УДК 004.056.5

СИСТЕМА ПРЕДОТВРАЩЕНИЯ ИНСАЙДЕРСКИХ УГРОЗ И УТЕЧКИ КЛЮЧЕВОЙ ИНФОРМАЦИИ В УСЛОВИЯХ ГИБРИДНОГО ФОРМАТА РАБОТЫ

Селезнева Е. Ю.

к.э.н., доцент,

Вятский государственный университет,

Киров, Россия

Рыжкова В. Р.

студент,

Вятский государственный университет,

Киров, Россия

Рычкова Н. А.

студент,

Вятский государственный университет,

Киров, Россия

Аннотация

В статье рассматривается система предотвращения инсайдерских угроз и утечек ключевой информации в условиях гибридного формата работы, который сочетает офисное и удаленное пребывание сотрудников. Анализируются актуальные риски, статистические данные о росте инцидентов, а также технологические и организационные меры защиты, включая модель Zero Trust, системы DLP, UEBA и SIEM. Предлагается комплексный подход к минимизации угроз. Исследование основано на данных Роскомнадзора и международных отчетах

за 2024–2025 годы, демонстрирующих снижение утечек при внедрении многоуровневой безопасности.

Ключевые слова: система предотвращения, инсайдерские угрозы, гибридный формат, Zero Trust, DLP, UEBA, SIEM, IAM, RBAC, мониторинг поведения, кибербезопасность.

INSIDER THREAT PREVENTION SYSTEM AND LEAKAGE OF KEY INFORMATION IN A HYBRID WORKING ENVIRONMENT

Selezneva E. Yu.
PhD in Economics, Associate Professor,
Vyatka State University,
Kirov, Russia

Ryzhkova V.R.
Student,
Vyatka State University,
Kirov, Russia

Rychkova N. A.
Student,
Vyatka State University,
Kirov, Russia

Abstract

The article discusses the system for preventing insider threats and key information leaks in a hybrid work format that combines office and remote work. It analyzes

current risks, statistical data on the growth of incidents, and technological and organizational security measures, including the Zero Trust model, DLP, UEBA, and SIEM systems. The article proposes a comprehensive approach to minimizing threats. The study is based on Roskomnadzor data and international reports for 2024-2025, which demonstrate a decrease in leaks when multi-level security is implemented.

Key words: prevention system, insider threats, hybrid format, Zero Trust, DLP, UEBA, SIEM, IAM, RBAC, behavior monitoring, and cybersecurity.

Ставший возможным в результате развития информационно-телекоммуникационных технологий (ИКТ) дистанционный формат занятости появился довольно давно. Еще в 2013 г. в российском законодательстве были закреплены особенности регулирования труда дистанционных работников.

При этом, гибридный формат работы, ставший нормой после пандемии, расширил периметр корпоративной безопасности, сделав организации уязвимыми к инсайдерским угрозам – действиям сотрудников, контрагентов или партнеров, приводящим к утечкам ключевой информации. Динамика численности удаленных работников представлена на рисунке 1.

Рисунке 1 – Динамика численности удаленных работников [8]

Дистанционный или гибридный режим более распространен в отраслях, где работа реже требует присутствия сотрудников на определенном рабочем месте для взаимодействия с клиентами и с производственным оборудованием, транспортом (Рис. 2).

Рисунок 2 – Структура удаленной работы по отраслям, % [8]

К концу 2023 года только 1,4% всех работников оставались полностью на удалённой форме работы. Но появился гибридный формат: часть недели -

дома, часть - в офисе. В 2025 году гибридная работа стала новой нормой, особенно в крупных городах и среди молодых специалистов. Более того, многие соискатели сейчас буквально требуют удалению работу или гибридный формат, и даже не рассматривают вакансии без подобного формата работы. Гибридная форма работы - станет стандартом для большинства офисных профессий.[9]

С января по неполный декабрь 2025 года работодатели разместили более 900 тысяч вакансий с возможностью удаленной работы. Это около 10% от общего объема предложений на рынке труда, который превысил 9,7 млн вакансий. За год доля удаленных вакансии выросла на 2 п.п. [10]

Проблемы удаленной/гибридной работы по утверждению аналитиков заключаются в следующем:

- 73% руководителей уверены, что удаленные сотрудники могут представлять большую угрозу для безопасности;
- 60% компаний используют программы для мониторинга удаленных сотрудников;
- три самые большие проблемы, связанные с удаленной работой: отдохнуть после работы (22%), одиночество (19%) и общение с людьми (17%);
- более 50% удаленных сотрудников не проходят подготовку по интернет-безопасности, хотя регулярно пользуются конфиденциальными данными своей компании и ряд других проблем личного характера. [11]

Так, в 2024 году инсайдерские инциденты составили 35% всех нарушений [1], с средними затратами свыше 15 млн долларов на случай, что обусловлено использованием личных устройств, незащищенных домашних сетей и снижением прямого контроля. В России Роскомнадзор зафиксировал 135 утечек баз данных с 710 млн записей в 2024 году, а в первой половине 2025 года

– 35 случаев с 39 млн записей, с тенденцией к снижению благодаря ужесточению ответственности [2].

Помимо этого, за 2024 год экспертно-аналитический центр InfoWatch зарегистрировал 778 инцидентов утечек информации ограниченного доступа в российских организациях (рис. 3).

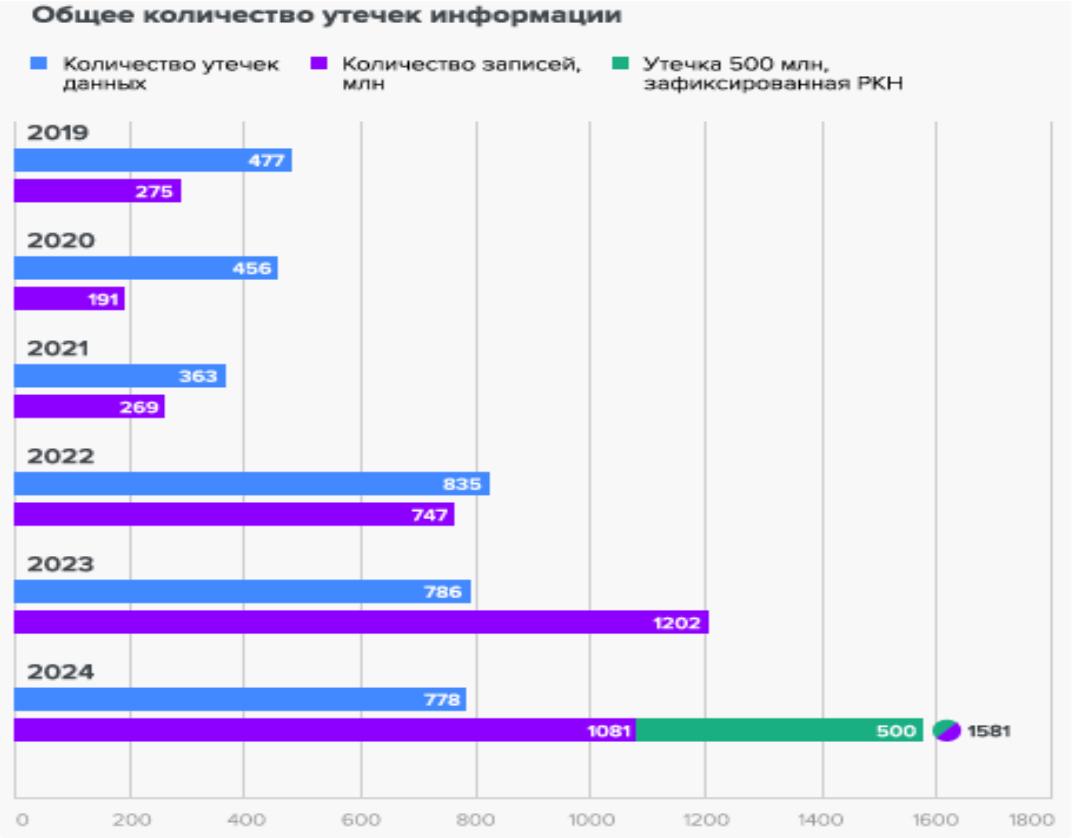

Рисунок 3 - Количество утечек информации и количество утекших записей персональных данных в России, 2019-2024 гг. [12]

В 2023 году было зафиксировано 786 инцидентов против 778 в 2024 (-8), то есть по сравнению с предыдущим периодом количество инцидентов практически не изменилось (сократилось на 1%). Отметим, что количество инцидентов, связанных с утечками данных в России, остается довольно стабильным третий год подряд после резкого увеличения в 2022 году. Ранее, в 2020-2021 годах, в разгар пандемии COVID-19, было зафиксировано снижение количе-

ства зарегистрированных инцидентов, что главным образом могло быть связано с высоким показателем сокрытия фактов утечек информации (латентностью) в тот период, а также с насыщением рынка данных на форумах в Дарквебе.

Распределение утечек информации по типам данных приведено на рисунке 4. Отметим, что произошло небольшое снижение доли персональных данных. Также снизился показатель утечек коммерческой тайны (с 7,7% до 6,0%). В то же время вырос процент зарегистрированных инцидентов, связанных с утечками государственной тайны (с 7,5% до 10,4%).

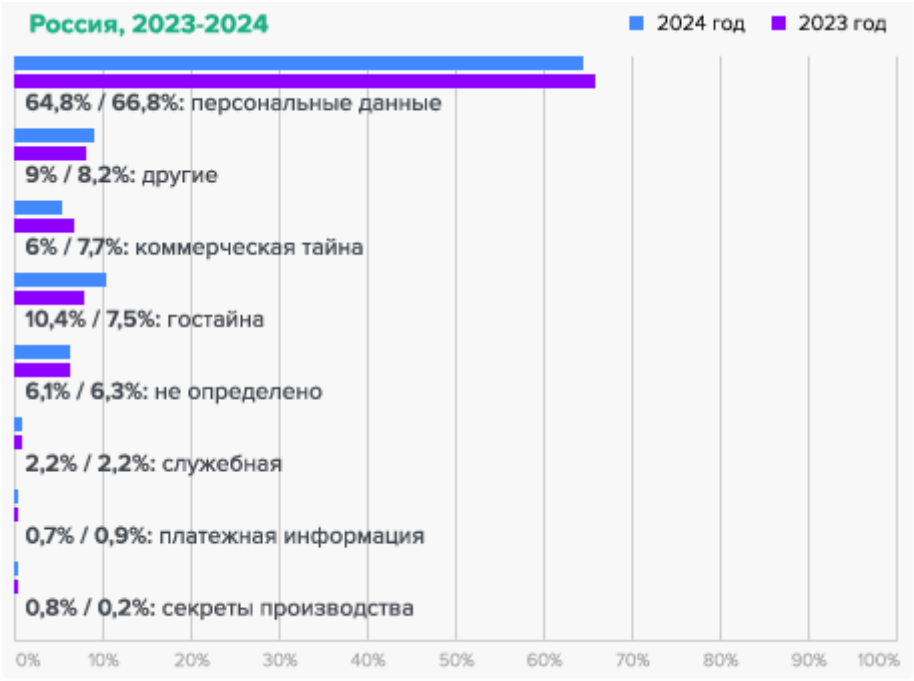

Рисунок 4 - Распределение утечек информации по типам скомпрометированных данных: Россия, 2023-2024 гг.[12]

В 2024 году доля утечек конфиденциальной информации, к которым привели кибератаки на российские организации, составила 70,1% (Рисунок 5). Почти каждое пятое нарушение стало следствием умышленных действий внутреннего нарушителя. Показатель незначительно вырос по сравнению с

предыдущим периодом. Доля нарушений в результате случайных действий персонала осталась на прежнем уровне (рис. 5).

Рисунок 5 - Распределение утечек информации по типам инцидентов: Россия, 2023-2024 гг. [12]

Также отдельно стоит отметить, что среди нарушений по вине сотрудников 95% инцидентов носят умышленный мотив (Рис. 6).

Рисунок 6 - Распределение утечек информации по умыслу: Россия, 2023-2024 гг. [12]

Картина утечек информации ограниченного доступа за прошедший год претерпела некоторые изменения. С одной стороны, сохраняется ландшафт

угроз на фоне СВО и все еще нарастающие риски со стороны киберпреступности. С другой стороны, наблюдается сдвиг в сторону роста количества нарушений со стороны персонала организаций (в том числе, руководства), который подтверждается как собранными за прошедший год данными, так и рядом проведенных опросов и исследований. Большинство руководителей, а также ИБ и ИТ специалистов видят основную угрозу информационным активам компании в умышленных и неумышленных действиях работников. Также мы все чаще можем наблюдать гибридные инциденты — кибератаки, совершенные на основе данных, полученных изнутри организации.

По данным компании «Еса Про», в 2025 году 73% всех утечек данных из российских организаций пришлось на госсектор — за отчётный период было слито более 105 млн строк данных с записями о пользователях и компаниях. На втором месте — ритейл (19%), на третьем — сфера услуг (6,5%). Всего за год утекло более 145 млн строк. [13]

По информации компании F6, в 2025 году зафиксировали около 225 крупных утечек данных российских компаний, суммарно затронувших более 767 млн строк. Среди отраслей, подвергшихся наибольшему риску взломов, выделяются ретейл, сфера здравоохранения, государственные службы и информационные технологии.[14]

Эти данные подчеркивают необходимость системного подхода к предотвращению угроз, сочетающего технологии анализа поведения, принцип нулевого доверия и повышение осведомленности персонала в условиях размытых границ между работой и домом.

Система предотвращения инсайдерских угроз в гибридной модели строится на многоуровневом подходе, где каждый слой усиливает предыдущий,

создавая непроницаемый барьер против рисков. Специфика угроз усугубляется в трех категориях (таблица 1), но превентивные меры нейтрализуют их эффективно.

Гибридная модель не создает принципиально новых типов угроз, но катализирует риски по каждому из существующих категорий, расширяя поверхность атаки и усложняя задачи по обнаружению аномалий. Это требует адаптации системы защиты, смещая её фокус с контроля сетевого периметра на непрерывную проверку доверия к пользователю, устройству, сессии и контексту действия.

Таблица 1 - Специфика инсайдерских угроз в условиях гибридного формата работы [3]

Категория инсайдера	**Ключевые факторы риска в гибридной модели**	**Примеры инцидентов**
Небрежный инсайдер (Непреднамеренная утечка)	Работа в незащищенных публичных и домашних сетях (Wi-Fi). Использование неподконтрольных ИБ-службе личных устройств (BYOD) с устаревшим ПО. Смешение личных и рабочих цифровых пространств (учетные записи, мессенджеры). Повышенная отвлекаемость и менее формальная обстановка домашнего офиса.	Отправка конфиденциального документа на личный email для «удобства работы». Потеря или кража незашифрованного личного ноутбука с рабочими файлами. Сохранение файлов в публичное облачное хранилище (Google Диск, Яндекс.Диск). Утечка информации через плечо в коворкинге или кафе.
Злонамеренный инсайдер (Умышленный вред)	Отсутствие физического наблюдения и непосредственного контроля со стороны коллег. Использование неподотчетных личных каналов связи и устройств для вывода данных. Сложность разграничения легитимных действий и злонамеренной активности в распределенной среде. Возможность действовать в нерабочее время с домашней сети.	Планомерное копирование баз данных или интеллектуальной собственности на личный носитель. Использование шифрованных личных мессенджеров для передачи информации третьим лицам. Установка на личный компьютер скрытого ПО для перехвата данных. Саботаж или порча данных в системах, доступных удаленно.
Скомпрометированный инсайдер (Учетные данные	Повышенная уязвимость к фишингу и социальной инженерии через неформальные каналы.	Кража учетных данных через фишинговое письмо, имитирующее корпоративный сервис, на личную почту. Перехват

под контролем злоумышленника)	Сложность отслеживания аномального поведения из-за разнообразия мест доступа. Использование слабых методов аутентификации (только логин/пароль). Отсутствие сегментации доступа по принципу «что необходимо для работы».	учетных данных при работе через публичный Wi-Fi. Внедрение вредоносного ПО на личное устройство сотрудника для кражи сессий доступа (кейлоггер). Доступ злоумышленника к корпоративным системам «под видом» сотрудника из нехарактерного региона.

Для перехода к реализации такой системы предотвращения ключевую роль играет модель Zero Trust [4], революционная концепция, отвергающая традиционное слепое доверие внутри корпоративной сети и требующая непрерывной верификации каждого пользователя, устройства и запроса независимо от их расположения – будь то офис, дом или общественное место. Эта парадигма "никогда не доверяй, всегда проверяй" разрушает периметр безопасности, заменяя его динамической защитой, идеально подходящей для гибридных условий, где границы размываются.

Архитектура системы должна включать следующие взаимосвязанные компоненты.

Первый уровень – контроль доступа через системы IAM (Identity and Access Management) и RBAC (Role-Based Access Control), где применение многофакторной аутентификации и строгого принципа минимальных привилегий блокирует до 99,9% автоматизированных атак, ограничивая доступ сотрудников только теми ресурсами, которые необходимы для выполнения их ролей в конкретный момент времени, независимо от того, работают ли они из офиса или дома [5]. Это особенно важно в гибридных условиях, когда учетные записи могут быть скомпрометированы через фишинг, а динамическая сегментация сети по Zero Trust предотвращает латеральное перемещение злоумышленников внутри инфраструктуры, минимизируя ущерб от инсайдеров.

Второй уровень составляют DLP-системы (Data Loss Prevention), которые осуществляют непрерывный мониторинг трафика, фильтрацию электронной почты, мессенджеров и баз данных, выявляя и блокируя инсайдерские действия в реальном времени – от попыток копирования конфиденциальных файлов на USB-носители до передачи данных через облачные сервисы или личные аккаунты [6]. В гибридном формате эти системы интегрируются с контекстным анализом, распознавая паттерны поведения, такие как необычные объемы скачиваний в нерабочее время.

Третий уровень – мониторинг и аудит с использованием UEBA, EDR-инструментов (Endpoint Detection and Response) и обязательного VPN для всех удаленных подключений, обеспечивающих полную видимость конечных точек вне корпоративного периметра. Непрерывный анализ поведения выявляет отклонения, такие как аномальные логины из новых геолокаций или доступ к нехарактерным файлам, а SIEM-платформы коррелируют события из разнородных источников, позволяя оперативно реагировать на угрозы до их реализации [7].

Четвертый уровень – организационные меры в виде регулярных тренингов по кибербезопасности и разработки строгих политик удаленного доступа, которые снижают неумышленные угрозы на 40–50% за счет повышения осведомленности сотрудников о рисках фишинга, безопасном использовании личных устройств и соблюдении протоколов. Обучение включает симуляции атак и разбор реальных кейсов, а политики фиксируют правила сегментации работы и дома, балансируя доверие с контролем и способствуя общей культуре безопасности в гибридных командах.

Комплексная многоуровневая система предотвращения на базе IAM, DLP, мониторинга, аудита и обучения интегрируется с Zero Trust, UEBA и SIEM, обеспечивая проактивную защиту от инсайдерских угроз в гибриде и

снижая риски. Статистика 2024–2025 годов подтверждает ее эффективность. Будущее – ИИ-усиление для полной адаптации под вызовы гибридной работы.

Библиографический список

1. Более 80% компаний борются с инсайдерами / Компьютерра [Электронный ресурс] // Компьютерра : [сайт]. — URL: https://www.computerra.ru/309947/bolee-80-kompanij-boryutsya-s-insajderami/
2. Роскомнадзор зафиксировал более 710 миллионов утекших записей о россиянах // РИА Новости. — 2025. — 16 янв. — URL: https://ria.ru/20250116/roskomnadzor-1993941562.html
3. Концептуальное моделирование инсайдерской деятельности в системах информационной безопасности / В. А. Минаев, Б. Н. Коробец, Е. В. Вайц, Ю. И. Стрельников // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. – 2018. – № 3. – С. 139-145. – DOI 10.25586/RNU.V9187.18.09.P.139. – EDN YBJHSH.
4. Solar Dozor Концепция нулевого доверия (Zero Trust): суть и принципы работы / Solar Dozor [Электронный ресурс] // Солар : [сайт]. — URL: https://rt-solar.ru/products/solar_dozor/blog/3824/
5. Новая модель работы: как защитить гибридное рабочее место / [Электронный ресурс] // ESET : [сайт]. — URL: https://www.eset.com/ua-ru/about/newsroom/blog/business-security/novaya-model-raboty-kak-zashchitit-gibridnoye-rabocheye-mesto-ru/
6. Антон Дятлов Что такое DLP-система и как она работает / Антон Дятлов [Электронный ресурс] // Академия Selectel : [сайт]. — URL: https://selectel.ru/blog/data-loss-prevention/
7. Infars. Инсайдерские угрозы: как защитить компанию изнутри? 2024. URL: https://infars.ru/blog/insayderskie-ugrozy-kak-zashchitit-kompaniyu-iznutri/

8. Удаленная занятость в России https://issek.hse.ru/news/976040462.html?ysclid=mjiz4myxva648075968

9. Сколько россиян работают удалённо в 2025 году? | Следи за цифрой | Дзен https://dzen.ru/a/aCMNSzdmzT1mSY98?ysclid=mjizflbkqy62565961

10. Доля вакансий с удаленной работой в России выросла до 10% в 2025 году https://www.kommersant.ru/doc/8295770?ysclid=mjiz3x1o63480501796

11. Статистика удаленной работы в мире (2025) https://inclient.ru/remote-work-stats/?ysclid=mjiz6m1u1r925844732

12. Россия: утечки информации ограниченного доступа 2023-2024 https://www.infowatch.ru/sites/default/files/analytics/files/rossiya-utechki-informatsii-ogranichennogo-dostupa-2023-2024.pdf?ysclid=mjizk6k0yi39313090

13. Хакеры власть не признают Утечки данных в России в 2025 году: госсектор лидирует по числу инцидентов https://www.kommersant.ru/doc/8313330

14. В 2025 году зафиксировали 225 крупных утечек данных российских компаний https://tass.ru/obschestvo/25921515