jild. 3 No 2 (2026)

MANAGEMENT AND ECONOMICS SCIENTIFIC RESEARCH JOURNAL

MENEJMENT VA IQTISODIYOT ILMIY-TADQIQOT JURNALI

НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ЖУРНАЛ МЕНЕДЖМЕНТА И ЭКОНОМИКИ

journals@timeedu.uz

+998 95 651 90 00

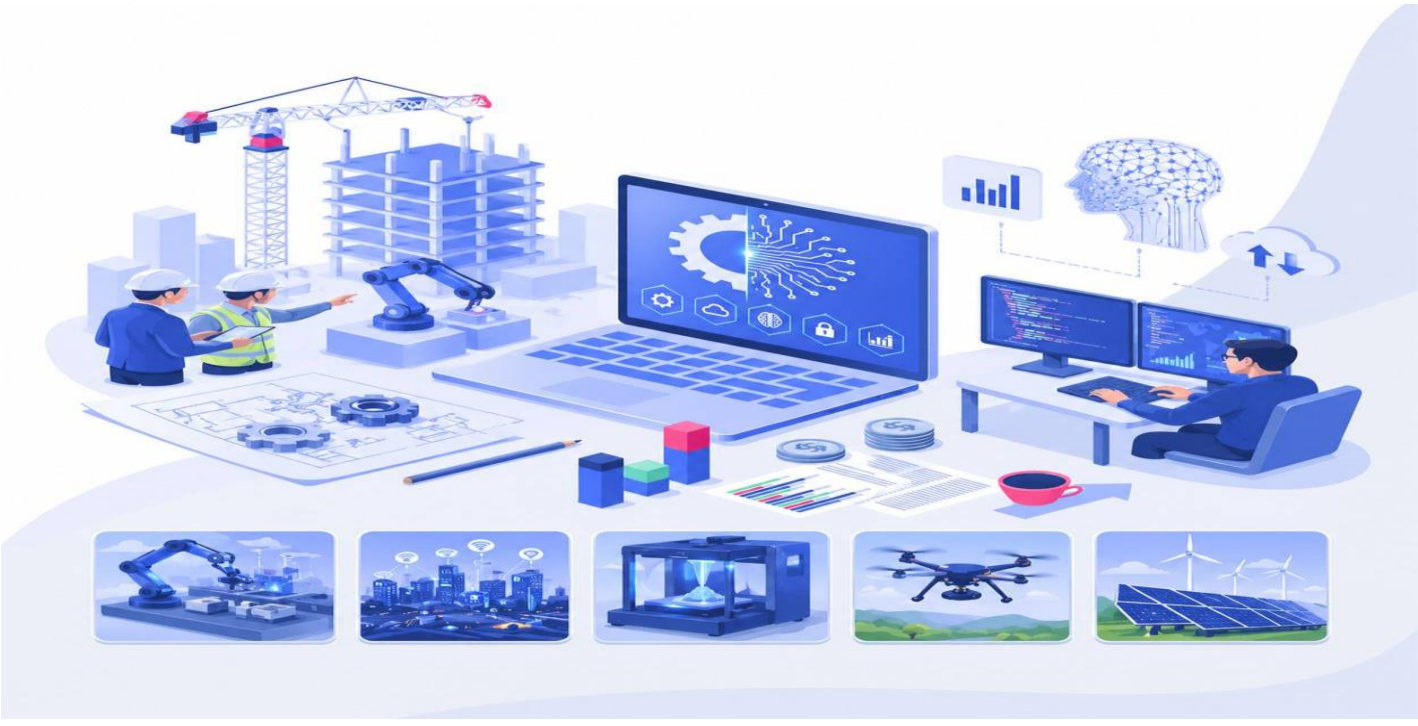
O‘ZBEKISTON RESPUBLIKASI

OLIY TA’LIM, FAN VA INNOVATSIYALAR VAZIRLIGI

TOSHKENT MENEJMENT VA IQTISODIYOT INSTITUTI

“MUHANDISLIKDA SUN’IY INTELLEKT VA RAQAMLI INNOVATSION TEXNOLOGIYALAR: ZAMONAVIY YECHIMLAR VA ISTIQBOLLAR” MAVZUSIDAGI

XALQARO ILMIY-AMALIY ANJUMAN MATERIALLARI



FARG‘ONA-2026

O'ZBEKISTON RESPUBLIKASI OLIY TA‘LIM, FAN VA INNOVATSIYALAR VAZIRLIGI

TOSHKENT MENEJMENT VA IQTISODIYOT INSTITUTI

“MUHANDISLIKDA SUN’IY INTELLEKT VA RAQAMLI INNOVATSION TEXNOLOGIYALAR: ZAMONAVIY YECHIMLAR VA ISTIQBOLLAR” MAVZUSIDAGI

XALQARO ILMIY-AMALIY ANJUMAN MATERIALLARI

21 MAY 2026 YIL

МИНИСТЕРСТВО ВЫСШЕГО ОБРАЗОВАНИЯ, НАУКИ И ИННОВАЦИЙ РЕСПУБЛИКИ УЗБЕКИСТАН

ТАШКЕНТСКИЙ ИНСТИТУТ УПРАВЛЕНИЯ И ЭКОНОМИКИ

МЕЖДУНАРОДНАЯ НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ НА ТЕМУ «ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ЦИФРОВЫЕ ИННОВАЦИОННЫЕ ТЕХНОЛОГИИ В ИНЖЕНЕРИИ: СОВРЕМЕННЫЕ РЕШЕНИЯ И ПЕРСПЕКТИВЫ»

21 МАЯ 2026 ГОДА

MINISTRY OF HIGHER EDUCATION, SCIENCE AND INNOVATIONS OF THE REPUBLIC OF UZBEKISTAN

TASHKENT INSTITUTE OF MANAGEMENT AND ECONOMICS

INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE ON THE THEME "ARTIFICIAL INTELLIGENCE AND DIGITAL INNOVATIVE TECHNOLOGIES IN ENGINEERING: MODERN SOLUTIONS AND PROSPECTS" 21 MAY 2026

“Muhandislikda sun’iy intellekt va raqamli innovatsion texnologiyalar: zamonaviy yechimlar va istiqbollar” Xalqaro ilmiy-amaliy anjuman tezislar to‘plami. 2026-yil 21-may.

Ushbu to‘plamda — “Muhandislikda sun’iy intellekt va raqamli innovatsion texnologiyalar: zamonaviy yechimlar va istiqbollar” Xalqaro ilmiy –amaliy anjuman ishtirokchilarining tezislari keltirilgan. Anjuman kun tartibiga kiritilgan masalalar dolzarb bo‘lib, u yalpi ma‘ruzalar va amaliy zamonaviy muhandislik ta’limida raqamli transformatsiya va sun’iy intellekt, muhandislik yechimlari va sanoat 4.0, robototexnika va avtomatlashtirilgan boshqaruv tizimlari, kiberxavfsizlik va ma'lumotlarni himoya qilish, ta’limda axborot va innovatsion texnologiyalarning qo‘llanilishi, biznes jarayonlar va raqamli iqtisodiyotga axborot texnologiyalarining o‘rni kabi sho‘balardan tashkil topgan. To‘plam sohasi mutaxassislari, ilmiy tadqiqotchilar, professor-o‘qituvchilar, doktorantlar, magistrlar va talabalar uchun mo‘ljallangan.

Maqolalarda keltirilgan ma‘lumotlarning haqqoniyligi uchun mualliflar mas‘uldir.

MANAGEMENT AND ECONOMICS
SCIENTIFIC RESEARCH JOURNAL

+998 95 651 90 00
journals@timeedu.uz
Shota Rustaveli ko'chasi, 114
tmijournals.ndc-agency.uz
TMII_ilmiy_bolim

Tahririyat jamoasi

АНАЛИЗ АРХИТЕКТУРНОГО СЛОЯ ИСТОЧНИКОВ ДАННЫХ DLP-СИСТЕМ ДЛЯ ГИБРИДНЫХ КОРПОРАТИВНЫХ СРЕД

Очилов Н
начальник Управления по внедрению технологий цифровизации и искусственного интеллекта Министерства высшего образования, науки и инноваций Республики Узбекистан
Набиев С
начальник Управления развития информационных технологий АК «Узбектелеком», г. Ташкент, Узбекистан

Annotatsiya. Maqola ma’lumotlar sizib chiqishining oldini olish tizimlari (DLP) arxitekturasidagi ma’lumotlar manbalari qatlamiga bag‘ishlangan. Mualliflar data-at-rest, data-in-motion va data-in-use holatlari bo‘yicha klassik taksonomiyani ko‘rib chiqadilar va ushbu modelning zamonaviy infratuzilmada - konteynerlashtirishda, SaaS xizmatlariga o‘tishda, BYOD va soyadagi IT amaliyotlarining tarqalishida - qaerda ishlamay qolishini ko‘rsatadilar. Shu asosda O‘zbekiston Respublikasida DLP konturini loyihalashtirish uchun "Shaxsiy ma'lumotlar to‘g‘risida"gi O'RQ-547-sonli Qonun [3] talablarini hisobga olgan holda amaliy xulosalar shakllantirilgan.

Калит сўзлар: DLP, маълумот манбалари, архитектура, маълумот ҳолатлари, BYOD, инвентаризация.

Аннотация. Статья посвящена слою источников данных в архитектуре систем предотвращения утечек (DLP). Авторы рассматривают классическую таксономию по состояниям data-at-rest, data-in-motion и data-in-use и показывают, где эта модель перестаёт работать в современной инфраструктуре - при контейнеризации, переходе в SaaS, распространении BYOD и теневых ИТ. На этой основе сформулированы практические выводы для проектирования DLP-контура в Республике Узбекистан с учётом требований Закона ЗРУ-547 «О персональных данных».

Ключевые слова: DLP, источники данных, архитектура, состояния данных, BYOD, инвентаризация.

Abstract. This article addresses the data source layer in the architecture of Data Loss Prevention (DLP) systems. The authors examine the classical taxonomy based on the data-at-rest, data-in-motion, and data-in-use states and demonstrate where this model breaks down in modern infrastructure — under containerization, the shift to SaaS, and the proliferation of BYOD and shadow IT. On this basis, practical conclusions are formulated for designing a DLP perimeter

in the Republic of Uzbekistan, taking into account the requirements of the Law of the Republic of Uzbekistan No. 547 "On Personal Data" [3].

Keywords: DLP, data sources, architecture, data states, shadow IT, BYOD, inventory.

Введение

Любая система предотвращения утечек данных (Data Loss Prevention, DLP) начинается с того, что именно она видит. Это поле зрения задаётся слоем источников - тем уровнем архитектуры, на котором снимается первичная телеметрия и появляется само понятие «контролируемой сущности». В нашей предыдущей работе мы давали общий обзор современного состояния DLP-систем и трёх поколений их архитектур [1]. Настоящая статья продолжает это исследование, но ограничена одним архитектурным слоем: полнота и корректность именно этого слоя, как нам представляется, и определяют верхнюю границу качества всей системы.

Классическая модель источников была сформулирована около пятнадцати лет назад на разделении данных по трём состояниям [2] и рассчитывалась на гомогенную корпоративную среду с чётким периметром и доменной аутентификацией. Сегодняшняя инфраструктура устроена иначе. Она гетерогенна, частично размещена у внешних провайдеров, насыщена peer-to-peer и групповыми взаимодействиями, и понятие «источник» в ней то и дело теряет однозначность. Пока этот слой не пересмотрен, любые усилия над верхними компонентами - детекторами, политиками, реагированием - упираются в слепые зоны на входе.

В статье мы разбираем слой источников DLP по существу: формулируем рабочее определение источника, систематизируем классы источников с их инженерной точкой съёма телеметрии, показываем, где классическая таксономия даёт сбой, и предлагаем рекомендации по проектированию этого слоя в условиях Республики Узбекистан с учётом требований Закона ЗРУ-547 «О персональных данных» [3].

Методика обзора

Работа представляет собой структурированный аналитический обзор, ограниченный архитектурным уровнем источников. Вопросы детектирования содержимого, политик и реагирования за её рамками. В выборку вошли публикации Springer, IEEE и Cluster Computing, отчёты Gartner и Forrester, материалы российских изданий, нормативные документы Республики Узбекистан и справочные материалы вендоров. Период публикаций - 2010–2024 годы; такой диапазон позволяет проследить эволюцию представлений об источниках от ранней

«трёхсостоянийной» модели [2] до современных гибридных конструкций [4, 5].

Метод работы складывается из трёх шагов. Сначала мы вводим рабочее определение источника, привязанное к месту и способу съёма телеметрии. Затем упорядочиваем классы источников по технологическому признаку и сопоставляем их с состояниями данных. И наконец, опираясь на пограничные случаи, в которых классическая модель сбоит, формулируем требования к современному слою источников.

Источник данных как архитектурная единица DLP-системы

Термин «источник данных» в литературе по DLP используется в двух смыслах. В широком им называют любую точку возникновения чувствительной информации - включая бизнес-процессы и людей. В узком, инженерном - а именно его мы здесь и используем - источник это техническая точка съёма телеметрии: процесс, файловая система, сетевой стек, драйвер устройства, агент СУБД, API облачного сервиса. Удобное для проектирования определение звучит так: источник данных в DLP - это устойчиво идентифицируемая программная или аппаратная сущность, относительно которой система может (а) перехватить или зафиксировать обращение к данным, (б) сопоставить это обращение с идентичностью субъекта и (в) построить контекст события, достаточный для решения политикой [4].

Из такого определения вытекают три требования к источнику: его наблюдаемость, идентифицируемость субъекта и контекстная достаточность. Если по источнику нельзя достоверно установить, кто именно к данным обратился, в смысле DLP он неполноценен. Если телеметрия с него лишена контекста - приложения, пользователя, пути, направления - она вырождается в шум. Если источник наблюдается с задержкой, превышающей время самой утечки, его ценность близка к нулю. Эти три требования и образуют тот фильтр, через который должна проходить любая попытка ввести в DLP-контур новый класс источников.

Классическая таксономия, восходящая к работам начала 2010-х [2], упорядочивает источники по состояниям данных. К data-at-rest относят данные на устройствах хранения и в базах: файловые серверы, NAS, SAN, СУБД, архивы. К data-in-motion - данные, передаваемые по сетевым каналам: SMTP, HTTP/HTTPS, FTP, мессенджеры, сетевые расшаривания. К data-in-use - данные, обрабатываемые на конечных точках: операции с буфером обмена, печать, копирование на съёмные носители, скриншоты, ввод в приложениях. Эта триада до сих пор задаёт структуру продуктовых линеек большинства вендоров [5]. Но её исходное допущение - что в

данный момент сущность находится строго в одном состоянии - современная инфраструктура нарушает регулярно.

Классическая таксономия источников DLP по состояниям данных

Таблица 1

Состояние	Типичные источники	Способ съёма	Архитектурное предположение
Data-at-rest	Файловые серверы, СУБД, архивы, NAS/SAN	Сканер по расписанию, агент на хосте, коннектор СУБД	Объект однозначно локализован
Data-in-motion	SMTP, HTTP/HTTPS, FTP, мессенджеры	Сетевой сенсор, SSL-инспекция, ICAP	Поток имеет различимое направление
Data-in-use	Буфер обмена, печать, USB, ввод в приложении	Endpoint-агент, перехват API ОС	Действие совершает идентифицируемый пользователь

Источник: составлено авторами на основе [2, 4, 5].

Допущения, перечисленные в правом столбце таблицы 1, удобны для классификации, но в реальной эксплуатации каждое из них даёт сбои. Документ в облачном хранилище одновременно лежит на дисках провайдера (at-rest), синхронизируется на устройства (in-motion) и редактируется в браузере (in-use). Поток в групповом мессенджере не имеет однозначного направления «изнутри наружу». Действие в SaaS-приложении совершается уже не пользователем напрямую, а делегированным OAuth-токеном, привязка которого к человеку - отдельная задача. Эти расхождения не отменяют ценности таксономии как языка описания, но требуют рассматривать её скорее как набор проекций одной и той же сущности, чем как жёсткую разметку.

Технологическая декомпозиция классов источников DLP

Разбор удобнее вести не по состояниям, а по технологическим классам. Именно на этом уровне принимаются конкретные инженерные решения о способе съёма телеметрии. Сначала рассмотрим классы, исторически образующие ядро DLP, затем те, что оформились за последнее десятилетие.

Процессы и файловые объекты на конечных точках исторически были первыми источниками. Endpoint-агент перехватывает системные вызовы открытия файлов, операции с буфером обмена, копирование на съёмные носители, отправку на печать и обращения к сетевым ресурсам. Сильная сторона класса в близости к реальному действию пользователя, слабая в стоимости поддержки агентов на гетерогенном парке и в

зависимости от ABI операционной системы. К корпоративной файловой структуре добавляются сетевые шары, NAS и распределённые файловые системы, и здесь обычно используют связку сканера с агентами на серверах [4].

Сетевые соединения остаются центральным классом для каналов SMTP, HTTP/HTTPS, FTP и проприетарных протоколов корпоративных сервисов. Сетевой сенсор работает в трёх режимах: пассивное зеркалирование, инлайн через ICAP или прокси, TLS-инспекция на корпоративном шлюзе. Главная архитектурная боль сегодня в массовом распространении TLS 1.3 и протоколов поверх QUIC. Пассивное наблюдение перестаёт давать содержательный сигнал, а инлайн-инспекция упирается в pinning сертификатов на клиентах [4, 5]. Центр тяжести смещается с сетевого пакета на инспекцию уровня приложения и API.

Съёмные носители, печать и буфер обмена образуют классическую группу локальных каналов утечки. Для них endpoint-агент остаётся единственным реалистичным источником. Архитектурно важна здесь не техника перехвата, а связывание события с пользователем сеанса и содержимым документа. Без этой связки запись об обращении к USB-устройству бесполезна для политики. Базы данных стоят особняком. Телеметрию с них снимают на уровне сетевого протокола СУБД, через нативный аудит или через агента на сервере БД, и каждый вариант по-своему балансирует полноту контекста и нагрузку на систему [6].

Картину дополняют классы, оформившиеся за последнее десятилетие. Виртуальные машины и контейнеры заставляют переносить точку наблюдения на гипервизор и контейнерный runtime, в Kubernetes удобнее всего ставить sidecar или eBPF-датчик уровня узла. SaaS-сервисы (почта, офисные пакеты, CRM, репозитории кода) наблюдаются через провайдерские API и журналы аудита, и источник превращается из трафика в событийную ленту. BYOD-устройства порождают трафик и события, но контролируются ограниченно из-за юридического статуса. Теневые ИТ, то есть несанкционированные SaaS и личные облака, формируют класс источников, неизвестных DLP по построению. Обнаруживаются они только косвенно, через анализ DNS- и прокси-логов [7, 8].

Прослеживается общая закономерность. Чем дальше источник от управляемого периметра, тем ниже полнота контекста, доступного DLP-системе. Endpoint-агент и агент на сервере БД дают высокую полноту, сетевой сенсор и средства контейнерного runtime среднюю, SaaS зависят от

провайдера, BYOD контролируется ограниченно, а теневые ИТ остаются неизвестны по построению и фиксируются лишь косвенно [4, 6, 7, 8].

Пределы применимости классической модели в гибридной инфраструктуре

Если разбирать слой источников вглубь, ограничения классической модели сводятся к трём узлам напряжения: архитектурная асимметрия источника и приёмника, мультисостоятельность одной и той же сущности, неоднозначность субъекта обработки. Каждый из них стоит рассмотреть отдельно - именно они задают границы применимости таксономии и формируют требования к её преемнице.

Асимметрия «источник - приёмник» предполагает, что у каждого контролируемого события есть различимая внутренняя сторона (источник) и различимая внешняя (приёмник). На этой асимметрии и держатся ключевые политики: «не отправлять файл наружу», «не загружать в чужой облачный сервис», «не пересылать на личный адрес». В корпоративной почте 2000-х такое разделение было естественным; в современных средах оно ломается. В групповых мессенджерах и коллаборативных платформах участники одной комнаты одновременно и источники, и приёмники, а отправка сообщения вовсе не является «выходом» в традиционном смысле. В peer-to-peer обмене внутри корпоративных сред граница «внутрь - наружу» определяется уже не сетью, а схемой прав доступа. В межорганизационном B2B-обмене контрагент одновременно и внешний, и доверенный участник процесса; обращаешься с ним как с «внешним приёмником» - получаешь ложные срабатывания, как с «внутренним» - рискуешь утечкой [9].

Второе фундаментальное ограничение - мультисостоятельность. Классическая модель предполагала, что объект в данный момент находится строго в одном из трёх состояний; современный документ в облачном хранилище ломает это допущение по построению. На дисках провайдера он лежит как data-at-rest, каждые несколько секунд синхронизируется с устройствами как data-in-motion и одновременно редактируется в браузере как data-in-use. Снимая телеметрию по одному состоянию, мы не покрываем действий, идущих в других состояниях с той же сущностью; политика, привязанная к состоянию, оказывается локальной, тогда как утечка по природе глобальна. На практике это толкает к переходу от событий, привязанных к каналам, к событиям, привязанным к идентификатору самой сущности (object-centric DLP), где канал становится атрибутом события, а не его первичным ключом [10].

Третье ограничение - неоднозначность субъекта обработки. Классическая модель неявно подразумевала, что за каждым событием стоит конкретный пользователь домена. В современной инфраструктуре субъектами выступают сервисные аккаунты, технологические идентичности, делегированные OAuth-токены, межсистемные интеграции, а также автономные программные агенты. Одно и то же действие - скажем, выгрузка большого набора данных из CRM - может быть инициировано пользователем напрямую, скриптом от его имени, сервисным аккаунтом или внешним B2B-партнёром по делегированным правам. Без явного слоя идентичности, привязывающего телеметрию источника к ответственному субъекту, события превращаются в технические записи, по которым уже невозможно ни применить политику, ни провести расследование [4].

Сюда же примыкает проблема инвентаризации: значительная доля источников в реальной инфраструктуре формально неизвестна владельцу. Под shadow data принято понимать копии чувствительных данных, образовавшиеся вне процесса учёта; под dark data - данные, существующие в системах хранения, но не охваченные ни одной политикой; под теневыми ИТ - целые сервисы, используемые без согласования. Любой из этих классов вне поля зрения слоя источников - для DLP-системы это эквивалент невидимости [7, 8]. Из чего и следует, что современная архитектура слоя источников должна включать не только наблюдение известного, но и активный механизм обнаружения нового.

Результаты обзора

Обзор дал три группы результатов.

Во-первых, классы источников систематизированы по способу съёма телеметрии, а не по состояниям данных. Полнота контекста монотонно убывает по мере удаления источника от управляемого периметра: от endpoint-агентов и агентов СУБД к сетевым сенсорам, контейнерному runtime, SaaS-API, BYOD и теневым ИТ.

Во-вторых, выявлены три узла напряжения, в которых классическая трёхсостоянийная модель систематически сбоит: асимметрия «источник - приёмник» (групповые мессенджеры, B2B), мультисостоятельность сущности (документы в облачных хранилищах) и неоднозначность субъекта обработки (сервисные аккаунты, OAuth-токены, автономные агенты).

В-третьих, зафиксирован класс источников, не охватываемых классической таксономией по построению: shadow data, dark data и

теневые ИТ. Их обнаружение является самостоятельной функцией слоя источников, а не побочным эффектом наблюдения за известным.

Обсуждение

Сказанное применимо к условиям Республики Узбекистан. ЗРУ-547 требует локализации обработки и контролируемого трансграничного обмена, а это упирается в слой источников. Оператор обязан знать, где данные лежат, куда уходят и кому делегированы права. Без инвентаризации и привязки телеметрии к субъекту соответствие закону остаётся бумажным.

Мы выносим три положения. Первое касается рабочего определения источника. Это устойчиво идентифицируемая сущность с наблюдаемостью, идентифицируемостью и контекстной достаточностью. Определение работает как фильтр при проектировании: кандидат без идентификации и контекста отсеивается заранее, иначе контур получит ещё один источник шума.

Второе положение о переходе от событий «по каналу» к событиям «по сущности», где канал становится атрибутом, а не первичным ключом. Толкает к этому мультисостоятельность. Документ в облачном хранилище живёт сразу в нескольких состояниях, и при канальной привязке действия через разные каналы между собой не связываются. Объектно-ориентированная модель снимает разобщённость, но требует переписать модель данных и состыковать её с классификацией.

Третье положение о слое идентичности между источниками и политиками. Раньше субъектом считался пользователь домена. Сегодня за событием стоит сервисный аккаунт, OAuth-токен, межсистемная интеграция или автономный агент. Без этого слоя политики применяются к техническим записям, а не к субъектам, и DLP теряет смысл и в превенции, и в расследовании.

В отраслях с высокой долей госприсутствия (телекомы, банки, здравоохранение, госинформсистемы) слой источников расширяется по трём направлениям. Это SaaS через провайдерские API, теневые ИТ через корреляцию DNS- и прокси-логов, идентичность для сервисных аккаунтов, токенов и B2B-интеграций. Приоритеты разные. Банкам в первую очередь нужна идентичность из-за плотности B2B. Здравоохранению SaaS из-за ухода в облако. Телекомам теневые ИТ из-за масштаба базы.

Отсюда перечень шагов под ЗРУ-547. Инвентаризация источников по декомпозиции из раздела 2. Расширение контура за счёт SaaS-API и теневых ИТ. Связывание телеметрии с субъектом. Пересмотр политик в логике объектно-ориентированной привязки. Фиксация матрицы

покрытия источников и состояний отдельным артефактом, а не пунктом в приложениях. Этим и сокращается разрыв между декларативным и фактическим соответствием.

Заключение

Классическая таксономия источников DLP по состояниям data-at-rest, data-in-motion и data-in-use сохраняет ценность как язык описания, но как разметка для проектирования уже недостаточна: одна сущность одновременно живёт в нескольких состояниях, асимметрия источника и приёмника ломается в коллаборативных и B2B-средах, субъект обработки распадается на множество идентичностей. Эти ограничения требуют надстройки в виде слоёв инвентаризации, идентичности и объектно-ориентированной привязки событий. Предложенное операциональное определение источника, переход к объектно-ориентированной модели событий и выделение слоя идентичности образуют минимально необходимый набор архитектурных решений для приведения слоя источников DLP-систем в соответствие с современной гибридной инфраструктурой и требованиями законодательства Республики Узбекистан о персональных данных.

Список использованной литературы

1. Очилов Н.Н., Набиев С.Б. Современное состояние DLP-систем и три поколения архитектур // Management and Economics Scientific Research Journal. - 2026.
2. Shabtai A., Elovici Y., Rokach L. A Survey of Data Leakage Detection and Prevention Solutions. - Springer, 2012. - DOI: 10.1007/978-1-4614-2053-8.
3. Закон Республики Узбекистан «О персональных данных» от 02.07.2019 г. № ЗРУ-547. - URL: https://lex.uz/docs/4396428.
4. Alneyadi S., Sithirasenan E., Muthukkumarasamy V. A survey on data leakage prevention systems // Journal of Network and Computer Applications. - 2016. - Vol. 62. - P. 137–152. - DOI: 10.1016/j.jnca.2016.01.008.
5. Gartner. Market Guide for Data Loss Prevention. - Gartner Research, 2023. - URL: https://www.gartner.com/en/documents/data-loss-prevention.
6. Kul G., Upadhyaya S. Towards a Cyber Ontology for Insider Threats in the Financial Sector // J. Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications. - 2015. - Vol. 6, № 4. - P. 64–85.
7. Forrester. The State of Data Security, 2024. - Forrester Research, 2024. - URL: https://www.forrester.com/report/the-state-of-data-security-2024.
8. Silic M., Back A. Shadow IT - A view from behind the curtain // Computers & Security. - 2014. - Vol. 45. - P. 274–283. - DOI: 10.1016/j.cose.2014.06.007.

9. Cheng L., Liu F., Yao D. Enterprise data breach: causes, challenges, prevention, and future directions // WIREs Data Mining and Knowledge Discovery. - 2017. - Vol. 7, № 5. - DOI: 10.1002/widm.1211.
10. Ahmad A., Maynard S.B., Park S. Information security strategies: towards an organizational multi-strategy perspective // Cluster Computing. - 2014. - Vol. 17, № 1. - P. 1–17. - DOI: 10.1007/s10586-013-0314-3.

Ingliz tili muharriri: *Norbekov Shohzod Mamarasul o'g'li*
Sahifalovchi va dizayner: *Zoirov Sardor Ziyodin o‘g‘li*

2026. № 2

Mazkur jurnalda maqolalar chop etish uchun quyidagi havolalarga maqola, reklama, hikoya va boshqa ijodiy materiallar yuborishingiz mumkin.
Materiallar va reklamalar pulli asosda chop etiladi.
El. pochta: journals@timeedu.uz
Tel.: +998 95 651 90 00

“Management and Economics Scientific Research Journal” jurnali 19.09.2024-yildan O‘zbekiston Respublikasi Prezidenti Administratsiyasi huzuridagi Axborot va ommaviy kommunikatsiyalar agentligi tomonidan 404368-son reyestr raqami tartibi bo‘yicha ro‘yxatdan o‘tkazilgan. Litsenziya raqami: C-5669639
PNFL: 308906510

Manzilimiz: *Toshkent shahar Yakkasaroy tumani Shota Rustaveli ko'chasi, 114*