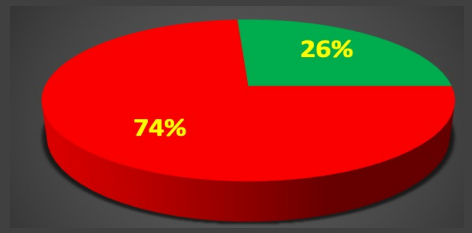
Интеграция поведенческих и психологических факторов в управлении инсайдерскими рисками

Ларин Сергей Павлович
Рафальская Елена Александровна

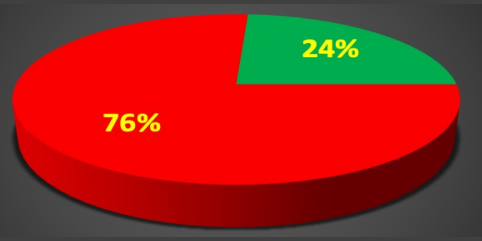
Актуальность и масштаб инсайдерского риска

В 2025 году Verizon проанализировала 22 052 эпизода, связанных с информационными инцидентами. Из этого числа 12 195 случаев сопровождались фактической утратой конфиденциальной информации. Исследование охватило инциденты в 139 странах



Из всех зарегистрированных нарушений безопасности 74% - человеческий фактор

76% современных организаций ежегодно сталкиваются как минимум с одним деструктивным инцидентом с участием внутреннего нарушителя.

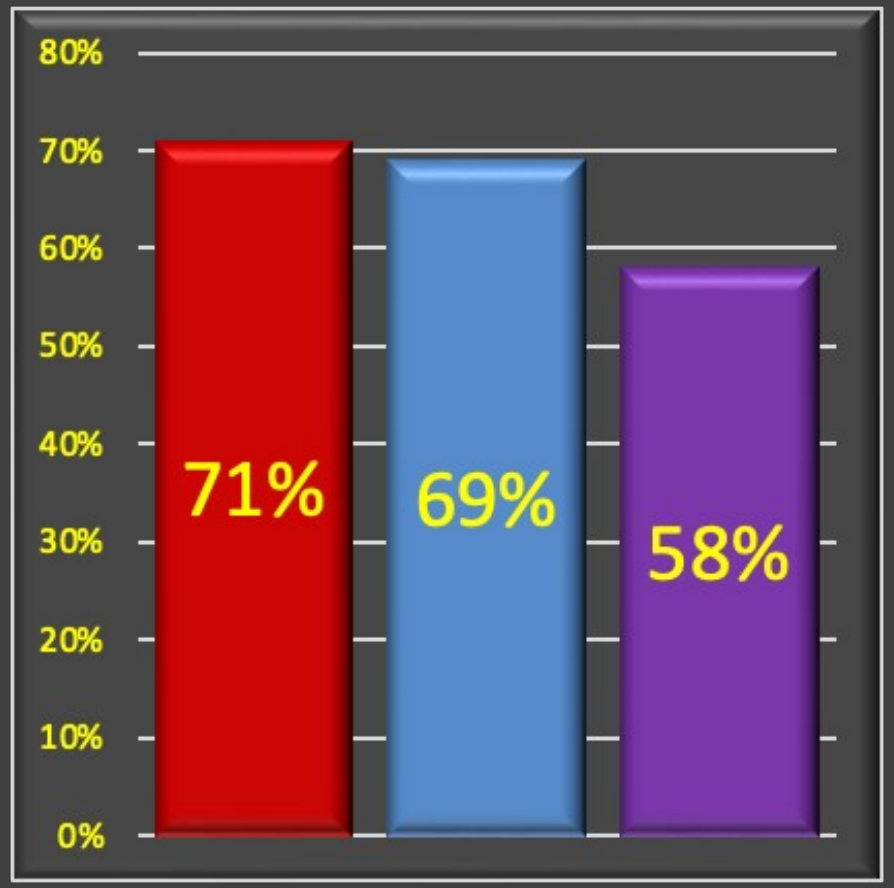


Средний экономический ущерб от ликвидации последствий одной атаки достигает — 17,4 млн долларов

Инсайдерский риск имеет одновременно высокий масштаб, высокую стоимость и выраженный человеческий компонент.

Источник: исходный материал пользователя; показатели приведены без независимой верификации.

Барьеры препятствующие внедрению эффективных программ управления инсайдерскими рисками



Недостаточность или технологическое несовершенство существующих инструментов мониторинга (71%);

Жесткие бюджетные ограничения организаций (69%);

Этические и правовые проблемы обеспечения конфиденциальности сотрудников (58%)

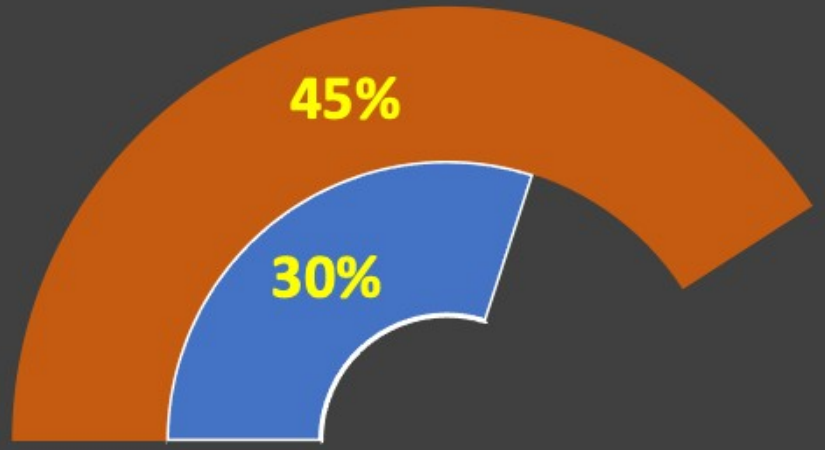
Отчет Cybersecurity Insiders за 2025 г

Ограничения традиционных систем (DLP/SIEM)

Реактивный подход

- Фиксация инцидента в момент совершения или постфактум.
- Опора на технические индикаторы, которые обеспечивают менее 30% полноты обнаружения рисков.
- Неспособность выявлять намерения до их реализации.

Потенциал превентивного анализа



- Технические индикаторы обеспечивают **не более 30% полноты обнаружения угроз**. Они видят лишь техническое следствие, но полностью игнорируют причину.
- Поведенческие и психологические факторы позволяют выявить **до 45% инсайдерских рисков на самых ранних, латентных стадиях**, когда умысел нарушителя только зарождается.

Анализ CPNI (Великобритания) показывает, что личные стрессоры являются триггером разглашения в 45% случаев.

«Риски нужно выявлять до того, как они станут инцидентами» — Ф. Грейтцер.

Концепция целостного анализа «Whole-Person Analysis»

Парадигма анализа

• Деструктивное проявление сотрудника рассматривается не как случайный изолированный сбой, а как финал длительного процесса.
• Система учитывает синергетический эффект как внешних (организационных), так и внутренних (психологических) факторов.
• Цель подхода — перенос точки обнаружения угрозы на этап до совершения реального ущерба («left of boom»).

Примеры систем оценки и управления инсайдерскими рисками:

SOFIT

Иерархическая концепция из более чем 300 индивидуальных и средовых факторов риска.

Модель BRIM (2025)

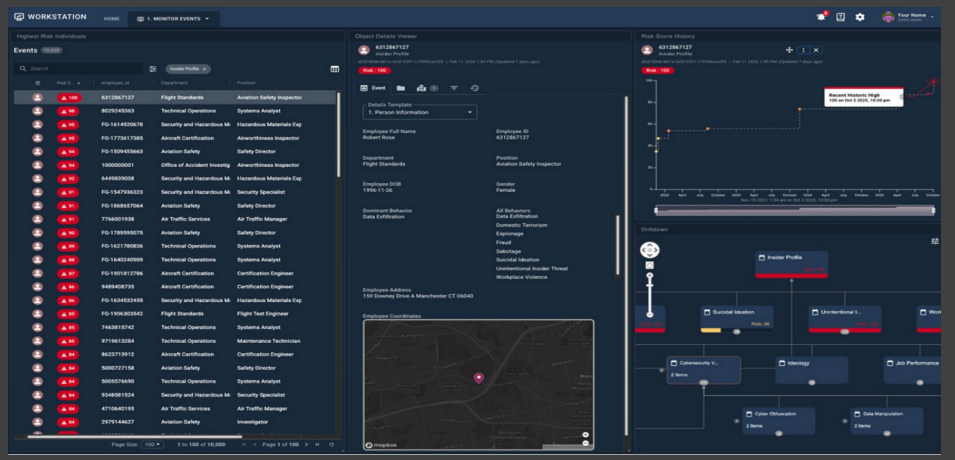
Математически верифицированные скрытые когнитивные индикаторы и триггеры характера.

АРХИТЕКТУРА И МАСШТАБ БАЗЫ ЗНАНИЙ SOFIT

Модель оцифровывает причинно-следственные связи инсайдерской активности, увязывая дефекты корпоративной среды с психологическим профилем сотрудника и его цифровым следом в инфраструктуре.

ОБЩЕЕ ЧИСЛО ПОКАЗАТЕЛЕЙ: более 320

Точность обнаружения скрытых взаимосвязей на этапе зарождения умысла достигает 92–97%



ИНДИВИДУАЛЬНЫЕ (ЧЕЛОВЕЧЕСКИЕ) ФАКТОРЫ

включает в себя 271 показателей в 4-х категориях

Психоэмоциональный статус

Фиксация скрытых обид, выгорания, резких флуктуаций настроения, признаков профессиональной деградации или депрессивных состояний.

Коммуникативные маркеры

Вербальные индикаторы выраженного недовольства, агрессии или цинизма, выявляемые методами ИИ в корпоративных переписках.

Поведенческие девиации

Резкие нелинейные изменения повседневных паттернов поведения, спады продуктивности и регулярные нарушения рабочих регламентов.

ИТ-аномалии взаимодействия

Непосредственные цифровые отклонения: аномальные поисковые запросы, нетипичное время активности и подготовка данных.

ОРГАНИЗАЦИОННЫЕ ФАКТОРЫ УЯЗВИМОСТИ СРЕДЫ

включает в себя 49 показателей в 3-х категориях

Управленческие дефекты

Оцифровка деструктивных стилей менеджмента со стороны руководства, проявления несправедливости при кадровых решениях и отсутствие обратной связи.

HR-сбои и перегрузки

Мониторинг общего уровня выгорания внутри подразделений, систематических перегрузок сотрудников и отсутствия институциональной психологической поддержки.

Дефекты политик безопасности

Сбои в регламентах ИБ, наличие избыточных прав доступа, непрозрачные правила контроля и организационные лазейки в бизнес-логике.

ЦИФРОВОЙ ПРОФИЛЬ «ТЕМНОЙ ТРИАДЫ» В МОДЕЛИ BRIM (2025)

- Разработана исследователями Оху и Джонсом в 2025 году.
- Фокусируется на латентных когнитивных индикаторах и аверсивных чертах характера.

74% корреляции с рисками:
Субклинические черты «Темной триады» (нарциссизм, макиавеллизм, психопатия).

68% корреляции с рисками:
«Цифровое поведение» — целенаправленный поиск сотрудником компромата или оправданий для будущего деструктивного умысла.

МАКИАВЕЛЛИЗМ

Циничный прагматизм и расчет

- Использование вымышленных учетных записей (фиктивных ID).
- Целенаправленный поиск лазеек и уязвимостей в DLP-системах.
- Хладнокровный обход ИБ-регламентов ради личной выгоды без проявления эмоций.

НАРЦИССИЗМ

Завышенное эго и дефицит эмпатии

- Убежденность в собственной исключительности: «правила ИБ написаны не для меня».
- Острая враждебность и жажда мести при малейших стрессорах (критика, отказ в повышении).
- Когнитивная легитимизация ущерба компании.

ПСИХОПАТИЯ

Импульсивность и безжалостность

- Тотальное отсутствие страха перед наказанием или последствиями.
- Импульсивные, спонтанные акты сабатажа ИТ-инфраструктуры.
- Агрессивное поведение в корпоративных чатах (онлайн-хейтинг, сталкинг).

Интеграция поведенческой психологии, нейрофизиологии и искусственного интеллекта для перехода от фиксации нарушений к упреждающей тактике

1. Психология

Выявление психологических индикаторов для раннего выявления рисков.

Певеденческие

Фиксация изменений в поведении: резкий рост недовольства, конфликты с руководством, частые отгулы, работа в неурочное время.

Психологические

Отслеживание цепочки: Личностные особенности → Провоцирующий фактор → Психологическая декомпенсация → Поведенческие маркеры → Техническое действие.

Психолингвистические

Анализ тональности коммуникаций (email, мессенджеры) на предмет выявления выгорания, обиды, агрессии или финансового стресса.

2. Нейрофизиология и биометрия

Изучение паттернов взаимодействия с техникой и фиксация измененных состояний.

Взаимодействие с техникой

Анализ паттернов кинематики мыши, динамики нажатия клавиш и задержек ввода. Позволяет выявить измененное психоэмоциональное состояние (стресс, опьянение, крайнюю степень усталости).

Айтрекинг и микромимика

Фиксация движений глаз и микровыражений лица при прохождении сотрудниками регулярных комплаенс-процедур и специализированных тестов.

3. Экспертный ИИ

Связующий элемент для профилирования и снижения ложных срабатываний.

Профилирование базовой линии

ИИ строит индивидуальный профиль «нормального» поведения сотрудника и в реальном времени фиксирует любые аномалии.

Снижение ложных срабатываний

Сопоставление технического триггера (скачивание базы данных) с поведенческим контекстом (сотрудник находится в процессе увольнения или высказывал недовольство).

КОГНИТИВНАЯ ВОЙНА И ИНСАЙДЕРСКИЕ РИСКИ

Концепция «Когнитивной декогеренции»

Современная когнитивная война — это борьба не за саму информацию, а за структуры ее интерпретации и принятия решений.
Стратегический инструмент удара —целенаправленное разрушение «системных инвариантов» — базовых ментальных опор, обеспечивающих связность, когерентность и адаптивность человека в социотехнической системе (когнитивная декогеренция)

Фаза 1: Когнитивное истощение

Информационный перегруз и хронический стресс размывают эпистемические фильтры восприятия информации.

Фаза 2: Ценностный сдвиг

Утрата институционального доверия и обрыв связи с коллективом («Я» отделяется от «Мы — компания»).

Фаза 3: Телеологический обрыв

Фиксация точки невозврата.
Исчезновение будущего в системе запускает активный деструктивный паттерн.

Инсайдер рождается не в момент клика, а в момент невидимого распада внутренних ментальных опор личности.

Матрица деструкции: от инварианта к инсайдеру

Системный инвариант	Проявление когнитивной декогеренции (Риск инсайдера)	Паттерн инсайдера
1. Эпистемические структуры (Стандарты истины)	Сотрудник перестает верить официальным каналам компании. Подвержен конспирологии, дезинформации, внешнему манипулированию.	Модель BRIM: «цифровое поведение в поисках подтверждения» (поиск альтернативных, деструктивных трактовок событий в сети).
2. Аксиологические иерархии (Ранжирование ценностей)	Смещение ценностей. Корпоративная безопасность и лояльность падают в приоритете. На первое место выходят личная выгода (жажда денег) или месть.	Резкие изменения в паттернах общения, лингвистические маркеры цинизма, фиксация черт «Темной триады» в коммуникациях.
3. Конструкты идентичности (Принадлежность к группе)	Отчуждение. Сотрудник больше не идентифицирует себя с командой («Я им чужой», «Меня не ценят»). Переход в позицию «Мы против Них».	Снижение социальной активности в корпоративных мессенджерах, изоляция, рост конфликтных/токсичных взаимодействий.
4. Архитектуры доверия (Доверие к лидерам и процедурам)	Полный крах доверия к руководству, HR и ИБ-политикам. Правила компании воспринимаются как враждебные.	Демонстративное или скрытое нарушение регламентов ИБ, поиск уязвимостей в ИТ-системах, обход ограничений (DLP).
5. Телеологические проекции (Картина будущего)	Потеря видения своего будущего в компании (выгорание, понимание неизбежного увольнения или сокращения).	Аномальное падение продуктивности, поиск вакансий с рабочего места, массовое копирование «портфолио» или баз данных перед уходом.

Заключение

Обеспечение информационной безопасности современной организации сегодня невозможно без глубокого понимания и интеграции человеческого фактора в контур защиты.

Использование научных подходов, объединяющих поведенческие науки, нейрофизиологию и экспертные ИИ-системы, позволяет успешно перевести IRM из реактивной плоскости наказания в проактивную плоскость превентивного предотвращения.

Использование передовых моделей машинного обучения для анализа бесконтактной биометрии и цифровых паттернов успешно разрешает фундаментальное противоречие между необходимостью глубокого мониторинга рисков и соблюдением права сотрудников на конфиденциальность. Внедрение такого комплексного подхода — это безальтернативный шаг для перехода к реальной киберустойчивости социотехнических систем.

Спасибо за внимание!