещение. Злоумышленники часто используют явные учетные данные для доступа к другим узлам сети;

– событие 1102 (очистка логов) указывает на попытку скрыть следы атаки;

– событие 4688 (создание процесса) и 4104 (журнал PowerShell) выявляют использование скриптов и вредоносных утилит;

– события 4886-4887 (событие получения Certificate Services запроса на сертификат и подтверждение запроса и выдача сертификата) позволяют быстро определить недоверенные попытки получения сертификатов от центра сертификации.

Систематизация полученных результатов представлена в таблице 1 интеграции технических и организационных мер защиты AD. Таблица демонстрирует, что на каждом уровне защиты (сетевой периметр, сетевая инфраструктура, доменная архитектура, конечные точки, система мониторинга) техническая мера не может функционировать эффективно без соответствующей организа-

ционной меры. Например, МЭ и IDS/IPS на сетевом периметре требуют политики фильтрации входящего трафика, определяющей правила и процедуры их настройки и поддержки.

Сегментация сети требует матрицы доступа между сегментами, документирующей, какие подразделения и с какими протоколами и портами могут взаимодействовать. Отключение NTLM и внедрение Kerberos требует регламента смены паролей служебных учетных записей и политики миграции.

Таблица 1 – Интеграция технических и организационных мер защиты AD

Уровень защиты	Техническая мера	Организационная мера	Критичность
Сетевой периметр	Межсетевые экраны, IDS/IPS	Политика фильтрации входящего трафика	Высокая
	Почтовые шлюзы с песочницей	Обучение персонала противодействию фишингу	Высокая
Сетевая инфраструктура	Сегментация сети (VLAN)	Матрица доступа между сегментами	Критическая
	Изоляция контроллеров домена	Процедура управления административным доступом	Критическая
Доменная архитектура	Отключение NTLM, внедрение Kerberos	Регламент смены паролей служебных учетных записей	Критическая
	Политики сложности паролей, LAPS	Политика управления привилегированными учетными записями	Высокая
	Защита учетной записи krbtgt	Процедура ежегодной ротации пароля krbtgt	Критическая
Конечные точки	EDR, антивирусная защита	Политика управления рабочими станциями	Высокая
	Контроль запуска программ (белые списки)	Реестр утвержденного программного обеспечения	Средняя
Система мониторинга	SIEM для корреляции событий	Процедура реагирования на инциденты	Критическая
	Аудит событий Windows (4624, 4625, 4768)	Регламент мониторинга событий безопасности	Высокая

Анализ векторов атак согласно матрице MITRE ATT&CK и соответствующих интегрированных контрмер представлен в таблице 2. Таблица показывает, что для каждой тактики атакующего существует набор технических контрмер, которые должны поддерживаться организационными контрмерами. Например, для противодействия первоначальному доступу через фишинговые

письма (T1566) недостаточно внедрить почтовые шлюзы и песочницы – необходимо также обучение сотрудников и политика обработки писем. Для предотвращения бокового перемещения через RDP/SMB (T1021) недостаточно сегментации сети и изоляции контроллеров домена – требуется матрица доступа и процедуры аудита административных действий.

Таблица 2 – Векторы атак и интегрированные контрмеры (на основе MITRE ATT&CK)

Тактика MITRE ATT&CK	Описание вектора атаки	Технические контрмеры	Организационные контрмеры
Initial Access (T1566)	Фишинговые письма с вредоносными вложениями	Почтовые шлюзы, песочницы, блокировка вложений	Обучение сотрудников, политика обработки писем
Initial Access (Removable Media)	Заражение через USB-накопители	Политика белых списков USB-устройств	Регламент использования съемных носителей
Credential Access (T1003)	Дамп памяти LSASS для кражи учетных данных	Credential Guard, ограничение доступа к LSASS	Политика управления привилегированными учетными записями
Lateral Movement (T1021)	Использование RDP/SMB для бокового перемещения	Сегментация сети, изоляция DC, отключение SMB	Матрица доступа, процедуры аудита административных действий
Lateral Movement (NTLM Relay)	Перехват и ретрансляция NTLM-аутентификации	SMB Signing, отключение NTLM	Политика миграции на Kerberos
Credential Access (T1558)	Атаки на Kerberos (Kerberoasting)	Сильные пароли служебных учетных записей	Процедура аудита служебных учетных записей
Persistence (Golden Ticket)	Компрометация krbtgt для создания поддельных билетов	Регулярная смена пароля krbtgt	Регламент ежегодной ротации критических паролей
Defense Evasion (T1070)	Очистка журналов событий (Event ID 1102)	Централизованное хранение логов, мониторинг события 1102	Процедура расследования инцидентов
Privilege Escalation (T1068)	Эксплуатация уязвимостей в устаревших системах	Своевременное обновление ОС и ПО	Процесс управления уязвимостями, патч-менеджмент

События Windows для системы мониторинга инцидентов представлены в таблице 3. Из таблицы видно, что различные события имеют различный приоритет мониторинга в зависимости от того, насколько они индицируют компрометацию системы. Критический приоритет имеет событие 1102 (очистка жур-

нала событий безопасности), поскольку это прямой индикатор попытки сокрытия следов атаки. Высокий приоритет имеют события, связанные с аутентификацией Kerberos (4768, 4769), поскольку они могут индицировать атаки Golden Ticket и Silver Ticket. Средний приоритет имеют события создания процесса (4688) и успешного входа (4624), которые в изолированном виде могут быть легитимными, но в корреляции с другими событиями могут указывать на вредоносную активность.

Таблица 3 – События Windows для системы мониторинга инцидентов

Идентификатор события (Event ID)	Описание события	Индикатор компрометации	Приоритет мониторинга
4624	Успешный вход в систему	Вход в нехарактерное время/место	Средний
4625	Неудачная попытка входа	Множественные неудачные попытки (Brute Force)	Высокий
4768	Запрос билета TGT (Ticket Granting Ticket)	Аномальные параметры билета (Golden Ticket)	Высокий
4769	Запрос билета TGS (Ticket Granting Service)	Необычные запросы сервисов (Silver Ticket)	Высокий
4648	Вход с использованием явных учетных данных	Горизонтальное перемещение (Lateral Movement)	Высокий
1102	Очистка журнала событий безопасности	Попытка сокрытия следов атаки	Критический
4688	Создание нового процесса	Запуск подозрительных утилит (Mimikatz, PsExec)	Средний
4104	Выполнение скрипта PowerShell	Выполнение обфусцированных команд	Высокий
4886-4887	Запрос и выдача сертификата	Запросы сертификатов от неавторизованных субъектов	Высокий

Выводы

По итогам проведенной работы были сделаны следующие выводы.

Первое: защита доменной инфраструктуры AD не может быть эффективной при фрагментарном подходе, когда технические средства внедряются изолированно от организационных процессов их поддержки.

Второе: интеграция технических и организационных мер на пяти уровнях (сетевой периметр, сетевая инфраструктура, доменная архитектура, конечные точки, система мониторинга) создает эшелонированную систему защиты, где

компрометация одного уровня не приводит к полной компрометации инфраструктуры.

Третье: критичность мер защиты определяется не только их технической сложностью, но и их положением в цепочке противодействия атаке – меры, предотвращающие компрометацию критических компонентов (контроллеры домена, учетная запись krbtgt), имеют критический приоритет (рис. 16).

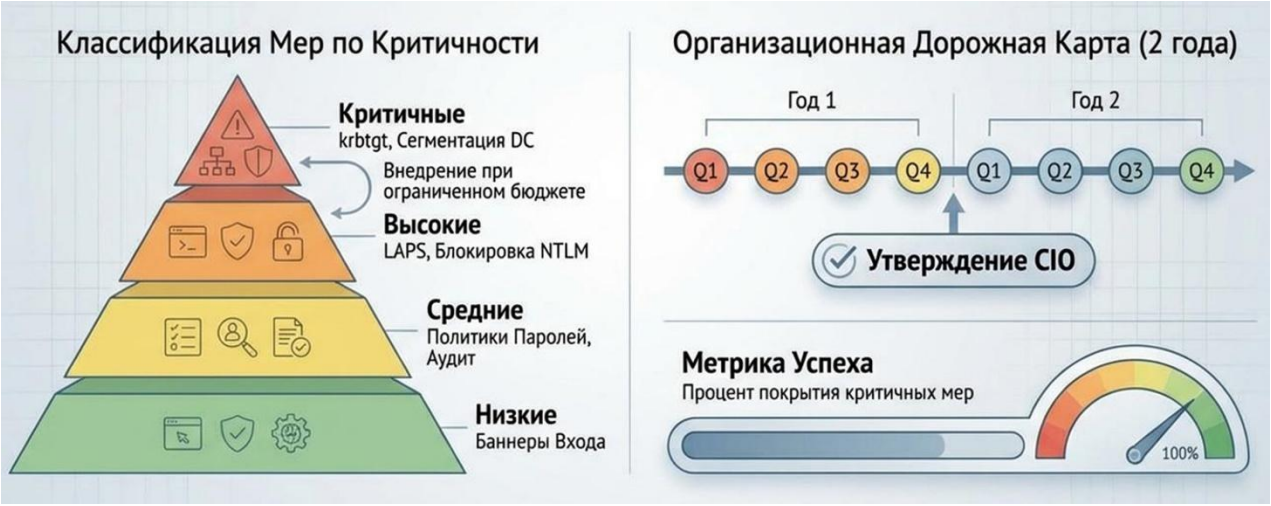

Рис. 16. Критичность мер защиты

Четвертое: система мониторинга на основе интеграции SIEM и EDR является не дополнительным уровнем, а интеграционным слоем, объединяющим все предыдущие уровни защиты и обеспечивающим корреляцию событий для выявления сложных многоэтапных атак.

Пятое: даже в условиях ограниченного бюджета возможно значительное повышение защищенности через использование открытых решений и приоритизацию внедрения мер критичного уровня.

На внедрение высококлассной архитектуры защиты уйдут годы, но если будет внедрено даже 50% из описанных мер, защита будет выстроена лучше, чем в 90% организаций. Необходимо создание междисциплинарных команд, включающих сетевых инженеров, инженеров по управлению уязвимостями, команду SOC, системных инженеров, инженеров по ИБ, CISO и администраторов домена, где каждый специалист понимает свою роль в защите и общую архитектуру системы.

Необходимо не ждать пока AD атакуют, а учиться нейтрализовывать и обнаруживать угрозы до того, как их последствия станут необратимыми. Атаки на AD происходят ежедневно, и тот факт, что организация в это время мигрирует на другое решение или внедряет новые средства защиты, не поможет оправдаться, если компрометация происходит прямо сейчас. Если AD используется в организации здесь и сейчас, не следует пренебрегать мероприятиями по защите, несмотря ни на что.

Литература

1. Использование Active Directory в инфраструктуре предприятия // Хабр [Электронный ресурс]. 23.04.2025. – URL: https://habr.com/ru/companies/first/articles/903572/ (дата обращения: 10.01.2026).

2. Active Directory Attacks // Cayosoft Blog [Электронный ресурс]. 08.12.2025. – URL: https://www.cayosoft.com/blog/active-directory-attacks (дата обращения: 10.01.2026).

3. Swapna S., Gokul Nath S., Yogesh S. G., Dillikumar P. S. Advanced Threat Detection with Active Directory and SIEM // International Journal for Research in Applied Science and Engineering Technology (IJRASET). 2025. Vol. 13. No. 4. doi: 10.22214/ijraset.2025.68478.

4. Khattab O. Conducting Empirical Research Study: How to Effectively and Securely Use the Vital Features of the Active Directory Network Server // Academia.edu [Электронный ресурс]. 2020. – URL: https://www.academia.edu/43009557/Conducting_Empirical_Research_Study_How_to_Effectively_and_Securely_Use_the_Vital_Features_of_the_Active_Directory_Network_Server (дата обращения: 10.01.2026).

5. Active Directory // Institute of Software Technology, TU Graz [Электронный ресурс]. 2024. – URL: https://www.isec.tugraz.at/wp-content/uploads/2024/09/04-active-directory-handout-2025.pdf (дата обращения: 10.01.2026).

6. Strengthening Active Directory Security: Detecting and Mitigating Kerberoasting Attacks // Computer. 2025. doi: 10.1109/MC.2024.3434535.

7. Simulation of Pre-Ransomware Attacks on Active Directory // 2024 17th International Conference on Security of Information and Networks (SIN). 2024. doi: 10.1109/SIN63213.2024.10871611.

8. Attacks on Active Directory – Resource-based Constrained Delegation and New Patches. 2025. doi: 10.1109/KI64036.2025.10916465.

9. Active Directory Kerberoasting Attack Monitoring and Detection Techniques // Proceedings of the 17th International Conference on Security and Cryptography. 2020. doi: 10.5220/0008955004320439.

10. Decoding the MITRE Engenuity ATT&CK Enterprise Evaluation: An Analysis of EDR Performance in Real-World Environments. 2024. doi: 10.1145/3589334.3645333.

11. Demo: Synthesizing Realistic Enterprise Active Directory Attack Graphs with ADSynth // ACM SIGSAC Conference on Computer and Communications Security Companion. 2024. doi: 10.1145/3672202.3673732.

12. McDonald A., Papadopoulos P., Buchanan W. Ransomware: Analysing the Impact on Windows Active Directory Domain Services // Sensors. 2022. Vol. 22. No. 3. Art. 953. doi: 10.3390/s22030953.

13. Elmiger M., Lemoudden M., Pitropakis N., Buchanan W. Start thinking in graphs: using graphs to address critical attack paths in a Microsoft cloud tenant // International Journal of Information Security. 2023. doi: 10.1007/s10207-023-00751-6.

14. Syynimaa N. Exploring Attack Paths Using Graph Theory: Case – Microsoft Entra ID Pass-Through Authentication // Proceedings of the 11th International Conference on Information Systems Security and Privacy. 2025. doi: 10.5220/0013119100003899.

15. Nebbione G., Calzarossa M. A Methodological Framework for AI-Assisted Security Assessments of Active Directory Environments // IEEE Access. 2023. Vol. 11. P. 15119–15130. doi: 10.1109/access.2023.3244490.

16. Sabri M., Ghebrehiwet I., Zaki N., Mohamad M. Explainable deep learning approach for advanced persistent threats (APTs) detection in cybersecurity // Artificial Intelligence Review. 2024. Vol. 57. No. 11. doi: 10.1007/s10462-024-10890-4.

17. Barros S. R. S. M. U. I., Oliveira C. F. B. S. Privileged Access Management: A Comprehensive Survey // IEEE Access. 2022. Vol. 10. P. 11233–11253. – URL: https://www.ijfmr.com/papers/2024/2/30122.pdf (дата обращения: 09.03.2026).

18. Bridging Gaps in Active Directory Security: Threat Landscape, Limitations, and Future-Proof Solutions // International Journal for Electronic Crime Investigation. 2025. Vol. 9. No. 1. doi: 10.54692/ijeci.2025.0901245.

19. Kowalski R., Limber S., McCord A. A developmental approach to cyberbullying: Prevalence and protective factors // Aggression and Violent Behavior. 2019. Vol. 45. P. 20–32.

20. Janeway T. The NIST Cybersecurity Framework – Third Parties Need Not Comply // ISACA Journal. 2020. Vol. 1. – URL: https://www.isaca.org/resources/isaca-journal/issues/2020/volume-1/the-nist-cybersecurity-framework-third-parties-need-not-compl (дата обращения: 09.03.2026).

21. Глухов А. П., Прозрителев Е. Е., Кацук Д. С. Управление информационной безопасностью // Вестник СибАДИ. 2021. № 4 (100). С. 17–23.

22. Rasmussen J. Risk management in a dynamic society: a modelling problem // Safety Science. 1997. Vol. 27. No. 2–3. P. 183–213. doi: 10.1016/S0925-7535(97)00052-0.

23. GPO и Active Directory: управляем доступом через GPOAdmin // Хабр [Электронный ресурс]. 22.03.2021. – URL: https://habr.com/ru/companies/galssoftware/articles/543588/ (дата обращения: 09.03.2026).

References

1. Ispolzovanie Active Directory v infrastrukture predpriiatiia [Using Active Directory in enterprise infrastructure]. *Habr*. 23 April 2025. Available at: https://habr.com/ru/companies/first/articles/903572/ (accessed 10 January 2026) (in Russian).

2. Active Directory Attacks. *Cayosoft Blog*. 8 December 2025. Available at: https://www.cayosoft.com/blog/active-directory-attacks (accessed 10 January 2026).

3. Swapna S., Gokul Nath S., Yogesh S. G., Dillikumar P. Advanced Threat Detection with Active Directory and SIEM. *International Journal for Research in Applied Science and Engineering Technology (IJRASET)*, 2025, vol. 13, no. 4. doi: 10.22214/ijraset.2025.68478.

4. Khattab O. Conducting Empirical Research Study: How to Effectively and Securely Use the Vital Features of the Active Directory Network Server. *Academia.edu*, 2020. Available at: https://www.academia.edu/43009557/Conducting_Empirical_Research_Study_How_to_Effectively_and_Securely_Use_the_Vital_Features_of_the_Active_Directory_Network_Server (accessed 10 January 2026).

5. Active Directory. *Institute of Software Technology, TU Graz*, 2024. Available at: https://www.isec.tugraz.at/wp-content/uploads/2024/09/04-active-directory-handout-2025.pdf (accessed 10 January 2026).

6. Strengthening Active Directory Security: Detecting and Mitigating Kerberoasting Attacks. *Computer*, 2025. DOI: 10.1109/MC.2024.3434535.

7. Simulation of Pre-Ransomware Attacks on Active Directory. 2024 *17th International Conference on Security of Information and Networks (SIN)*, 2024. DOI: 10.1109/SIN63213.2024.10871611.

8. Attacks on Active Directory – Resource-based Constrained Delegation and New Patches, 2025. DOI: 10.1109/KI64036.2025.10916465.

9. Active Directory Kerberoasting Attack Monitoring and Detection Techniques. *Proceedings of the 17th International Conference on Security and Cryptography*, 2020. DOI: 10.5220/0008955004320439.

10. Decoding the MITRE Engenuity ATT&CK Enterprise Evaluation: An Analysis of EDR Performance in Real-World Environments, 2024. DOI: 10.1145/3589334.3645333.

11. Demo: Synthesizing Realistic Enterprise Active Directory Attack Graphs with ADSynth. *ACM SIGSAC Conference on Computer and Communications Security Companion*, 2024. DOI: 10.1145/3672202.3673732.

12. McDonald A., Papadopoulos P., Buchanan W. Ransomware: Analysing the Impact on Windows Active Directory Domain Services. *Sensors*, 2022, vol. 22, no. 3, art. 953. DOI: 10.3390/s22030953.

13. Elmiger M., Lemoudden M., Pitropakis N., Buchanan W. Start thinking in graphs: using graphs to address critical attack paths in a Microsoft cloud tenant. *International Journal of Information Security*, 2023. DOI: 10.1007/s10207-023-00751-6.

14. Syynimaa N. Exploring Attack Paths Using Graph Theory: Case – Microsoft Entra ID Pass-Through Authentication. *Proceedings of the 11th International Conference on Information Systems Security and Privacy*, 2025. DOI: 10.5220/0013119100003899.

15. Nebbione G., Calzarossa M. A Methodological Framework for AI-Assisted Security Assessments of Active Directory Environments. *IEEE Access*, 2023, vol. 11, pp. 15119–15130. DOI: 10.1109/access.2023.3244490.

16. Sabri M., Ghebrehiwet I., Zaki N., Mohamad M. Explainable deep learning approach for advanced persistent threats (APTs) detection in cybersecurity. *Artificial Intelligence Review*, 2024, vol. 57, no. 11. DOI: 10.1007/s10462-024-10890-4.

17. Barros S. R. S. M. U. I., Oliveira C. F. B. S. Privileged Access Management: A Comprehensive Survey. *IEEE Access*, 2022, vol. 10, pp. 11233–11253. Available at: https://www.ijfmr.com/papers/2024/2/30122.pdf (accessed 09 March 2026).

18. Bridging Gaps in Active Directory Security: Threat Landscape, Limitations, and Future-Proof Solutions. *International Journal for Electronic Crime Investigation*, 2025, vol. 9, no. 1. DOI: 10.54692/ijeci.2025.0901245.

19. Kowalski R., Limber S., McCord A. A developmental approach to cyberbullying: Prevalence and protective factors. *Aggression and Violent Behavior*, 2019, vol. 45, pp. 20–32.

20. Janeway T. The NIST Cybersecurity Framework – Third Parties Need Not Comply. *ISACA Journal*, 2020, vol. 1. Available at: https://www.isaca.org/resources/isaca-journal/issues/2020/volume-1/the-nist-cybersecurity-framework-third-parties-need-not-compl (accessed 09 March 2026).

21. Glukhov A. P., Prozritelev E. E., Katsuk D. S. Upravlenie informatsionnoi bezopasnost'iu [Information security management]. *Vestnik SibADI*, 2021, no. 4 (100), pp. 17–23 (in Russian).

22. Rasmussen J. Risk management in a dynamic society: a modelling problem. *Safety Science*, 1997, vol. 27, no. 2–3, pp. 183–213. DOI: 10.1016/S0925-7535(97)00052-0.

23. GPO i Active Directory: upravliaem dostupom cherez GPOAdmin [GPO and Active Directory: managing access via GPOAdmin]. *Habr*, 22 March 2021. Available at: https://habr.com/ru/companies/galssoftware/articles/543588/ (accessed 09 March 2026) (in Russian).

Статья поступила 27 февраля 2026 г.

Информация об авторах

Митрофанов Михаил Валерьевич – доктор технических наук, доцент. Доцент Военного учебного центра. Национальный исследовательский университет ИТМО. Область научных интересов: защита сетей передачи от компьютерных атак; обеспечение устойчивости сетей связи. E-mail: vonafortim@yandex.ru

Адрес: 197101, Россия, г. Санкт-Петербург, Кронверкский проспект, д. 49.

Лаута Олег Сергеевич – доктор технических наук, доцент. Профессор кафедры «Комплексного обеспечения информационной безопасности». Государственный университет морского и речного флота имени адмирала С.О. Макарова. Область научных интересов: защита сетей передачи от компьютерных атак; обеспечение устойчивости сетей связи. E-mail: laos-82@yandex.ru

Адрес: 198035, Россия, г. Санкт-Петербург, Двинская улица, д. 5/7.

Крамской Николай Николаевич – соискатель ученой степени кандидата технических наук. Начальник направления. ООО «Специальный Технологический Центр». Область научных интересов: защита информации; защита каналов управления. E-mail: kram.com@mail.ru

Адрес: 195220, Россия, г. Санкт-Петербург, проспект Непокорённых, д. 17.

Куракин Александр Сергеевич – кандидат технических наук. Заместитель директора по разработке специальных средств – генеральный конструктор систем и комплексов криптографической защиты информации. ООО «Специальный Технологический Центр». Область научных интересов: защита информации; защита каналов управления. E-mail: nirt@mail.ru

Integration of technical and organizational measures to protect the Active Directory domain: from network segmentation to incident monitoring system

M. I. Mitrofanov, O. S. Lauta, N. N. Kramskoy, A. S. Kurakin

Purpose. *In conditions of high dependence of corporate infrastructures on the domain architecture of Active Directory, domain protection is considered as a key element of ensuring the stability of the entire information system of the organization. However, operational practice demonstrates that even with a variety of technical means of protection, AD compromise remains possible due to the lack of system integration of technical and organizational measures. There is a fragmented implementation of security solutions, inconsistency in administration and monitoring procedures, as well as a gap between the security architecture and its maintenance processes. The purpose of the work is to develop an integrated Active Directory domain protection model that combines technical and organizational measures at all levels of the infrastructure — from network segmentation to an incident monitoring system — with formalization of criteria for their criticality and interrelationships.* ***Methods.*** *The methodology is based on a system analysis of domain infrastructure, decomposition of protection levels, analysis of the MITRE ATT&CK matrix, the method of expert assessments of the criticality of measures, as well as analysis of Windows event logs to build a monitoring model and incident correlation.* ***Novelty.*** *A five–level integrated Active Directory protection model is proposed, considering a monitoring system (SIEM-EDR) as an integration layer that combines technical and organizational countermeasures into a single layered architecture. A classification of measures according to the level of criticality has been introduced, depending on their position in the attack chain.* ***Results.*** *A structured model for the integration of technical and organizational AD protection measures has been developed, tables of matching attack vectors and countermeasures have been formed, priorities for monitoring Windows events and criteria for the criticality of protective measures have been determined.* ***Practical relevance.*** *The proposed model makes it possible to build a domain infrastructure protection architecture taking into account the limitations of real organizations, justify the priority of implementing measures, increase the effectiveness of incident response processes and rationally allocate the information security budget.*

Key words: *Active Directory, domain infrastructure, information security, network segmentation, SIEM, EDR, in-depth protection, incident monitoring, MITRE ATT&CK, privileged access management.*

Information about Authors

Mikhail Valerievich Mitrofanov – Dr of Engineering Sciences, Associate Professor. Associate Professor at the Military Training Center. National Research ITMO University. Field of research: protecting transmission networks from cyber attacks; ensuring the resilience of communication networks. E-mail: vonafortim@yandex.ru

Address: 197101, Russia, Saint-Petersburg, Kronverksky prospekt, 49

Oleg Sergeevich Lauta – Dr. of Engineering Sciences, Associate Professor. Professor at the Department of Integrated Information Security. Admiral Makarov State University of Maritime and Inland Shipping. Field of research: protecting transmission networks from cyber attacks; ensuring the resilience of communication networks. E-mail: laos-82@yandex.ru

Address: 198035, Russia, Saint-Petersburg, Dvinskaya street, 5/7.

Nikolai Nikolaevich Kramskoy – Doctoral Student. Head of Department. Limited Liability Company «Special Technology Center». Research interests: information security; control channel protection. E-mail: kram.com@mail.ru

Address: 195220, Russia, Saint-Petersburg, Nepokorennykh prospekt, 17

Aleksandr Sergeevich Kurakin – Ph.D. of Engineering Sciences. Deputy Director at the Development of Specialized Tools – General Designer of Cryptographic Information Protection Systems and Complexes. Limited Liability Company «Special Technology Center». Research interests: information security; control channel protection. E-mail: nirt@mail.ru