УДК 34 **DOI: 10.34670/AR.2025.92.78.051**

Инсайдерская угроза как ключевой фактор компрометации персональных данных граждан в информационных системах МВД РФ: анализ черного рынка и коррупционных механизмов

Воронин Сергей Анатольевич

Кандидат юридических наук,
Ректор,
Национальный научно-исследовательский институт,
115191, Российская Федерация, Москва, Духовской переулок, 17/15;
e-mail: info@voroninpravo.ru

Аннотация

Настоящее исследование представляет собой комплексный анализ системной угрозы, исходящей от инсайдеров в структурах Министерства внутренних дел Российской Федерации (МВД РФ), для безопасности персональных данных граждан. Рассматривается феномен «пробива» – незаконного получения и продажи информации из закрытых государственных баз данных в режиме реального времени – как прямое проявление коррупции, а не как традиционный сбой в системе кибербезопасности. В работе детально анализируется экономическая структура черного рынка этих данных, исследуются социально-криминологические мотивы инсайдеров из числа сотрудников правоохранительных органов и дается критическая оценка неадекватности существующих технических и административных мер контроля. Через анализ правоприменительной практики оценивается сдерживающий эффект действующих правовых санкций. В заключение предлагается многоуровневая стратегическая модель противодействия данной угрозе, интегрирующая передовые технические решения (UEBA, Honeypots, PoLP), фундаментальные организационные реформы (ротация кадров, независимый аудит) и действенные правовые и экономические сдерживающие факторы. Научная новизна работы заключается в ее целостном подходе, синтезирующем технические, социологические и криминологические перспективы для решения проблемы человеческого фактора как основной уязвимости в государственных информационных системах.

Для цитирования в научных исследованиях

Воронин С.А. Инсайдерская угроза как ключевой фактор компрометации персональных данных граждан в информационных системах МВД РФ: анализ черного рынка и коррупционных механизмов // Вопросы российского и международного права. 2025. Том 15. № 10А. С. 437-450. DOI: 10.34670/AR.2025.92.78.051

Ключевые слова

Инсайдерская угроза, персональные данные, информационная безопасность, МВД РФ, коррупция, черный рынок данных, кибербезопасность, правоохранительные органы.

Введение

Детальный эмпирический анализ теневого рынка персональных данных, источником которых являются базы МВД, выявляет сложную и хорошо организованную экосистему. Данный раздел деконструирует структуру этого рынка, определяя ключевых акторов - от инсайдера-источника до конечного потребителя, - и анализирует основные каналы сбыта, экономические механизмы и динамику цен, которые указывают на системные уязвимости внутри государственных структур.

Основное содержание

Черный рынок функционирует через сеть посредников, которые рекламируют свои услуги на теневых площадках, таких как даркнет-форумы и Telegram-каналы, и напрямую взаимодействуют с инсайдерами в государственных ведомствах. По состоянию на начало 2024 года на этом рынке активно действовал 81 посредник, что свидетельствует о наличии стабильной и профессионализированной криминальной индустрии. Наблюдается четкая специализация услуг, которые условно делятся на три категории: «госпробив» (данные из государственных баз), «мобильный пробив» (данные операторов связи) и «банковский пробив» (банковская информация). [Исследователи подсчитали, что стоимость «пробива» персональных данных россиян в 2024 году увеличилась на 15–20%, 2024]

Сегмент «госпробива» является наиболее крупным и активным: 71 из 81 посредника (почти 88%) предлагают услуги по получению данных из государственных источников. За последний год число поставщиков в этом сегменте выросло на 22%, что указывает на значительное смещение рыночного фокуса в сторону правительственных баз данных. [Исследователи подсчитали, что стоимость «пробива» персональных данных россиян в 2024 году увеличилась на 15–20%, 2024] Предложение услуг, связанных с государственными базами, описывается как «всегда имеющееся в избытке», что подчеркивает широкое распространение инсайдерских источников в государственных структурах. [Представлен ежегодный обзор черного рынка «пробива» российских физлиц с 2023 года, 2023]

Информация из ключевых систем МВД доступна по поразительно низким ценам. Например, проверка по базе ГИБДД стоит от 500 до 1 000 рублей, а получение данных из системы отслеживания перемещений «Розыск-Магистраль» - около 1 500 рублей за одну запись. Эти цены остаются стабильными или даже незначительно снижаются, что свидетельствует о насыщенности рынка и низком операционном риске для инсайдеров. Аналогичным образом, проверка по системе «Роспаспорт» стоит около 1 000 рублей. [Цены черного рынка на «пробив» персональных данных в России выросли на 15–20% за год, 2024]

Хотя медианная стоимость комплексного «пробива» за последние семь лет выросла в 18,5 раз, этот рост почти полностью обусловлен увеличением стоимости и сложности получения данных из коммерческого сектора. [Исследователи подсчитали, что стоимость «пробива» персональных данных россиян в 2024 году увеличилась на 15–20%, 2024] Стоимость «мобильного пробива» выросла в 3,3 раза, достигая 100 000 рублей за детализацию звонков абонента за один месяц у некоторых операторов. Цены на банковские данные также возросли на 51%. [Представлен ежегодный обзор черного рынка «пробива» российских физлиц с 2023 года, 2023].

Это делает государственные данные «входным билетом» на черный рынок, доступным для широкого круга злоумышленников. Данная динамика свидетельствует не о случайных рыночных колебаниях, а о фундаментальных различиях в уровнях безопасности. Резкий рост цен на коммерческие данные отражает успешные усилия банков и телекоммуникационных компаний по борьбе с инсайдерами, что повышает риски и, следовательно, стоимость услуг. В то же время, низкая и стабильная цена на государственные данные указывает на системный провал механизмов внутреннего контроля в МВД, что создает для инсайдеров низкорисковый и высокодоходный рынок. TTelegram-боты, стали агрегаторами и дистрибьюторами незаконно полученных данных, автоматизируя доступ для массовой аудитории. [В сеть слили базу данных с личной информацией 774 тысяч клиентов Telegram-бота «Глаз бога», 2025] Эти боты консолидируют информацию из многочисленных утечек и скомпрометированных баз данных, включая те, что поставляются инсайдерами, и предоставляют удобный интерфейс для поиска по номеру телефона, электронной почте или имени. [В Москве к администратору телеграм-бота «Глаз бога» пришли с обыском, 2021]

Правовые меры, включая признание таких ботов деятельности незаконной судом и возбуждение первого в России уголовного дела по новой статье 272.1 УК РФ, подчеркивают внимание властей к этим платформам как к ключевым узлам в экосистеме торговли данными. [В сеть слили базу данных с личной информацией 774 тысяч клиентов Telegram-бота «Глаз бога», 2025]

Низкая стоимость и повсеместная доступность данных МВД (история поездок, сведения о владении автомобилем, паспортные данные) означают, что надзорные и контрольные функции государства были фактически коммодифицированы. Это представляет собой приватизацию государственных функций коррумпированными субъектами, что коренным образом подрывает верховенство права и доверие к государственным институтам.

Хотя финансовая выгода является основным стимулом, сама по себе она не является достаточным объяснением. Решение о продаже данных опосредовано целым рядом психологических и организационных факторов. Ключевым из них является повсеместное чувство безнаказанности, при котором предполагаемая вероятность быть пойманным и понести суровое наказание оценивается как низкая. Этот фактор часто оказывает большее влияние, чем размер потенциального вознаграждения. Другие мотивы могут включать личную месть, идеологические соображения или простую халатность и слабое понимание протоколов безопасности. [Кто такой инсайдер, виды и как обнаружить, 2024] Однако в центре внимания данного исследования находится умышленный, злонамеренный инсайдер, движимый коррупционными мотивами. Низкие зарплаты, особенно в регионах, создают уязвимость, которая в сочетании с возможностью и отсутствием надлежащего контроля приводит к преступному поведению, снижая порог для оправдания коррупционных действий. [Цены черного рынка на «пробив» персональных данных в России выросли на 15–20% за год, 2024]

Критическим, но часто упускаемым из виду фактором является нормализация девиантного поведения внутри организации. Показательным является случай с ботом «Глаз Бога»: исследование показало, что 41 из 50 опрошенных сотрудников полиции использовали этот нелегальный сервис для своей работы. [У команды телеграм-бота «Глаз Бога» прошли обыски по первому в России делу о незаконном использовании персональных данных, 2025] Это указывает на системную проблему, при которой официальные каналы получения информации настолько бюрократизированы и медленны, что сотрудники для повышения эффективности обращаются к черному рынку.

Такие действия размывают этические границы, нормализуют использование нелегальных источников данных и создают культуру, в которой доступ к информации и ее передача вне правовых рамок воспринимаются как приемлемые. Эта культура напрямую способствует переходу от использования нелегальных данных для работы к их продаже с целью получения прибыли, поскольку психологический барьер уже преодолен.

Таким образом, по мнению автора, правоохранительные органы становятся не только источником утечек, но и ключевым потребителем черного рынка. Это переосмысливает проблему: инсайдерская угроза заключается не только в том, что несколько «недобросовестных» сотрудников продают данные из МВД, но и в системной зависимости от нелегальной экосистемы данных для выполнения служебных обязанностей. Возникает симбиотическая, паразитическая связь с черным рынком, который ведомство должно искоренять. Это порождает конфликт интересов, когда использование нелегальных данных становится рутинной частью работы, их продажа превращается в гораздо меньший этический компромисс.

Основная проблема заключается в том, что традиционные меры безопасности нацелены на предотвращение несанкционированного доступа. Инсайдер, по определению, обладает санкционированным доступом. Стандартные средства контроля, такие как пароли и ролевой доступ, оказываются бессильны с самого начала. Информационные системы МВД, как известно, имеют уязвимости, включая использование устаревшего программного обеспечения и недостаточные технические меры защиты, что усугубляет проблему. [Информационная безопасность в органах внутренних дел Российской Федерации, 2024]

Существующим системам не хватает возможностей проактивного мониторинга. Они могут фиксировать события в логах, но не способны эффективно анализировать их в режиме реального времени для выявления аномальных моделей поведения, которые указывали бы на злоупотребление инсайдером своими легитимными полномочиями.

В МВД существует формализованный процесс проведения служебных проверок, регулируемый ведомственными приказами. [Порядок организации и проведения служебных расследований, 2023] Однако само существование черного рынка данных из баз МВД является неопровержимым доказательством того, что эти процедуры неэффективны в качестве средства выявления и сдерживания. Эти проверки, как правило, носят реактивный характер и инициируются только после поступления жалобы или обнаружения очевидного нарушения, а не для проактивного поиска угроз.

Кроме того, сам процесс проверок может быть подвержен влиянию внутренней политики и коррупции, когда расследования в отношении коллег не проводятся с должной тщательностью. Отсутствует по-настоящему независимая функция аудита, способная анализировать логи запросов без предвзятости и опасений. Ведомственные нормативные акты, такие как «Инструкция по организации защиты персональных данных» (Приказ № 678) [Приказ МВД России от 06.07.2012 № 678 «Об утверждении Инструкции по организации защиты персональных данных...», 2012] и Положение о Департаменте информационных технологий, связи и защиты информации (Приказ № 444) [Об утверждении Положения о Департаменте информационных технологий, связи и защиты информации Министерства внутренних дел Российской Федерации, 2021], существуют на бумаге, но их реальное исполнение очевидно неэффективно.

Проблема заключается не только в отсутствии технологий или сбоях в процедурах, но и в их пагубном взаимодействии. Слабые технические средства контроля (отсутствие поведенческого анализа) создают возможность для злоупотреблений, а несовершенная

административная и культурная среда (неэффективные расследования, нормализация девиантного поведения) гарантирует, что этой возможностью можно воспользоваться с минимальным риском.

В данном разделе рассматривается правовое измерение проблемы. Анализируются судебные приговоры в отношении сотрудников МВД, осужденных за продажу данных, с акцентом на типы и суровость применяемых наказаний. Основная задача - оценить, являются ли эти меры достаточным сдерживающим фактором в сравнении с потенциальной финансовой выгодой и низким воспринимаемым риском разоблачения.

Дела в отношении сотрудников полиции часто возбуждались по таким статьям, как ст. 286 УК РФ («Превышение должностных полномочий»). Наказания могли включать штрафы (от 100 до 300 тыс. рублей), принудительные работы или лишение свободы. [Полицейских поймали на продаже персональных данных из БД МВД России, 2018] Также применялись статьи за неправомерный доступ к компьютерной информации (ст. 272) и нарушение тайны переписки. [Разглашение персональных данных — ответственность по ст. 137 УК РФ за распространение ПДн без согласия владельца, 2024]

Однако эти наказания, особенно штрафы, были несоизмеримо малы по сравнению с потенциальным совокупным доходом от продажи данных. В одном из дел упоминаются сотрудники, заработавшие более 700 000 рублей чуть более чем за год [Полицейских поймали на продаже персональных данных из БД МВД России, 2018] - сумма, значительно превышающая минимальные штрафы. Это создавало положительное математическое ожидание от преступной деятельности, делая ее экономически привлекательной.

Масштабная законодательная реформа, кардинально ужесточает ответственность за преступления, связанные с персональными данными.

– **Федеральный закон № 420-ФЗ** вносит поправки в Кодекс об административных правонарушениях (КоАП), вводя огромные, многоуровневые штрафы для организаций, размер которых зависит от количества субъектов, чьи данные утекли. Штрафы для юридических лиц могут достигать 15-20 млн рублей, а за повторные нарушения предусмотрены еще более высокие «оборотные» штрафы. [С 30 мая 2025 года значительно ужесточена ответственность за нарушение законодательства о персональных данных, 2025]
– **Федеральный закон № 421-ФЗ** вносит изменения в Уголовный кодекс (УК), вводя новую специальную статью 272.1 за незаконное использование и оборот персональных данных, предусматривающую наказание до 10 лет лишения свободы. [У команды телеграм-бота «Глаз Бога» прошли обыски по первому в России делу о незаконном использовании персональных данных, 2025]

Эти изменения представляют собой значительный сдвиг в подходе государства, сигнализируя о том, что защита данных теперь является высокоприоритетной задачей.

Таблица 1 - Эволюция юридической ответственности за незаконный оборот персональных данных в РФ

Вид правонарушения	Ответственность (до 2025 г.)	Ответственность (после 2025 г.)
Неправомерный доступ и продажа данных сотрудником	ст. 286 УК РФ: Штраф 100-300 тыс. руб. или лишение свободы [Полицейских поймали на продаже персональных данных из БД МВД России, 2018]	ст. 272.1 УК РФ: Лишение свободы на срок до 10 лет [У команды телеграм-бота «Глаз Бога» прошли обыски по первому в России делу о незаконном использовании персональных данных, 2025]

Вид правонарушения	Ответственность (до 2025 г.)	Ответственность (после 2025 г.)
Утечка данных (административная ответственность)	ст. 13.11 КоАП: Штраф для юрлиц 60-100 тыс. руб. [Ужесточение ответственности за нарушения при обработке персональных данных, 2025]	ст. 13.11 КоАП (новая ред.): Штрафы для юрлиц до 15-20 млн руб. и оборотные штрафы [С 30 мая 2025 года значительно ужесточена ответственность за нарушение законодательства о персональных данных, 2025]

Анализ нового законодательства выявляет потенциальное структурное несоответствие. Основные финансовые санкции нацелены на оператора данных как на юридическое лицо («принципала»). Однако в МВД проблема исходит от отдельного коррумпированного сотрудника («агента»), действующего в своих интересах. Сдерживающий эффект огромного институционального штрафа, который сотрудник лично не платит, на его персональный расчет «риск-вознаграждение» может быть ограниченным. Эффективность новых мер будет в решающей степени зависеть от того, насколько последовательно и жестко новые уголовные наказания по ст. 272.1 УК РФ будут применяться к отдельным сотрудникам.

На основе проведенного анализа предлагается комплексная, интегрированная стратегия по снижению инсайдерской угрозы в МВД. Предлагаемая модель структурирована по трем взаимозависимым уровням: техническому, организационному и право-экономическому. Данный подход основан на синергии, где каждый компонент усиливает остальные, создавая эшелонированную защиту, специально адаптированную к человеческому фактору.

Аналитика поведения пользователей и сущностей (UEBA): внедрение систем UEBA является первоочередной задачей. Эти системы используют машинное обучение для создания базовой модели нормального поведения каждого пользователя и затем автоматически обнаруживают отклонения. [Инсайдерские угрозы: как защитить компанию изнутри?, 2025] Примеры аномалий, которые может выявить UEBA: сотрудник внезапно запрашивает данные за пределами своей географической или ведомственной юрисдикции; получает доступ к необычно большому объему записей за короткий промежуток времени; запрашивает информацию о высокопоставленных лицах без привязки к зарегистрированному делу; входит в систему в нерабочее время. На российском рынке существуют решения UEBA, которые могут быть адаптированы для этих целей. [UEBA-системы: что это, обзор рынка, сравнительный анализ решений, 2024]

– «Приманки» (Honeypots) и технологии обмана: Стратегическое размещение фиктивных записей или баз данных-«приманок» внутри реальных систем может служить системой раннего предупреждения. [Что такое Honeypot? Как они используются в кибербезопасности, 2024] Любой доступ к этим фальшивым данным по определению является несанкционированным и злонамеренным. Это позволяет не только немедленно выявить инсайдера, но и собрать информацию о его методах и потенциальных заказчиках. [Подробное руководство по Honeypot, 2024]
– Принцип минимальных привилегий (PoLP): Необходимо радикальное и строгое внедрение PoLP. Доступ должен предоставляться не на основании звания или должности, а по принципу «необходимости знания» для конкретного, активного расследования. [Повышение безопасности приложений с помощью принципа наименьших привилегий, 2024] Это означает динамическое предоставление и отзыв доступа к конкретным наборам данных на ограниченный период времени (Just-in-Time доступ), а не постоянный доступ ко всем базам данных. Это резко сокращает «поверхность атаки», доступную любому потенциальному инсайдеру.

Таблица 2 - Сравнительный анализ проактивных технологий противодействия инсайдерам

Технология	Механизм действия	Основная польза для МВД	Проблемы внедрения
UEBA	Машинное обучение для выявления аномалий в поведении легитимных пользователей.	Выявление злоупотреблений законным доступом, что является ключевой проблемой.	Высокая стоимость; необходимость интеграции с устаревшими системами; требует квалифицированных аналитиков для настройки и снижения ложных срабатываний.
Honeypots	Размещение ложных данных-«приманок» в реальных системах. Любое обращение к ним - тревожный сигнал.	Раннее обнаружение инсайдеров и сбор информации об их действиях с минимальным риском для реальных данных.	Риск обнаружения «приманки» опытным злоумышленником; необходимость постоянного обновления для сохранения правдоподобности.
PoLP	Предоставление пользователям минимально необходимого набора прав для выполнения конкретной задачи.	Кардинальное сужение поля для злоупотреблений; даже в случае компрометации ущерб будет ограничен.	Организационное сопротивление; сложность в определении минимально необходимых прав для каждой роли; требует перестройки бизнес-процессов.

– Обязательная, внезапная ротация кадров: как проверенная антикоррупционная мера, сотрудники на должностях с доступом к чувствительным данным должны подвергаться регулярной и непредсказуемой ротации. [Федеральный закон от 27.07.2004 № 79-ФЗ «О государственной гражданской службе Российской Федерации», 2004] Это препятствует формированию устоявшихся коррупционных сетей и нарушает налаженные каналы продажи данных.

– Создание независимого подразделения аудита: необходимо создать специализированное, технически грамотное и организационно независимое подразделение с единственной задачей - аудит всех запросов к чувствительным базам данных. Это подразделение должно иметь полномочия расследовать действия любого пользователя, независимо от звания, и докладывать о результатах вышестоящему надзорному органу вне стандартной командной цепи МВД для обеспечения беспристрастности.

– Реформа внутренних расследований: Процесс служебных проверок должен быть реформирован, чтобы стать более прозрачным, быстрым и строгим в случаях компрометации данных. Цель - изменить восприятие риска инсайдером с «маловероятно быть пойманным» на «неизбежно быть расследованным».

Экономические и превентивные меры: изменение расчета «риск-вознаграждение»:

– Жесткое правоприменение: новые, более суровые наказания, предусмотренные законодательством 2025 года, должны применяться последовательно и публично в отношении осужденных сотрудников МВД. Широкое освещение приговоров может служить мощным сдерживающим фактором для других. Преступление должно квалифицироваться не как простая утечка данных, а как предательство общественного доверия и угроза государственной безопасности.

– Антикоррупционное просвещение и программы лояльности: хотя это часто воспринимается как «мягкие» меры, непрерывное и содержательное антикоррупционное

обучение необходимо для укрепления этических норм. [Первый федеральный университет антикоррупционного просвещения: обучение в сфере противодействия коррупции, 2025] Оно должно сочетаться с программами, направленными на повышение лояльности и морального духа сотрудников, устраняя коренные мотивационные факторы, такие как низкая оплата труда и плохие условия службы, тем самым сокращая «предложение» потенциальных инсайдеров. [Программа лояльности, 2024]

Внедрение этих мер требует фундаментального философского сдвига внутри МВД - перехода от модели, которая по умолчанию доверяет своим сотрудникам («доверяй, но проверяй»), к парадигме «нулевого доверия» (Zero Trust), являющейся основой современной кибербезопасности. [Принцип минимальных привилегий..., 2024] Это предполагает признание неудобной реальности, что наибольшая угроза может исходить изнутри, и построение системы, основанной на непрерывной верификации, а не на доверии по умолчанию. Это самая сложная, но и самая важная рекомендация данного исследования.

Заключение

Проблема инсайдерских угроз и коррупции в сфере доступа к чувствительным данным требует не изолированных решений, а комплексной и связанной системы мер. Предложенные в исследовании шаги — от внезапной ротации кадров и создания независимого аудита до ужесточения правоприменения и антикоррупционного просвещения — направлены на формирование многоуровневой системы сдерживания и профилактики. Их объединяет цель кардинально изменить внутреннее «рассчетливость» потенциального нарушителя, сместив баланс «риск-вознаграждение» в сторону неприемлемо высокого риска.

Однако подлинная эффективность этих мер возможна лишь при условии фундаментального культурного и философского сдвига внутри силовых структур. Необходим переход от устаревшей парадигмы «доверяй, но проверяй» к принципу архитектурного «нулевого доверия» (Zero Trust), где любое действие верифицируется, а доверие по умолчанию не предоставляется. Это предполагает признание того, что наибольшая угроза безопасности может исходить изнутри, и построение системы, основанной на непрерывном контроле и прозрачности.

Таким образом, борьба с внутренними угрозами — это не только вопрос технических и процедурных усовершенствований, но и проблема управления культурой организации. Реализация предложенных рекомендаций призвана создать не только барьеры для злоупотреблений, но и среду, в которой этика, лояльность и подотчетность становятся неотъемлемыми компонентами служебной деятельности. Это сложный, но необходимый путь для восстановления и защиты общественного доверия и государственной безопасности.

Библиография

1. Исследователи подсчитали, что стоимость «пробива … [Электронный ресурс] // Хакер. URL: https://xakep.ru/2024/03/20/probiv-stats/ (дата обращения: 05.10.2025).
2. Представлен ежегодный обзор черного рынка «пробива … [Электронный ресурс] // ITSec.Ru. URL: https://www.itsec.ru/news/predstavlen-ezhegodniy-obzor-chiornogo-rinka-probiva-rossiyskih-fizliz-c-2023-goda (дата обращения: 05.10.2025).
3. В России выросла стоимость «пробива» информации о гражданах [Электронный ресурс] // ITSec.Ru. URL: https://www.itsec.ru/news/v-rossii-virosla-stoimost-probiva-informazii-o-grazhdanah (дата обращения: 05.10.2025).
4. Цены черного рынка на «пробив» персональных данных … [Электронный ресурс] // BatmanStore.ru. URL: https://batmanstore.ru/news/75104/ (дата обращения: 05.10.2025).

5. Стоимость «слива» информации о гражданах России за год выросла в 2,5 раза [Электронный ресурс] // CNews. URL: https://www.cnews.ru/news/top/2024-03-20_stoimost_sliva_informatsii (дата обращения: 05.10.2025).
6. В сеть слили базу данных с личной информацией 774 тысяч … [Электронный ресурс] // CGITC. URL: https://cgitc.ru/media/v-set-slili-bazu-dannykh-s-lichnoy-informatsiey-774-tysyach-klientov-telegram-bota-glaz-boga/ (дата обращения: 05.10.2025).
7. У команды сервиса для «пробива» «Глаз Бога» прошли обыски … [Электронный ресурс] // Медуза. URL: https://meduza.io/news/2025/02/28/u-komandy-servisa-dlya-probiva-glaz-boga-proshli-obyski-telegram-bot-seychas-ne-rabotaet (дата обращения: 05.10.2025).
8. В Москве к администратору телеграм-бота «Глаз бога» пришли с обыском [Электронный ресурс] // ОВД-Инфо. URL: https://ovd.info/express-news/2021/04/07/v-moskve-k-administratoru-telegram-bota-glaz-boga-prishli-s-obyskom (дата обращения: 05.10.2025).
9. СМИ: дело «Глаза Бога» связано с попыткой взлома баз … [Электронный ресурс] // Банки.ру. URL: https://www.banki.ru/news/lenta/?id=10944637 (дата обращения: 05.10.2025).
10. У команды телеграм-бота «Глаз Бога» прошли обыски по … [Электронный ресурс] // iStories. URL: https://istories.media/news/2025/02/28/u-komandi-telegrambota-glaz-boga-proshli-obiski-po-pervomu-v-rossii-delu-o-nezakonnom-ispolzovanii-personalnikh-dannikh/ (дата обращения: 05.10.2025).
11. Кто такой инсайдер, виды и как обнаружить [Электронный ресурс] // Spectrumdata. URL: https://spectrumdata.ru/blog/proverka-soiskatelya/kto-takie-insaydery-i-pochemu-oni-opasny-dlya-biznesa-i-finansovykh-rynkov/ (дата обращения: 05.10.2025).
12. Информационная безопасность в органах внутренних дел … [Электронный ресурс] // uzulo.su. URL: http://uzulo.su/prav-inf/pdf-jpg/pi-2024-2-st18-s170-180.pdf (дата обращения: 05.10.2025).
13. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (Выписка) (утв. ФСТЭК РФ 15.02.2008).
14. Порядок организации и проведения служебных расследований [Электронный ресурс] // ИД «Советник». URL: https://sec-company.ru/articles/economics/poryadok_organizatsii_i_provedeniya_sluzhebnykh_rassledovaniy/ (дата обращения: 05.10.2025).
15. Федеральный закон от 30.11.2011 № 342-ФЗ (ред. от 28.12.2024) «О службе в органах внутренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации» (с изм. и доп., вступ. в силу с 05.02.2025).
16. Порядок проведения служебной проверки в органах, организациях и подразделениях Министерства внутренних дел Российской Федерации (Приложение к приказу МВД РФ от 26 марта 2013 г. № 161).
17. Приказ МВД России от 06.07.2012 № 678 (ред. от 07.12.2016) «Об утверждении Инструкции по организации защиты персональных данных, содержащихся в информационных системах органов внутренних дел Российской Федерации» (Зарегистрировано в Минюсте России 18.09.2012 № 25488).
18. Об утверждении Положения о Департаменте информационных … [Электронный ресурс] // CNTD.ru. URL: https://docs.cntd.ru/document/607325903 (дата обращения: 05.10.2025).
19. Приказ МВД России от 15.06.2021 № 444 (ред. от 31.03.2025) «Об утверждении положения о Департаменте информационных технологий, связи и защиты информации Министерства внутренних дел Российской Федерации».
20. Полицейских поймали на продаже персональных данных … [Электронный ресурс] // CNews. URL: https://www.cnews.ru/news/top/2018-03-14_dvoih_rossijskih_politsejskih_budut_sudit_za (дата обращения: 05.10.2025).
21. Разглашение персональных данных — ответственность по ст. 137 УК РФ за распространение ПДн без согласия владельца [Электронный ресурс] // Data-Sec.ru. URL: https://data-sec.ru/personal-data/disclosure-responsibility/ (дата обращения: 05.10.2025).
22. Преступления в сфере компьютерной информации — ст. 272 УК РФ [Электронный ресурс] // RTM Group. URL: https://rtmtech.ru/articles/prestupleniya-v-sfere-kompyuternoj-informatsii-st-272-uk-rf/ (дата обращения: 05.10.2025).
23. Ответственность за нарушение закона о персональных данных [Электронный ресурс] // ГАРАНТ. URL: https://www.garant.ru/actual/persona/otvetstvennost/ (дата обращения: 05.10.2025).
24. С 30 мая 2025 года значительно ужесточена ответственность за … [Электронный ресурс] // КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_490308/3b904c06ca00c18b687ec94295a0a967ddc5cce7/ (дата обращения: 05.10.2025).
25. Изменения в обработке и защите персональных данных в 2025 году [Электронный ресурс] // Сберкорус. URL: https://www.esphere.ru/blog/izmeneniya-v-obrabotke-i-zashchite-personalnykh-dannykh-v-2025-godu/ (дата обращения: 05.10.2025).
26. Ужесточение ответственности за нарушение законодательства о персональных данных [Электронный ресурс] // Юникон. URL: https://www.unicon.ru/insights/obzor-izmenenii-zakonodatelstva/Tougher_liability_for_violations_of_the_law_on_personal_data/ (дата обращения: 05.10.2025).

27. Ужесточение ответственности за нарушения при обработке персональных данных [Электронный ресурс] // Nordic Star. URL: https://www.nordicstar.law/news/%D1%83%D0%B6%D0%B5%D1%81%D1%82%D0%BE%D1%87%D0%B5%D0%BD%D0%B8%D0%B5-%D0%BE%D1%82%D0%B2%D0%B5%D1%82%D1%81%D1%82%D0%B2%D0%B5%D0%BD%D0%BD%D0%BE%D1%81%D1%82%D0%B8-%D0%B7%D0%B0-%D0%BD%D0%B0%D1%80%D1%83/ (дата обращения: 05.10.2025).
28. Персональные данные: ужесточение ответственности и другие законодательные инициативы [Электронный ресурс] // АБ ЕПАМ. URL: https://epam.ru/ru/media/view/personalnye-dannye:-uzhestochenie-otvetstvennosti-i-drugie-zakonodatelnye-iniciativy (дата обращения: 05.10.2025).
29. Ответственность за обработку персональных данных: изменения 2025 года [Электронный ресурс] // Контур. URL: https://kontur.ru/articles/55870-otvetstvennost_za_obrabotku_pers_dannyh (дата обращения: 05.10.2025).
30. Изменения закона о персональных данных в 2025 году [Электронный ресурс] // Qugo. URL: https://qugo.ru/blog/izmeneniya-zakona-o-personalnyh-dannyh-v-2025-godu (дата обращения: 05.10.2025).
31. Новые правила защиты данных с 2025 года: что нужно знать [Электронный ресурс] // NeptunIT. URL: https://ntcneptunit.ru/blog/novye-pravila-zashchity-dannyh-2025 (дата обращения: 05.10.2025).
32. Ужесточение штрафов за утечку персональных данных: что изменилось с 30 мая 2025 года [Электронный ресурс] // ЭР-Телеком. URL: https://r-soc.ertelecom.ru/announcements/article/33 (дата обращения: 05.10.2025).
33. Инсайдерские угрозы: как защитить компанию изнутри? [Электронный ресурс] // ИНФАРС. URL: https://infars.ru/blog/insayderskie-ugrozy-kak-zashchitit-kompaniyu-iznutri/ (дата обращения: 05.10.2025).
34. What Is User and Entity Behavior Analytics (UEBA)? [Электронный ресурс] // Microsoft. URL: https://www.microsoft.com/en-us/security/business/security-101/what-is-user-entity-behavior-analytics-ueba (дата обращения: 05.10.2025).
35. What is User Entity and Behavior Analytics (UEBA)? [Электронный ресурс] // Fortinet. URL: https://www.fortinet.com/resources/cyberglossary/what-is-ueba (дата обращения: 05.10.2025).
36. What is UEBA (User and Entity Behavior Analytics)? [Электронный ресурс] // Palo Alto Networks. URL: https://www.paloaltonetworks.com/cyberpedia/what-is-user-entity-behavior-analytics-ueba (дата обращения: 05.10.2025).
37. What is User and Entity Behavior Analytics (UEBA)? [Электронный ресурс] // CrowdStrike. URL: https://www.crowdstrike.com/en-us/cybersecurity-101/identity-protection/user-and-entity-behavior-analytics-ueba/ (дата обращения: 05.10.2025).
38. User and Entity Behavior Analytics (UEBA) [Электронный ресурс] // Check Point Software. URL: https://www.checkpoint.com/cyber-hub/threat-prevention/user-and-entity-behavior-analytics-ueba/ (дата обращения: 05.10.2025).
39. What is User and Entity Behavior Analytics (UEBA)? [Электронный ресурс] // Rapid7. URL: https://www.rapid7.com/fundamentals/user-behavior-analytics/ (дата обращения: 05.10.2025).
40. UEBA-системы: что это, обзор рынка, сравнительный анализ … [Электронный ресурс] // xn--80aidjgwzd.xn--p1ai. URL: https://xn--80aidjgwzd.xn--p1ai/news/ueba_sistemy/ (дата обращения: 05.10.2025).
41. Что такое Honeypot? Как они используются в кибербезопасности [Электронный ресурс] // IB-BANK.ru. URL: https://ib-bank.ru/bisjournal/news/15637 (дата обращения: 05.10.2025).
42. Что такое honeypot? Как ловушки служат кибербезопасности [Электронный ресурс] // Kaspersky. URL: https://www.kaspersky.ru/resource-center/threats/what-is-a-honeypot (дата обращения: 05.10.2025).
43. Подробное руководство по Honeypot: как работает ловушка для атакующих [Электронный ресурс] // Glabit. URL: https://glabit.ru/blog/honeypot-guide (дата обращения: 05.10.2025).
44. Подробное руководство по Honeypot [Электронный ресурс] // Habr. URL: https://habr.com/ru/companies/alexhost/articles/528796/ (дата обращения: 05.10.2025).
45. Технология Honeypot. Часть 1: Назначение Honeypot [Электронный ресурс] // SecurityLab. URL: https://www.securitylab.ru/analytics/275420.php (дата обращения: 05.10.2025).
46. Повышение безопасности приложений с помощью принципа наименьших привилегий [Электронный ресурс] // Microsoft Learn. URL: https://learn.microsoft.com/ru-ru/entra/identity-platform/secure-least-privileged-access (дата обращения: 05.10.2025).
47. Принцип минимальных привилегий. Кибрарий [Электронный ресурс] // Сбербанк. URL: https://www.sberbank.ru/ru/person/kibrary/vocabulary/princip-minimalnykh-privilegij (дата обращения: 05.10.2025).
48. Что такое доступ с наименьшими привилегиями? [Электронный ресурс] // Keeper Security. URL: https://www.keepersecurity.com/ru_RU/resources/glossary/what-is-least-privilege-access/ (дата обращения: 05.10.2025).
49. Понимание принципа минимальных привилегий в Microsoft Entra ID Governance [Электронный ресурс] // Microsoft Learn. URL: https://learn.microsoft.com/ru-ru/entra/id-governance/scenarios/least-privileged (дата обращения: 05.10.2025).

50. Принцип минимальных привилегий (Principle of least privilege) [Электронный ресурс] // Энциклопедия Kaspersky. URL: https://encyclopedia.kaspersky.ru/glossary/principle-of-least-privilege-polp/ (дата обр.: 05.10.2025).
51. Принцип наименьших привилегий [Электронный ресурс] // IBM Docs. URL: https://www.ibm.com/docs/ru/aix/7.1.0?topic=software-least-privilege (дата обращения: 05.10.2025).
52. What Is the Principle of Least Privilege? [Электронный ресурс] // Palo Alto Networks. URL: https://www.paloaltonetworks.com/cyberpedia/what-is-the-principle-of-least-privilege (дата обращения: 05.10.2025).
53. Федеральный закон от 27.07.2004 № 79-ФЗ (ред. от 29.09.2025) «О государственной гражданской службе Российской Федерации».
54. Сборник материалов по исследованию зарубежного опыта противодействия коррупции [Электронный ресурс] // GOV.KZ. URL: https://www.gov.kz/memleket/entities/anticorruption/press/article/details/2281?lang=ru (дата обращения: 05.10.2025).
55. Ротация кадров на государственной службе как мера по предупреждению коррупции … [Электронный ресурс] // Молодой учёный. URL: https://moluch.ru/archive/443/96911 (дата обращения: 05.10.2025).
56. Как бороться с коррупцией среди чиновников? Один из вариантов — ротация [Электронный ресурс] // Onlíner. URL: https://people.onliner.by/2019/10/31/rotate (дата обращения: 05.10.2025).
57. Первый федеральный университет антикоррупционного просвещения: обучение в сфере противодействия коррупции [Электронный ресурс] // ФУАП. URL: https://fuap.ru/ (дата обращения: 05.10.2025).
58. Типовые программы в области противодействия коррупции: обучение госслужащих [Электронный ресурс] // ФУАП. URL: https://fuap.ru/lib/antikorruptsionnoe-obuchenie/tipovye-programmy-v-oblasti-protivodeystviya-korruptsii-obuchenie-gossluzhashchikh/ (дата обращения: 05.10.2025).
59. Программа лояльности [Электронный ресурс] // Московская федерация профсоюзов. URL: https://mtuf.ru/loyalty-program/ (дата обращения: 05.10.2025).

Insider Threat as a Key Factor in Compromising Citizens' Personal Data in Information Systems of the Ministry of Internal Affairs of the Russian Federation: Analysis of the Black Market and Corruption Mechanisms

Sergei A. Voronin

PhD in Legal Sciences, Rector,
National Scientific Research Institute,
115191, 17/15, Dukhovskoy lane, Moscow, Russian Federation;
e-mail: info@voroninpravo.ru

Abstract

This research presents a comprehensive analysis of the systemic threat emanating from insiders within the structures of the Ministry of Internal Affairs of the Russian Federation (MVD RF) for the security of citizens' personal data. The phenomenon of "probiv" – illegal acquisition and sale of information from closed state databases in real-time mode – is examined as a direct manifestation of corruption, rather than as a traditional failure in the cybersecurity system. The work analyzes in detail the economic structure of the black market for this data, investigates socio-criminological motives of insiders among law enforcement personnel, and provides a critical assessment of the inadequacy of existing technical and administrative control measures. Through analysis of law enforcement practice, the deterrent effect of current legal sanctions is evaluated. In conclusion, a multi-level strategic model for countering this threat is proposed, integrating advanced technical solutions (UEBA, Honeypots, PoLP), fundamental organizational reforms (personnel rotation, independent audit), and effective legal and economic deterrents. The scientific novelty of the work lies in its holistic approach, synthesizing technical, sociological, and criminological perspectives to address the problem of the human factor as the main vulnerability in state information systems.

For citation

Voronin S.A. (2025) Insayderskaya ugroza kak klyuchevoy faktor komprometatsii personal'nykh dannykh grazhdan v informatsionnykh sistemakh MVD RF: analiz chernogo rynka i korruptsionnykh mekhanizmov [Insider Threat as a Key Factor in Compromising Citizens' Personal Data in Information Systems of the Ministry of Internal Affairs of the Russian Federation: Analysis of the Black Market and Corruption Mechanisms]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 15 (10A), pp. 437-450. DOI: 10.34670/AR.2025.92.78.051

Keywords

Insider threat, personal data, information security, MVD RF, corruption, data black market, cybersecurity, law enforcement agencies.

References

1. Researchers have calculated that the cost of "penetrating... [Electronic resource] // Hacker. URL: https://xakep.ru/2024/03/20/probiv-stats/ (date of access: 05.10.2025).
2. An annual review of the black market for "penetrating..." is presented [Electronic resource] // ITSec.Ru. URL: https://www.itsec.ru/news/predstavlen-ezhegodniy-obzor-chiornogo-rinka-probiva-rossiyskih-fizliz-c-2023-goda (date of access: 05.10.2025).
3. The cost of "penetrating" information about citizens has increased in Russia [Electronic resource] // ITSec.Ru. URL: https://www.itsec.ru/news/v-rossii-virosla-stoimost-probiva-informazii-o-grazhdanah (Accessed: 05.10.2025).
4. Black market prices for "leaking" personal data... [Electronic resource] // BatmanStore.ru. URL: https://batmanstore.ru/news/75104/ (Accessed: 05.10.2025).
5. The cost of "leaking" information about Russian citizens has increased 2.5 times in a year [Electronic resource] // CNews. URL: https://www.cnews.ru/news/top/2024-03-20_stoimost_sliva_informatsii (Accessed: 05.10.2025).
6. A database containing the personal information of 774,000 people was leaked online... [Electronic resource] // CGITC. URL: https://cgitc.ru/media/v-set-slili-bazu-dannykh-s-lichnoy-informatsiey-774-tysyach-klientov-telegram-bota-glaz-boga/ (accessed: 10/05/2025).
7. The team behind the "God's Eye" intelligence service were searched... [Electronic resource] // Meduza. URL: https://meduza.io/news/2025/02/28/u-komandy-servisa-dlya-probiva-glaz-boga-proshli-obyski-telegram-bot-seychas-ne-rabotaet (accessed: 10/05/2025).
8. In Moscow, the administrator of the "Eye of God" Telegram bot was searched [Electronic resource] // OVD-Info. URL: https://ovd.info/express-news/2021/04/07/v-moskve-k-administratoru-telegram-bota-glaz-boga-prishli-s-obyskom (accessed: 05.10.2025).
9. Media: the "Eye of God" case is connected with an attempt to hack the databases of ... [Electronic resource] // Banki.ru. URL: https://www.banki.ru/news/lenta/?id=10944637 (accessed: 05.10.2025).
10. The team of the "Eye of God" Telegram bot was searched ... [Electronic resource] // iStories. URL: https://istories.media/news/2025/02/28/u-komandi-telegrambota-glaz-boga-proshli-obiski-po-pervomu-v-rossii-delu-o-nezakonnom-ispolzovanii-personalnikh-dannikh/ (Accessed: 05.10.2025).
11. Who is an insider, types and how to detect [Electronic resource] // Spectrumdata. URL: https://spectrumdata.ru/blog/proverka-soiskatelya/kto-takie-insaydery-i-pochemu-oni-opasny-dlya-biznesa-i-finansovykh-rynkov/ (05.10.2025).
12. Information security in internal affairs agencies … [Electronic resource] // uzulo.su. URL: http://uzulo.su/prav-inf/pdf-jpg/pi-2024-2-st18-s170-180.pdf (Accessed: 05.10.2025).
13. "Basic Model of Personal Data Security Threats When Processed in Personal Data Information Systems" (Extract) (approved by the FSTEC of the Russian Federation on 15.02.2008).
14. Procedure for Organizing and Conducting Official Investigations [Electronic resource] // Publishing House "Advisor". URL: https://sec-company.ru/articles/economics/poryadok_organizatsii_i_provedeniya_sluzhebnykh_rassledovaniy/ (Accessed: 05.10.2025).
15. Federal Law No. 342-FZ of November 30, 2011 (as amended on December 28, 2024) "On Service in the Internal Affairs Bodies of the Russian Federation and Amendments to Certain Legislative Acts of the Russian Federation" (as amended and supplemented, effective February 5, 2025).
16. Procedure for Conducting an Internal Investigation in Bodies, Organizations, and Divisions of the Ministry of Internal Affairs of the Russian Federation (Appendix to Order No. 161 of the Ministry of Internal Affairs of the Russian Federation dated March 26, 2013).

17. Order of the Ministry of Internal Affairs of Russia dated July 6, 2012 No. 678 (as amended on December 7, 2016) "On Approval of the Instructions for Organizing the Protection of Personal Data Contained in the Information Systems of the Internal Affairs Bodies of the Russian Federation" (Registered in the Ministry of Justice of Russia on September 18, 2012 No. 25488).
18. On Approval of the Regulation on the Department of Information … [Electronic resource] // CNTD.ru. URL: https://docs.cntd.ru/document/607325903 (date accessed: October 5, 2025).
19. Order of the Ministry of Internal Affairs of Russia dated June 15, 2021 No. 444 (as amended on March 31, 2025) "On Approval of the Regulation on the Department of Information Technology, Communications, and Information Protection of the Ministry of Internal Affairs of the Russian Federation".
20. Police officers caught selling personal data... [Electronic resource] // CNews. URL: https://www.cnews.ru/news/top/2018-03-14_dvoih_rossijskih_politsejskih_budut_sudit_za (date of access: 05.10.2025).
21. Disclosure of personal data — liability under Article 137 of the Criminal Code of the Russian Federation for dissemination of personal data without the owner's consent [Electronic resource] // Data-Sec.ru. URL: https://data-sec.ru/personal-data/disclosure-responsibility/ (date of access: 05.10.2025).
22. Crimes in the field of computer information — Article 272 of the Criminal Code of the Russian Federation [Electronic resource] // RTM Group. URL: https://rtmtech.ru/articles/prestupleniya-v-sfere-kompyuternoj-informatsii-st-272-uk-rf/ (Accessed: October 5, 2025).
23. Liability for Violating the Law on Personal Data [Electronic Resource] // GARANTEE. URL: https://www.garant.ru/actual/persona/otvetstvennost/ (Accessed: October 5, 2025).
24. From May 30, 2025 The penalties for... have been significantly increased [Electronic resource] // ConsultantPlus. URL: https://www.consultant.ru/document/cons_doc_LAW_490308/3b904c06ca00c18b687ec94295a0a967ddc5cce7/ (accessed on October 5, 2025).
25. Changes in the processing and protection of personal data in 2025 [Electronic resource] // Sberkorus. URL: https://www.esphere.ru/blog/izmeneniya-v-obrabotke-i-zashchite-personalnykh-dannykh-v-2025-godu/ (accessed on October 5, 2025).
26. Increased penalties for violating personal data legislation [Electronic resource] // Unicon. URL: https://www.unicon.ru/insights/obzor-izmenenii-zakonodatelstva/Tougher_liability_for_violations_of_the_law_on_personal_data/ (Accessed: 05.10.2025).
27. Tightening Penalties for Violations in the Processing of Personal Data [Electronic Resource] // Nordic Star. URL: https://www.nordicstar.law/news/%D1%83%D0%B6%D0%B5%D1%81%D1%82%D0%BE%D1%87%D0%B5%D0%BD%D0%B8%D0%B5-%D0%BE%D1%82%D0%B2%D0%B5%D1%82%D1%81%D1%82%D0%B2%D0%B5%D0%BD%D0%BD%D0%BE%D1%81%D1%82%D0%B8-%D0%B7%D0%B0-%D0%BD%D0%B0%D1%80%D1%83/ (date of access: 05.10.2025).
28. Personal Data: Tightening Liability and Other Legislative Initiatives [Electronic resource] // EPAM Law Firm. URL: https://epam.ru/ru/media/view/personalnye-dannye:-uzhestochenie-otvetstvennosti-i-drugie-zakonodatelnye-iniciativy (accessed: 05.10.2025).
29. Liability for Personal Data Processing: Changes in 2025 [Electronic resource] // Kontur. URL: https://kontur.ru/articles/55870-otvetstvennost_za_obrabotku_pers_dannyh (accessed: 05.10.2025).
30. Changes to the Law on Personal Data in 2025 [Electronic resource] // Qugo. URL: https://qugo.ru/blog/izmeneniya-zakona-o-personalnyh-dannyh-v-2025-godu (accessed on October 5, 2025).
31. New data protection rules from 2025: what you need to know [Electronic resource] // NeptunIT. URL: https://ntcneptunit.ru/blog/novye-pravila-zashchity-dannyh-2025 (accessed on October 5, 2025).
32. Tightening fines for personal data leaks: what has changed since May 30, 2025 [Electronic resource] // ER-Telecom. URL: https://r-soc.ertelecom.ru/announcements/article/33 (accessed on October 5, 2025).
33. Insider threats: how to protect the company from the inside? [Electronic resource] // INFARS. URL: https://infars.ru/blog/insayderskie-ugrozy-kak-zashchitit-kompaniyu-iznutri/ (date of access: 05.10.2025).
34. What Is User and Entity Behavior Analytics (UEBA)? [Electronic resource] // Microsoft. URL: https://www.microsoft.com/en-us/security/business/security-101/what-is-user-entity-behavior-analytics-ueba (date of access: 05.10.2025).
35. What is User Entity and Behavior Analytics (UEBA)? [Electronic resource] // Fortinet. URL: https://www.fortinet.com/resources/cyberglossary/what-is-ueba (date of access: 05.10.2025).
36. What is UEBA (User and Entity Behavior Analytics)? [Electronic resource] // Palo Alto Networks. URL: https://www.paloaltonetworks.com/cyberpedia/what-is-user-entity-behavior-analytics-ueba (date of access: 05.10.2025).
37. What is User and Entity Behavior Analytics (UEBA)? [Electronic resource] // CrowdStrike. URL: https://www.crowdstrike.com/en-us/cybersecurity-101/identity-protection/user-and-entity-behavior-analytics-ueba/ (date of access: 05.10.2025).

38. User and Entity Behavior Analytics (UEBA) [Electronic resource] // Check Point Software. URL: https://www.checkpoint.com/cyber-hub/threat-prevention/user-and-entity-behavior-analytics-ueba/ (Accessed: 05.10.2025).
39. What is User and Entity Behavior Analytics (UEBA)? [Electronic resource] // Rapid7. URL: https://www.rapid7.com/fundamentals/user-behavior-analytics/ (Accessed: 05.10.2025).
40. UEBA systems: what are they, market overview, comparative analysis... [Electronic resource] // xn--80aidjgwzd.xn--p1ai. URL: https://xn--80aidjgwzd.xn--p1ai/news/ueba_sistemy/ (Accessed: 05.10.2025).
41. What is a Honeypot? How are they used in cybersecurity [Electronic resource] // IB-BANK.ru. URL: https://ib-bank.ru/bisjournal/news/15637 (date of access: 05.10.2025).
42. What is a Honeypot? How Traps Serve Cybersecurity [Electronic resource] // Kaspersky. URL: https://www.kaspersky.ru/resource-center/threats/what-is-a-honeypot (date of access: 05.10.2025).
43. A Detailed Guide to Honeypots: How a Honeypot Works for Attackers [Electronic resource] // Glabit. URL: https://glabit.ru/blog/honeypot-guide (date of access: 05.10.2025).
44. A Detailed Guide to Honeypots [Electronic resource] // Habr. URL: https://habr.com/ru/companies/alexhost/articles/528796/ (accessed: 05.10.2025).
45. Honeypot Technology. Part 1: Honeypot Purpose [Electronic resource] // SecurityLab. URL: https://www.securitylab.ru/analytics/275420.php (accessed: 05.10.2025).
46. Improving Application Security Using the Principle of Least Privilege [Electronic resource] // Microsoft Learn. URL: https://learn.microsoft.com/ru-ru/entra/identity-platform/secure-least-privileged-access (accessed: 05.10.2025).
47. The Principle of Least Privilege. Cyberary [Electronic resource] // Sberbank. URL: https://www.sberbank.ru/ru/person/kibrary/vocabulary/princip-minimalnykh-privilegij (accessed: 05.10.2025).
48. What is Least Privilege Access? [Electronic resource] // Keeper Security. URL: https://www.keepersecurity.com/ru_RU/resources/glossary/what-is-least-privilege-access/ (accessed: 05.10.2025).
49. Understanding the Principle of Least Privilege in Microsoft Entra ID Governance [Electronic resource] // Microsoft Learn. URL: https://learn.microsoft.com/ru-ru/entra/id-governance/scenarios/least-privileged (accessed: 05.10.2025).
50. Principle of least privilege [Electronic resource] // Kaspersky Encyclopedia. URL: https://encyclopedia.kaspersky.ru/glossary/principle-of-least-privilege-polp/ (accessed: 05.10.2025).
51. Principle of least privilege [Electronic resource] // IBM Docs. URL: https://www.ibm.com/docs/ru/aix/7.1.0?topic=software-least-privilege (accessed: 05.10.2025).
52. What Is the Principle of Least Privilege? [Electronic resource] // Palo Alto Networks. URL: https://www.paloaltonetworks.com/cyberpedia/what-is-the-principle-of-least-privilege (date of access: 05.10.2025).
53. Federal Law of 27.07.2004 No. 79-FZ (as amended on 29.09.2025) "On the State Civil Service of the Russian Federation".
54. Collection of materials on the study of foreign experience in combating corruption [Electronic resource] // GOV.KZ. URL: https://www.gov.kz/memleket/entities/anticorruption/press/article/details/2281?lang=ru (date of access: 05.10.2025).
55. Rotation of Personnel in the Civil Service as a Measure to Prevent Corruption... [Electronic Resource] // Young Scientist. URL: https://moluch.ru/archive/443/96911 (date of access: 05.10.2025).
56. How to Fight Corruption Among Officials? One Option is Rotation [Electronic Resource] // Online. URL: https://people.onliner.by/2019/10/31/rotate (date of access: 05.10.2025).
57. First Federal University of Anti-Corruption Education: Training in the Field of Combating Corruption [Electronic Resource] // FUAP. URL: https://fuap.ru/ (date of access: 05.10.2025).
58. Model Programs in the Field of Combating Corruption: Training of Civil Servants [Electronic Resource] // FUAP. URL: https://fuap.ru/lib/antikorruptsionnoe-obuchenie/tipovye-programmy-v-oblasti-protivodeystviya-korruptsii-obuchenie-gossluzhashchikh/ (accessed: 05.10.2025).
59. Loyalty Program [Electronic resource] // Moscow Federation of Trade Unions. URL: https://mtuf.ru/loyalty-program/ (accessed: 05.10.2025).