индид × Айдентити Клуб

Identity Security 2026:

Кто и как управляет доступом в российских компаниях

Исследование российского рынка защиты учетных данных и управления доступом

Индид

Индид — российский разработчик комплекса решений в области защиты айдентити. Продукты Индид уже более 17 лет внедряют крупнейшие компании из России и СНГ, работающие во всех отраслях экономики. Программное обеспечение Индид включено в реестр Минцифры (реестр российского ПО, ранее — реестр Минкомсвязи), подходит для выполнения требований программы импортозамещения, принятой в РФ. Также помогает соблюдать положения различных нормативно-правовых актов в сфере информационной безопасности (государственных стандартов, постановлений ФСТЭК и других подобных документов). Индид самостоятельно разрабатывает все свои продукты на территории Российской Федерации.

Айдентити Клуб

Единственное в России профессиональное сообщество экспертов в области Identity Security. Участники Клуба на постоянной основе обмениваются практическим опытом, обсуждают изменения рынка и технологий и совместно формируют новые подходы к защите айдентити.

Содержание отчета

Задачи и методология исследования	04
Рынок Identity Security: ключевые факты	06
PAM	12
IDM/IGA	23
MFA/SSO/IAM	37
Контроль ИИ-агентов	50
Организация процесса управления доступом	57
Главное об Identity Security в 15 цифрах	73

Описание исследования

Задачи и методология

200 респондентов и 21 интервью

Задачи исследования

Сформировать целостную картину российского рынка Identity Security: оценить его объем и структуру, понять, как компании на практике управляют доступом и насколько зрелы их процессы. Отдельно — какие инциденты с учетными записями переживают организации, что мешает внедрять решения и от чего зависит их выбор.

Как оценивали рынок

Расчеты «сверху вниз» и «снизу вверх»: открытая отчетность, закупки, данные интеграторов, кейсы и поисковый спрос. Оценки сопоставлены, скорректированы на наценку посредников и проверены в интервью с вендорами. Объем рынка — в денежном выражении за 2025 год.

Как проводили исследование

Количественный этап

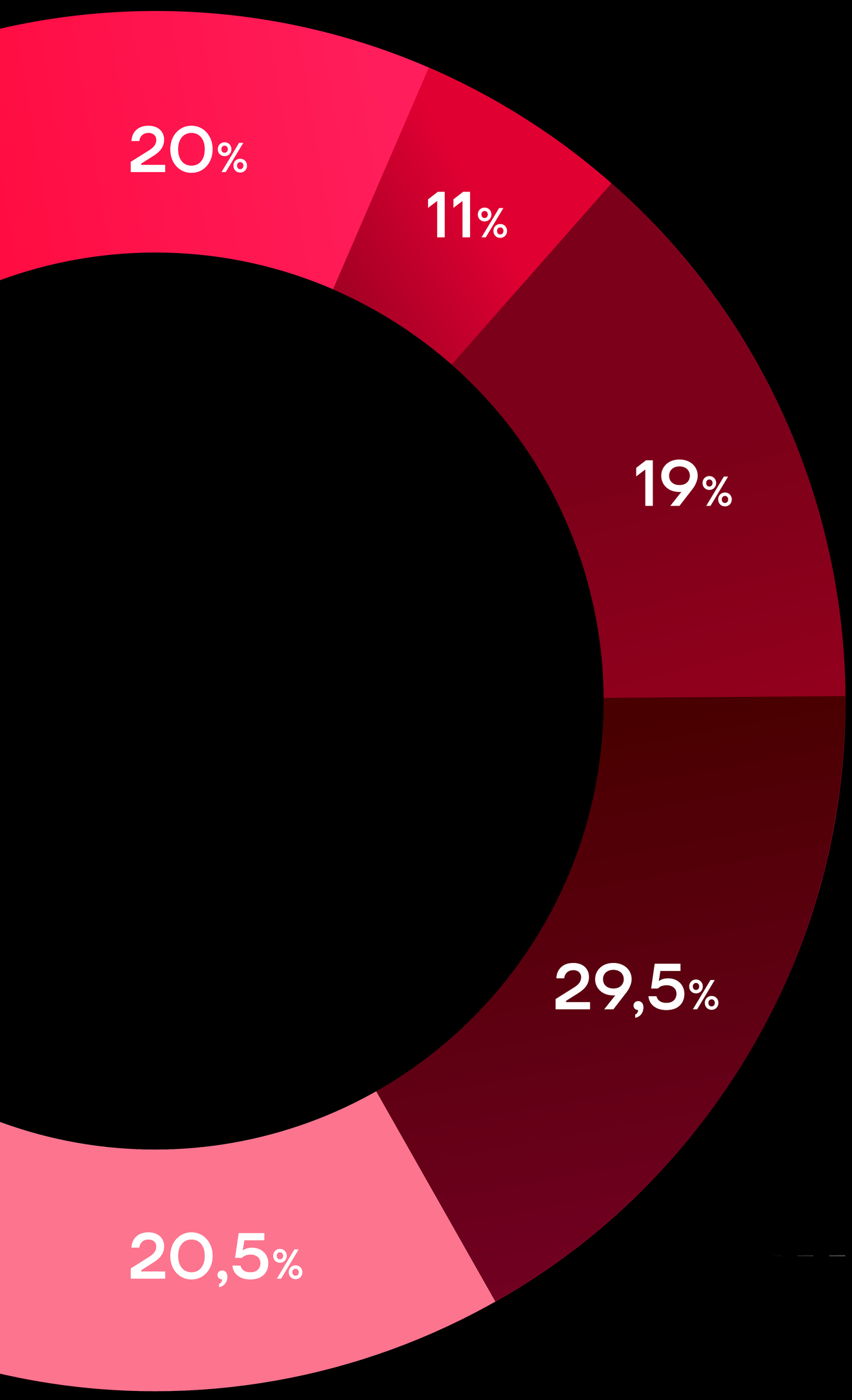
В исследовании приняли участие 200 респондентов из 200 организаций со штатом от 100 сотрудников, включая крупнейшие российские и международные компании с численностью более 10 000 человек. Участники имели опыт работы с управлением доступом, а их компании использовали хотя бы одно решение Identity Security.

Качественный этап

Проведено 21 глубинное интервью: 11 — с компаниями-эксплуатантами (шесть экспертов открыто, пять CISO анонимно) и 10 — с российскими вендорами.

Портрет выборки

11 отраслей: финансы, государственное управление, ритейл и торговля, телеком-услуги и связь, энергетика, обрабатывающая промышленность, разработка ПО и ИТ-услуги, логистика и транспорт, строительство, добывающая промышленность, здравоохранение.



Размер компаний

Число сотрудников

Более 10 000

3001-10 000

1001-3000

251-1000

101-250

Профиль респондентов

48% Информационные технологии

36% Информационная безопасность

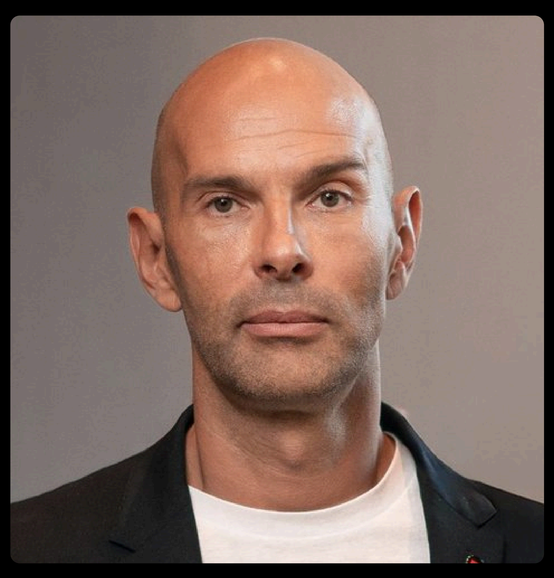
11% Управление персоналом

5% Генеральное руководство

Рынок Identity Security: ключевые факты

17 млрд ₽

российский рынок
Identity Security в 2025 году



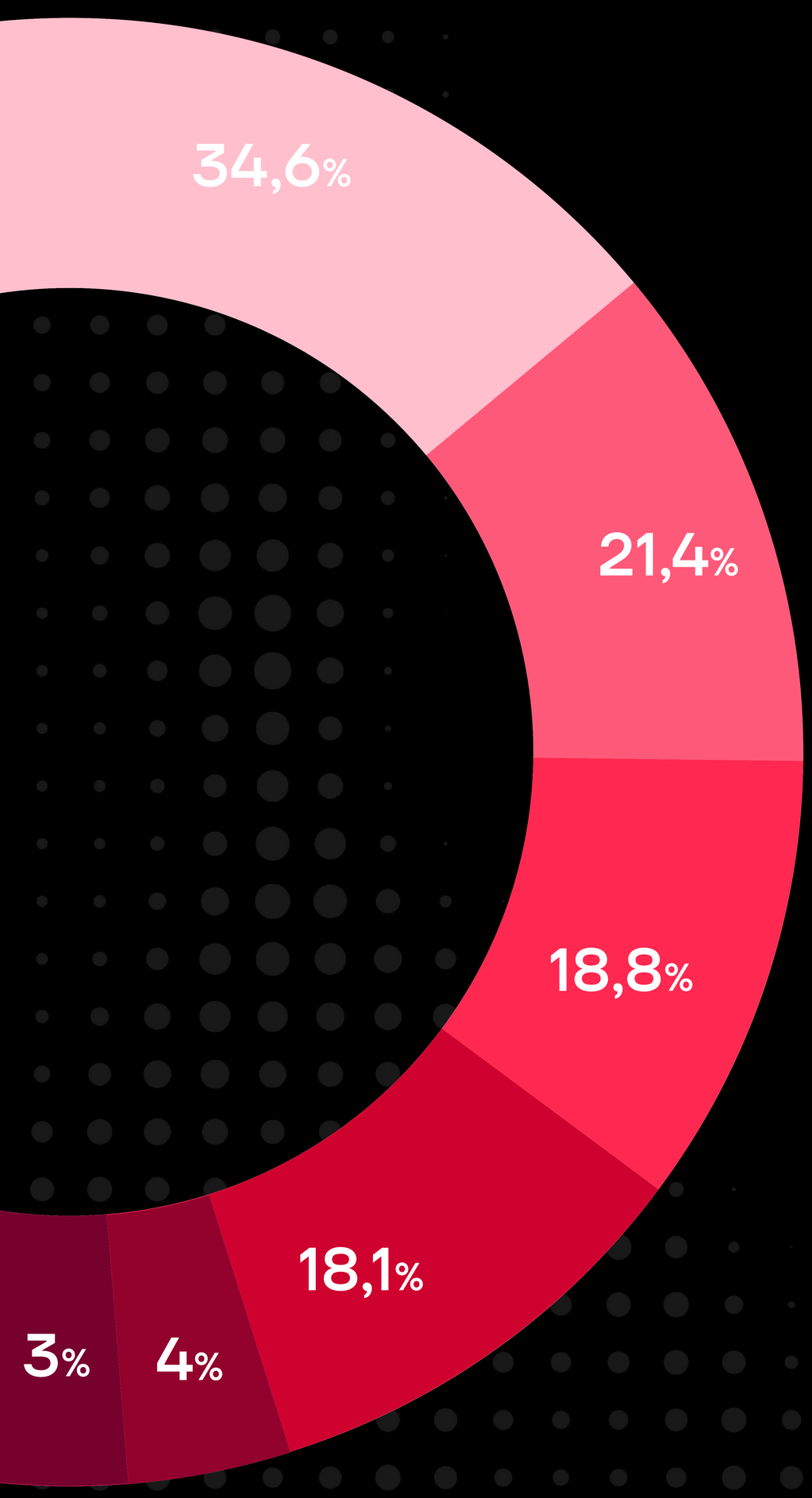
Identity Security — относительно молодое направление в сегменте информационной безопасности, которое сейчас проходит этап активного формирования.

При этом рынок защиты айдентити быстро меняется: растет число цифровых идентичностей, усложняются инфраструктуры, появляются новые сценарии доступа и новые требования к их защите. Чтобы принимать взвешенные решения, компаниям недостаточно ориентироваться только на отдельные технологии — нужно понимать общую динамику рынка, реальные практики и уровень зрелости организаций. Исследование помогает увидеть эту картину целиком: какие инструменты уже стали стандартом, где сохраняются барьеры и в каких направлениях этот сегмент будет развиваться в ближайшие годы. Такая оценка дает возможность понять, куда движется рынок, какие изменения уже становятся системными и принимать решения с учетом реальной динамики отрасли.

Алексей Баранов,
Генеральный директор Индид

34,6%

рынка приходится на PAM — крупнейший сегмент Identity Security



PAM
5,8 млрд ₽ (34,6%)

IdM/IGA
3,6 млрд ₽ (21,4%)

Службы каталогов
3,2 млрд ₽ (18,8%)

MFA/SSO/IAM
3,1 млрд ₽ (18,1%)

CMS/PKI
0,7 млрд ₽ (4%)

Корпоративные менеджеры паролей
0,5 млрд ₽ (3%)

Какие инструменты безопасности учетных записей и контроля прав доступа используются в организации?*

69,5% Двухфакторная аутентификация (2FA/MFA)

48% Система управления цифровыми сертификатами (CMS/PKI)

45% Технология единого входа (SSO)

42,5% Корпоративный менеджер паролей

42% Система управления привилегированным доступом (PAM)***

35% Система управления жизненным циклом учетных записей (IdM/IGA)**

34% Служба каталогов, отличная от Microsoft AD

69,5%

компаний используют MFA — самый распространенный инструмент Identity Security

Двухфакторная аутентификация – инструмент безопасности айдентити с наибольшим проникновением

* Сумма превышает 100%, так как респонденты могли выбрать несколько вариантов ответа.
** К IdM/IGA системам пользователи могли относить самописные системы и скрипты для автоматизации управления учетными записями.
*** PAM применяется не только для контроля администраторов, поэтому доля выше, чем на странице 17 (36,5%).

Службы каталогов

34%

компаний используют службы каталогов, отличные от Microsoft AD

Это третий по объему сегмент рынка:
3,2 млрд ₽, или 18,8%. Каждая третья компания уже работает со службой каталогов, отличной от Microsoft AD, — импортозамещение затронуло и базовый слой идентификации.

87,5% организаций сталкивались с инцидентами вокруг учетных записей

Статистика инцидентов Identity Security*

Ошибки администраторов при ручном назначении прав, приведшие к временному доступу посторонних лиц к конфиденциальным данным	43,5%
Действия сотрудников, находящихся в отпуске или на длительном больничном, совершенные вопреки политикам безопасности	39%
Компрометация привилегированных/ административных учетных записей	35,5%
Несанкционированная активность технических или сервисных учетных записей, владельцев которых трудно установить	35,5%
Успешные атаки методами социальной инженерии (фишинг, передача паролей третьим лицам, открытие вредоносных ссылок)	34%
Доступ в системы со стороны уже уволенных сотрудников	33,5%
Использование скомпрометированных учетных записей, полученных злоумышленниками из-за отсутствия MFA	25,5%
Нарушение принципа разделения полномочий (SoD), повлекшее за собой финансовые или операционные риски	22,5%
Несанкционированные действия внешних подрядчиков в доверенном контуре организации	22%
Не было проблем, связанных с эксплуатацией учетных записей и прав доступа	12,5%

Главный источник инцидентов — ручные операции: ошибки администраторов при выдаче прав (43,5%).
Новый тренд — в топ-4 вошла несанкционированная активность сервисных учетных записей (35,5%).

* Сумма превышает 100%, так как респонденты могли выбрать несколько вариантов ответа.

Сегмент

PAM

Рынок PAM сегодня

34,6%

крупнейший сегмент рынка
+13% за год

5,8

млрд ₽
размер рынка
в 2025 году

13%

темп роста рынка в 2025 году
по отношению к 2024 году
(в денежном выражении)

~350

проектов было выполнено в 2025 году (из них ~260 — у топ-2 вендоров)

Топ-3

вендоров по выручке от продажи лицензий и техподдержки:

- Индид (Indeed PAM)
- АйТи Бастион (СКДПУ-НТ)
- ГК «Солар» (Solar SafeInspect)

Покупательские тренды

Снижение порога входа для среднего бизнеса за счет упрощения архитектуры PAM

Дифференциация подходов к управлению привилегированными пользователями — полный контроль с элементами Zero Trust для подрядчиков, повышение удобства и скорости работы для администраторов

Расширение использования PAM для нетипичных задач (защита бизнес-транзакций, баз данных и т.д.)

Гипотезы вендоров: enterprise уже защищен — PAM идет в средний бизнес

Создание облегченных версий PAM

По оценкам вендоров, крупнейшие корпоративные заказчики (enterprise) в значительной степени защищены PAM-решениями. Регуляторные требования как основной фактор развития рынка постепенно исчерпывают себя. Поскольку кибератаки смещаются в сторону менее защищенного среднего бизнеса, компании этого сегмента начинают активно задумываться о защите привилегированного доступа. Вендоры выводят на рынок облегченные «коробочные» версии.

Вывод на рынок PAM как услуги

В отличие от западного рынка, где облачный PAM активно развивается, вендоры не видят в России массового спроса на PAM как облачный сервис. MSSP-модель PAM находится в стадии формирования рынка и продвигается вендорами скорее «вручную», сталкиваясь с осторожным отношением клиентов.

“

Рынок PAM как сервис, по сути, только формируется. Российский рынок имеет свою специфику: компании, привыкшие платить за безопасность, обычно не очень любят облачные решения. Но и это меняется, в том числе. под воздействием дефицита бюджетов и кадров.

Константин Родин,

Заместитель директора по развитию бизнеса, АйТи Бастион

PAM Lite — это версия лицензии, которая естественно сложилась из практики работы с заказчиками. Она максимально закрывает потребности компаний с компактной инфраструктурой и небольшими командами ИТ и кибербезопасности.

Артем Назаретян,

Руководитель BI.ZONE PAM

64,5%

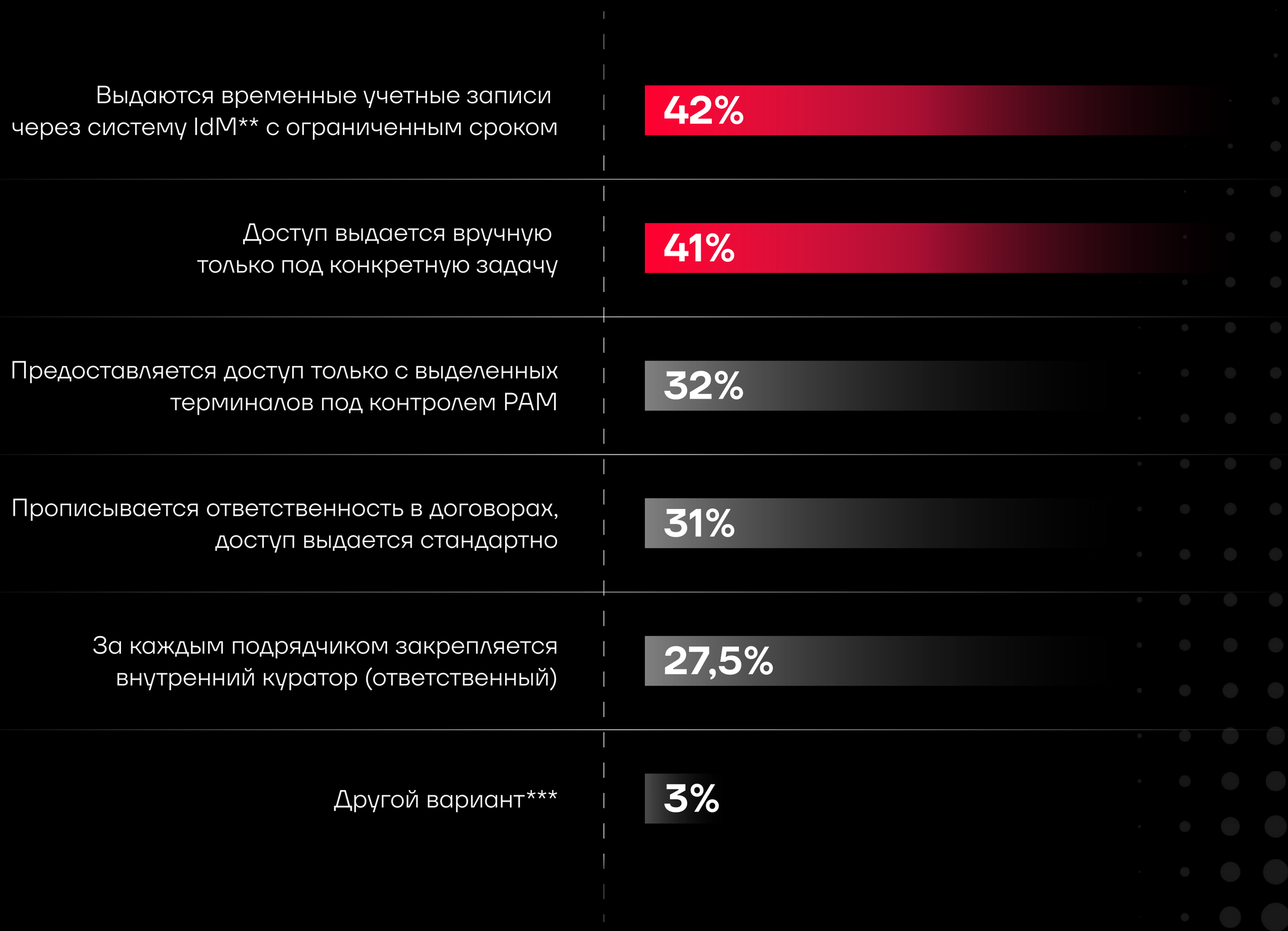
компаний контролируют администраторов регламентами, а не PAM

Как организовано управление доступом администраторов и других сотрудников с привилегированными правами?*

Большинство организаций контролирует доступ администраторов регламентами и логированием. Специализированные PAM-системы используют только 36,5% компаний, что указывает на высокий потенциал роста сегмента.

* Сумма превышает 100%, так как респонденты могли выбрать несколько вариантов ответа.
** В категорию «Другой вариант» попали ответы: через RDP; IDM; система 4 глаз (совместный доступ под контролем офицера безопасности, УЗ с расширенными правами заблокированы); используются отдельные УЗ; исполнение требований согласно стандартам ИБ организации; специальные учетные записи вида adm_familiya@mydomen с MFA, выдача административных прав только на управляемые данным индивидом системы.

Как в организации решен вопрос доступа для внешних подрядчиков?*



32% компаний допускают подрядчиков через PAM

Чаще доступ выдают временно через IdM (42%) или вручную под конкретную задачу (41%).

* Сумма превышает 100%, так как респонденты могли выбрать несколько вариантов ответа.
** Не только вендорские системы IdM, но и другие варианты автоматизации процесса управления учетными записями.
*** В категорию «Другой вариант» попали ответы о том, что подрядчикам не выдается доступ в инфраструктуру организации.

Для администраторов PAM — удобство, для подрядчиков — жесткий контроль

Важно упростить работу администраторов

Если для внешних разработчиков главная цель — это ограничение и контроль доступа (что, где и зачем они делают), то для своих администраторов это скорее история про упрощение жизни и безопасность. С помощью PAM мы хотим, чтобы у сотрудника была одна корпоративная учетная запись: с ней он входит в PAM, а внутри получает весь необходимый набор доступов к серверам и системам. Сам вход в PAM мы закрываем максимально строго: второй фактор и сетевые ограничения. Для подрядчиков у нас стоит другая система. Подрядчик заходит в консоль, видит доступные ему сервера, кликает и попадает туда с предоставленными правами, не задумываясь о паролях, которые могут автоматически меняться. Пока мы используем ее для ИТ-подрядчиков и для тех пользователей, кому выдаем какие-то серьезные, расширенные доступы.

Андрей Нуйкин,

Начальник отдела обеспечения безопасности информационных систем, Евраз

Для разделения внутренних и внешних пользователей используется PAM

У нас есть как внутренние, так и внешние сотрудники. На тестовом контуре у представителей разработки или тестирования доступ есть, но возникает необходимость протестировать решение в «бою». Они заходят в IdM и создают заявку, выбирая нужную систему. Внутри IdM зафиксирован список систем для разных категорий пользователей, и их маршрут зависит от статуса сотрудника. Если это штатный специалист, IdM понимает, что внутренний пользователь. Допустим, права не выдались автоматически по бизнес-роли, ему можно выдать доступ напрямую — у него просто появляется ярлык системы, и он заходит в нее. Если IdM видит, что запрос к боевой системе поступает от внешнего специалиста, заявка направляется по другому маршруту. IdM отправляет запрос через API в систему PAM. Там для него автоматически создается сервисная учетная запись (если он до этого ни разу не запрашивал доступ), для которой «нарезаются» определенные права в целевой системе.

Николай Черенков,

Руководитель отдела сопровождения процессов информационной безопасности, Банк Синара

+ Сценарии применения PAM для администраторов и внешних подрядчиков принципиально отличаются по целям, архитектуре и требуемому уровню контроля. При работе с администраторами важно упростить повседневную работу ИТ-отдела, одновременно убрав риски утечки паролей. При работе с подрядчиками — минимизировать риски и обеспечить строгий контроль каждого их действия.

Какое в организации отношение к подходу Zero Trust («никому не доверяй»)?

22%
Внедрены элементы Zero Trust только для внешних подключений и подрядчиков

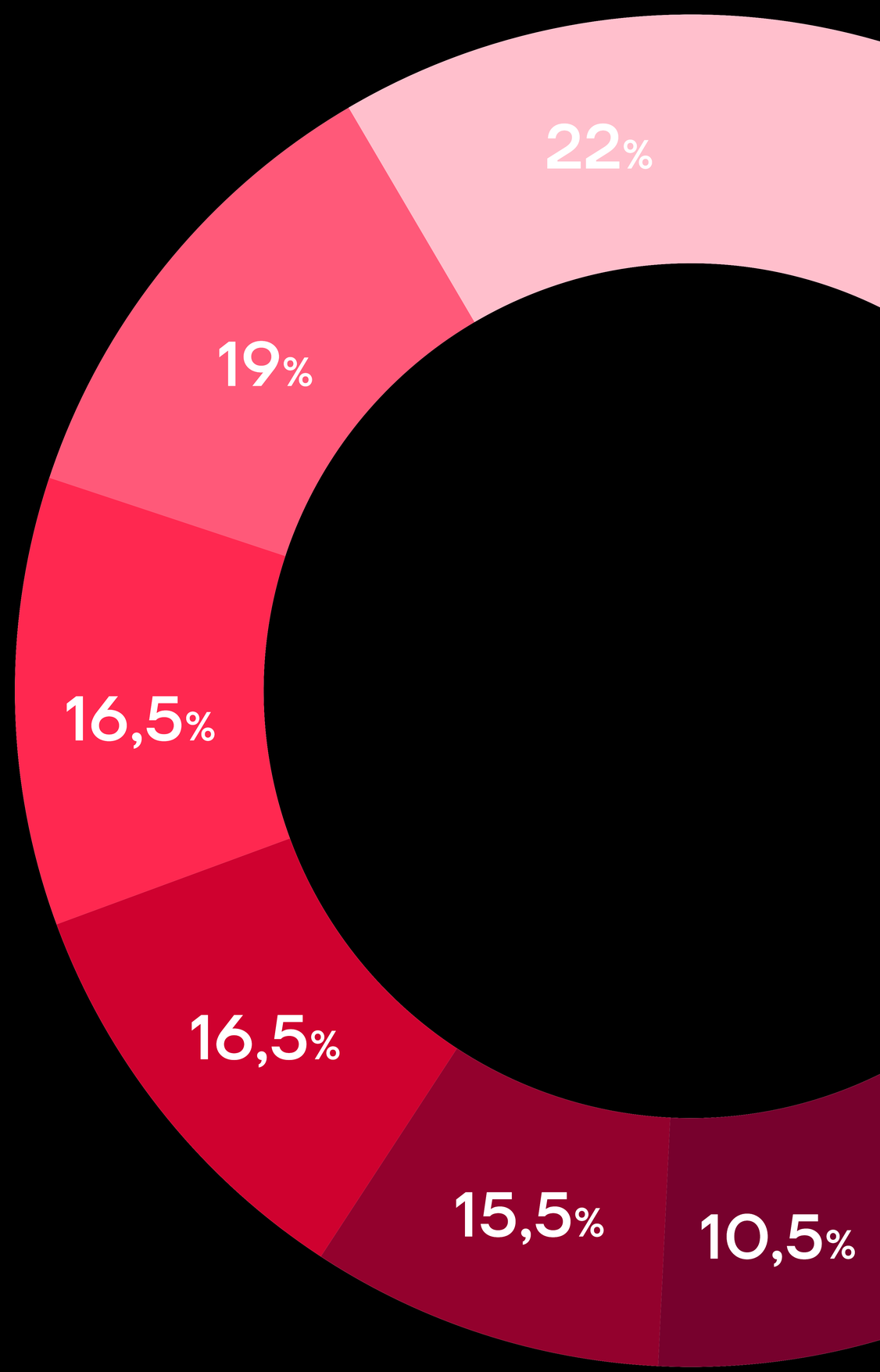
19%
Внедрены отдельные элементы Zero Trust, но путь к нему займет годы

16,5%
В организации уже внедрены основные элементы Zero Trust

16,5%
Zero Trust является недостижимым идеалом, всегда будет компромисс с бизнесом

15,5%
Затрудняюсь ответить

10,5%
Zero Trust избыточен для нашей организации

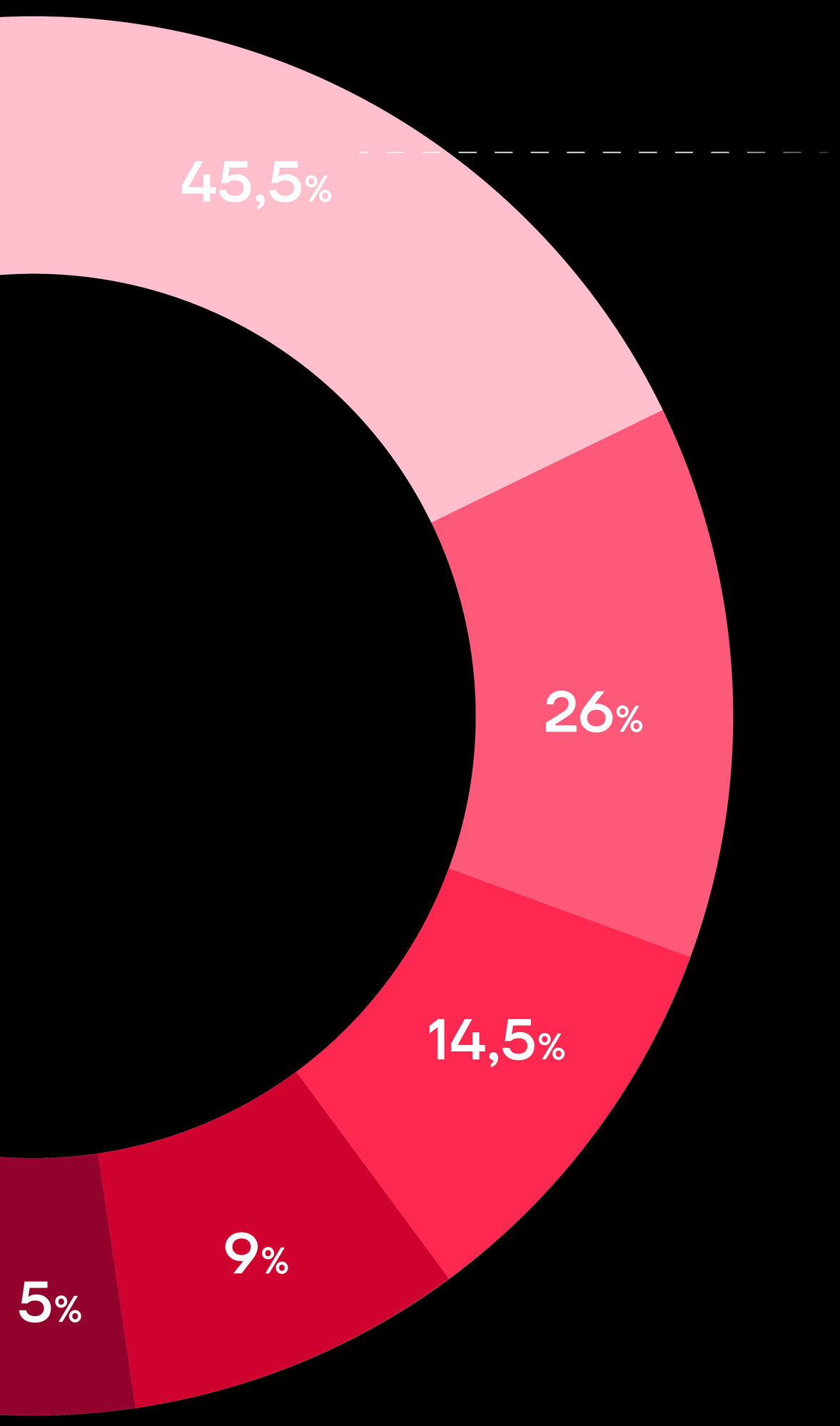


22% компаний применяют Zero Trust только к внешним подключениям

Примерно в каждой пятой организации Zero Trust применяется только к внешним подключениям и доступу подрядчиков. Основные элементы этой концепции внедрены лишь в 16,5% компаний.

45,5%

организаций выдают права бессрочно — Just-in-Time пока редкость



Используете ли вы концепцию доступа «точно вовремя» (Just-in-Time)?

45,5%
Нет, права выдаются на постоянной основе до отзыва

26%
Да, нужные права выдаются только на время выполнения задачи

14,5%
Права привязаны к графику работы (автоматическая выдача по расписанию)

9%
Доступ выдается на жестко ограниченное окно (например, 2 часа) под присмотром

5%
Затрудняюсь ответить

PAM выходит за пределы ИТ: веб-приложения, бизнес-пользователи, платежи

Традиционно PAM рассматривался как сугубо инфраструктурный инструмент для ИТ-администраторов и подрядчиков — например, для контроля доступа по SSH. Однако сегодня границы его применения существенно расширяются:

Масштабирование на бизнес-пользователей в компаниях с цифровой бизнес-моделью

Если в компании критическая концентрация высокорисковых цифровых активов, под контроль PAM переводят не только системных администраторов, но и другие категории сотрудников, имеющих доступ к ключевым элементам инфраструктуры.

Контроль веб-приложений

Помимо классических протоколов (SSH/RDP) для работы с хостами, через PAM начинают организовывать и мониторить доступ внешних контрагентов к прикладным внутренним веб-сервисам.

Защита бизнес-процессов

PAM внедряют в операционные цепочки для сквозного контроля критических действий — например, при проведении платежей в бухгалтерии.

Тем не менее, этот тренд сдерживается двумя барьерами: высокой стоимостью тяжелых PAM-систем (особенно чувствительной при масштабировании на широкий круг пользователей) и сильным сопротивлением бизнес-сотрудников из-за громоздких интерфейсов. В результате компании часто находят компромисс, отказываясь от использования классического PAM для несвойственных ему задач в пользу более легких, специализированных и экономичных решений.

> У нас есть бизнес-пользователи с привилегированным доступом, но сейчас мы постепенно пересматриваем эту практику. Перед командой разработки стоит комплексная задача: собрать требования бизнеса и создать удобные инструменты для выполнения необходимых операций. Например, если сотруднику из бизнеса требуется регулярно что-то выгружать, вместо прямого доступа к базе лучше предоставить готовый интерфейс, в котором такая выгрузка уже реализована. Это позволяет сохранить удобство для бизнеса и одновременно снизить риски, связанные с избыточными правами доступа к системам и базам данных. Если ты не ИТ-специалист и не администратор, то привилегированный доступ напрямую к системам и базам тебе не нужен.

Илья Кулешов,

Руководитель отдела развития информационной безопасности, Ламода Тех

34,5%

компаний используют менеджеры паролей вендоров

Используются ли в вашей компании специализированные менеджеры паролей для управления учетными записями?*

34,5%	Да, используется специализированный вендорский менеджер паролей
22,5%	Да, используется хранилище паролей в рамках PAM-системы
16%	Да, используется open-source решение для управления паролями
20,5%	Нет, но планируется внедрение
17,5%	Это нецелесообразно на текущем этапе

\+ 22,5% компаний используют функцию хранилища паролей в PAM.

* Сумма превышает 100%, так как респонденты могли выбрать несколько вариантов ответа.

Сегмент

IDM/IGA

Рынок IdM/IGA сегодня

+16%

за год — самый быстрый рост среди PAM, IdM и MFA

3,6

млрд ₽
размер рынка
в 2025 году

16%

темп роста рынка в 2025 году
по отношению к 2024 году
(в денежном выражении)

~40 проектов было начато в 2025 году (из них ~23 проекта начали топ-2 вендоров рынка)

Топ-3 вендоров по выручке от продажи лицензий, консалтинга и техподдержки:

- Аванпост (Avanpost IDM)
- Газинформсервис (Ankey IDM)
- ГК «Солар» (Solar inRights)

Покупательские тренды

Фокус на сокращении сроков онбординга, включая процесс безопасного удаленного пред-онбординга (на этапе кандидата)

Использование ИИ-агентов и чат-ботов для автоматизации процессов

Смена парадигмы внедрения: «Есть слона по частям» вместо «Семь раз отмерь – один отрежь»

«IdM-центричность»: выстраивание сквозного процесса управления доступами вокруг IdM

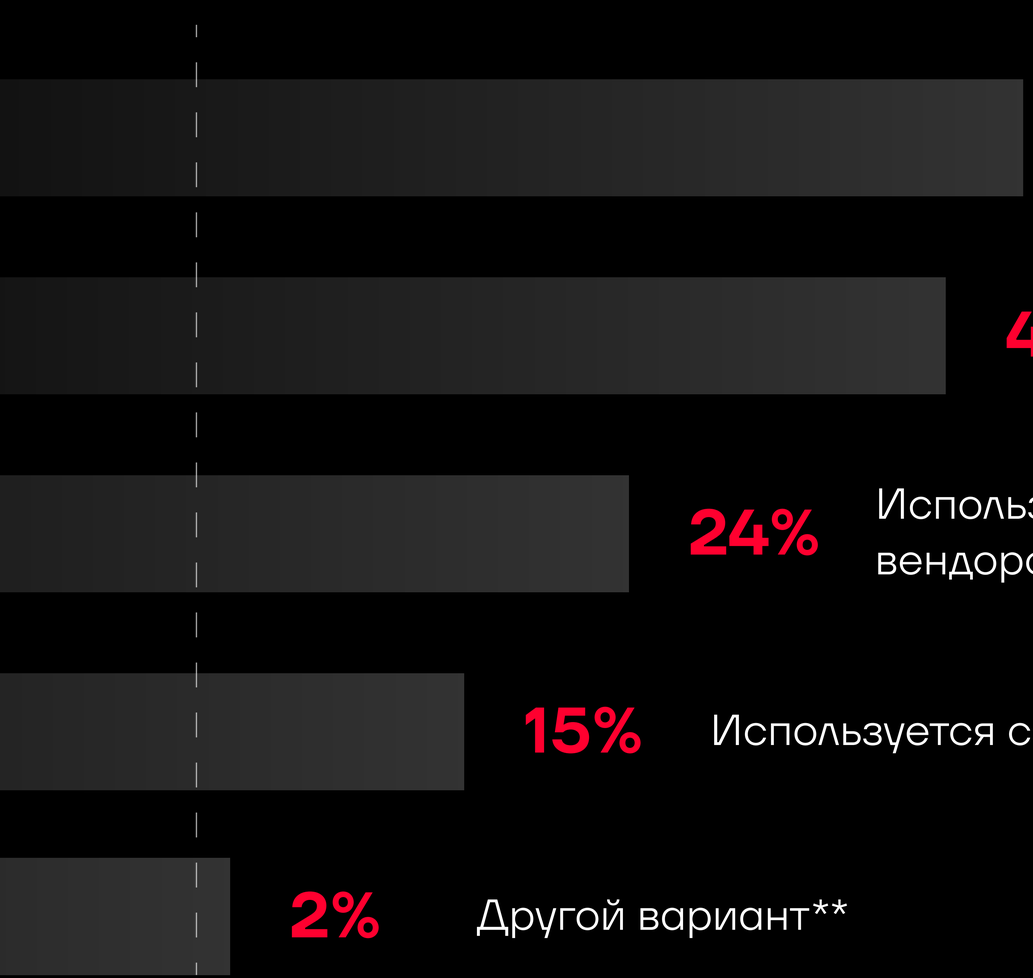
Экспоненциальный рост сервисных учетных записей

Высокая доля собственной разработки IdM

24%

компаний имеют
специализированную IdM

Как организовано управление жизненным циклом учетных записей?*



46% Автоматизирован процесс через связку HR-системы, Service Desk и скриптов

40% Обработка заявки пользователя и выдача доступа происходит вручную

24% Используется специализированное вендорское решение (IdM/IGA-система)

15% Используется самописное решение

2% Другой вариант**

+ Чаще всего для управления жизненным циклом учетных записей используется связка имеющихся решений или ручная обработка заявок пользователей. Специализированная IdM есть только в каждой четвертой организации.

* Сумма превышает 100%, так как респонденты могли выбрать несколько вариантов ответа.
** В категорию «Другой вариант» попали ответы: автоматизация JML на основе данных HR-системы; заявки через внутренний портал от руководителя; ручной отзыв прав при увольнении; скрипты на базе ЗУП; управление сроком действия паролей в AD.

20 000 → 60 000

учетных записей: без IdM поддержка не справится

Бизнес-требования: скорость онбординга, производительность труда

Для бизнеса это означает задержку полноценного включения сотрудника в работу и дополнительные издержки. На фоне дефицита ИТ-специалистов автоматизация этих процессов позволяет масштабировать инфраструктуру и поддерживать рост компании без пропорционального увеличения штата администраторов.

Рост кадрового хаоса (по мере роста масштаба инфраструктуры)

Если компания со 100 пользователями может администрировать права в ручном режиме, то для крупных организаций (с десятками тысяч учетных записей) это становится невыполнимым. При ручном отзыве прав в системах массово остаются активные учетные записи уволенных сотрудников.

Причин, почему мы смотрим в сторону IdM, несколько. Это прозрачное управление жизненным циклом учетных записей. У нас огромное количество информационных систем и аккаунтов. Где возможно, используется единая AD-аутентификация. Но остаются легаси-системы и сервисы со своей локальной базой пользователей, где все приходится делать вручную с большим количеством нюансов. Вторая причина — это запрос от кадров. Коллеги борются за дебюрократизацию и скорость выдачи прав. Все хотят как в идеальном мире: сотрудник выходит в первый день, на столе его ждут настроенный ноутбук и мерч, он садится и сразу работает. У нас пока так не получается. Еще одна причина — снижение нагрузки на администраторов и техподдержку. Сейчас у нас порядка 20 тысяч учетных записей, а в планах — расширение до 60 тысяч. Рост в три раза означает и трехкратное увеличение объема работы по выдаче, изменению и отзыву прав. Без автоматизации поддержка просто «ляжет».

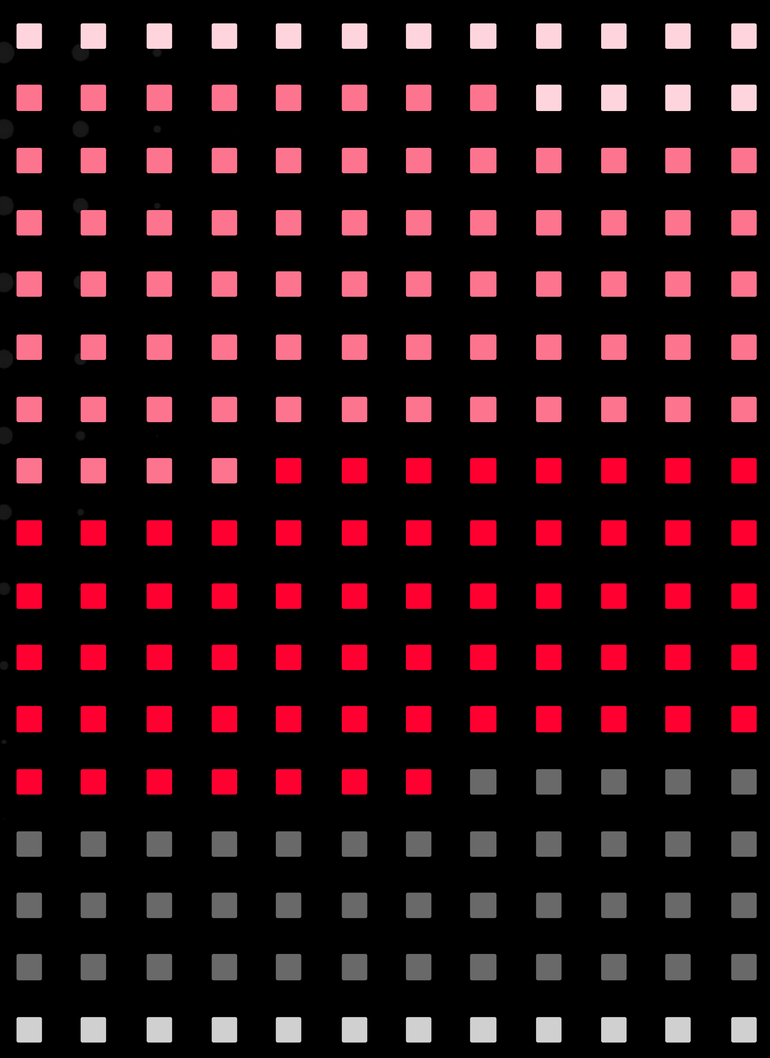
Андрей Нуйкин,

Начальник отдела обеспечения безопасности информационных систем, Евраз

71,5%

компании выдают права новичку **1 день и дольше**

Сколько времени в среднем занимает онбординг (выдача всех прав) нового сотрудника?



8,5% Более недели

33,5% От 2 до 5 рабочих дней

29,5% Один рабочий день

22,5% Менее 4 часов

6% Процесс начинается еще до выхода (на этапе кандидата)

Сроки онбординга сотрудников все еще высоки.
Чтобы получить права, новому сотруднику, как правило, требуется более одного дня.

Порог 30%

как крупные компании автоматизируют роли

Ведущие компании избегают чрезмерной сложности процесса создания и назначения бизнес-ролей. Например, в компании «Ламода Тех» обучили алгоритм анализировать пересечения ролей: если 100% сотрудников на определенной должности имеют конкретную личную роль, IdM автоматически переводит ее в разряд должностных. Если покрытие составляет от 80% до 100%, роль назначается автоматически после быстрой верификации со стороны ИБ. В Банке Синара внедрили эвристику для тестовых серверов: если более 30% сотрудников отдела разработки уже имеют доступ к конкретному тестовому серверу, IdM автоматически открывает его для всей команды.

Использование высокоуровневых бизнес-ролей

Сейчас мы стараемся двигаться в сторону бизнес-ролей, чтобы новые сотрудники создавали как можно меньше ручных заявок. Это позволит оптимизировать время администраторов: к тестовым серверам в банке привлекается очень много разработчиков, которые постоянно подавали по 10 или даже 30 ручных заявок на разные сервера. Вручную проанализировать, какому именно подразделению разработчиков какой сервер нужен, чтобы сразу зашить это в бизнес-роль, сложно. Поэтому мы пошли по следующему пути: IdM автоматически добавляет сотрудникам отдела доступ к серверу, если в штате этого подразделения более 30% сотрудников уже имеют туда доступ. На тестовом контуре мы это сделаем пока вообще без отдельных заявок. А на боевом контуре схема должна быть чуть строже.

Николай Черенков,

Руководитель отдела сопровождения процессов информационной безопасности, Банк Синара

Первичные доступы выдаются на основе базовых ролей

Значительная часть доступов выдается автоматически в рамках преднастроенных ролей. У нас сформирован набор около 10 базовых стартовых ролей разных категорий — разработчик, бизнес, кибербезопасность и других, — которые назначаются при онбординге сотрудников. Данные о должности и подразделении из HR-системы используются для автоматического назначения базовых доступов при создании профиля сотрудника. Таким образом, значительная часть необходимых сотруднику прав уже заложена в сам процесс его появления в компании, а дополнительные доступы оформляются отдельно по мере необходимости.

Даниил Мирошник,

Руководитель направления SOC, Домклик

Доступ до первого рабочего дня: «рекрут», чат-бот и IdM-гид

Как российские компании автоматизируют доступ для нового сотрудника

Пре-онбординг со статусом «Рекрут»

Кандидату, который только принял оффер, еще до официального подписания приказа о приеме создается учетная запись со статусом «рекрут». Он получает минимальные права для удаленного входа в закрытый контур, чтобы ознакомиться с регламентами и подписать документы в КЭДО. Организуется интеграция с HeadHunter — соискатель еще до трудоустройства получает индивидуальную ссылку, переходит по ней и загружает сканы своих документов. Данные импортируются в 1С, полностью исключая ручной ввод со стороны HR-отдела.

Доставка первого пароля в обход людей

Реализуется через одноразовые ссылки или через чат-бота в мессенджерах. Чтобы первый пароль не знали рекрутеры и руководители, компания «Ламода Тех» берет личную почту кандидата из кадровой системы и отправляет туда одноразовую ссылку, которая сгорает после первого перехода и содержит временный пароль. В компании «Домклик» регистрация и первая выдача реквизитов завязаны на чат-бота. Бот выдает первый пароль, помогает найти контакты коллег, а в дальнейшем позволяет сотруднику самостоятельно сбросить забытый пароль без обращения в техподдержку.

Мультимедийный IdM-гид

Текстовые инструкции по безопасности никто не читает. В Банке Синара предложили концепцию, при которой новый сотрудник при первом входе видит интерактивный анимационный ролик (по аналогии с игровыми туториалами).

Было бы отлично, если бы в IdM можно было реализовать интерактивный туториал для пользователей — например, с анимацией или в формате пошагового путеводителя. Одна из главных проблем новичков, особенно молодых сотрудников, в том, что они приходят и не всегда понимают, как все устроено. Иногда человек даже не до конца представляет, на какую должность он пришел, в какое подразделение попал и с какими задачами ему предстоит работать. Такой путеводитель мог бы знакомить сотрудника с сервисами, которыми ему придется пользоваться, и последовательно вводить его в рабочие процессы. Например, человек только вводит логин и пароль, еще даже не увидев рабочий стол, а система уже запускает мультимедийное приветствие: «Приветствуем тебя! Ты присоединился к такой-то команде...».

Николай Черенков,

Руководитель отдела сопровождения процессов информационной безопасности, Банк Синара

90 дней

без входа — сигнал к блокировке учетной записи

Чтобы пересмотр прав работал эффективно, системы стоит сегментировать: разделить по уровню критичности и регулярно проверять доступ к наиболее важным из них. Стажерам лучше выдавать только минимально необходимые права, доступ подрядчиков — регулярно сверять с компанией-партнером, а неактивные учетные записи — блокировать. Дополнительно анализ бизнес-логов помогает выявлять подозрительные действия даже у пользователей с легитимным доступом.

Отключение неактивных учетных записей через интеграцию с SIEM

В нашем банке интеграция IdM с SIEM настроена, и работает она следующим образом: SIEM регулярно опрашивает целевые системы на предмет аккаунтов, неактивных более 90 дней. Если обнаружена учетная запись, которой долго не пользовались, SIEM передает в IdM логин и идентификатор соответствующей системы. Получив эти данные, IdM запускает автоматический процесс: ставит метку на отключение и отправляет в целевую систему команду заблокировать учетную запись, меняя ее статус.

Николай Черенков,

Руководитель отдела сопровождения процессов информационной безопасности, Банк Синара

Частота пересмотра прав зависит от критичности процесса

Все системы в компании разбиты по «очередям» — от 1-й до 4-й. К первой относятся сервисы, сбой в которых приводит к полной остановке бизнеса. Любые доступы к системам здесь попадают под регулярный процесс ресертификации. Проверку проходят не только привилегированные, но и обычные пользовательские права. Для критичных систем первой очереди мы можем ставить периодичность ресертификации раз в три или шесть месяцев. А для менее критичных сервисов — более раза в год.

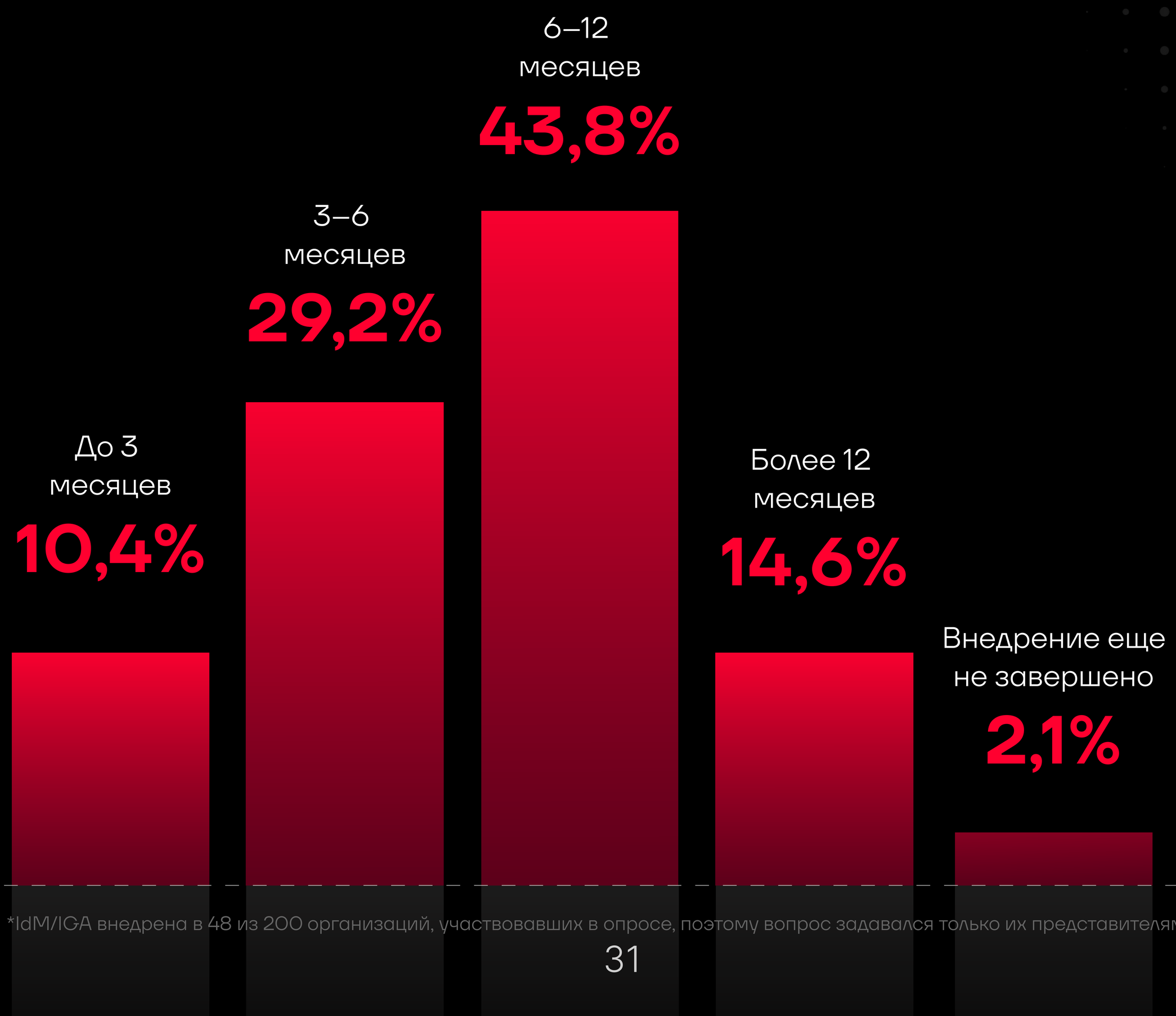
Илья Кулешов,

Руководитель отдела развития информационной безопасности, Ламода Тех

43,8%

компаний внедряли **IdM**
от 6 до 12 месяцев

Какая была продолжительность полного внедрения IdM-системы (от старта проекта до эксплуатации)?*



*IdM/IGA внедрена в 48 из 200 организаций, участвовавших в опросе, поэтому вопрос задавался только их представителям.

80% заявок обрабатываются автоматически: IdM эффективнее внедрять поэтапно

Компании часто говорят о необходимости глубокого аудита процессов перед стартом IdM, хотя на деле такой анализ требует значительных ресурсов и быстро теряет актуальность. Секрет успешных внедрений — в правильном фокусе: автоматизировать нужно не самые стабильные процессы, а те, где ускорение выхода нового сотрудника на работу приносит бизнесу наивысшую ценность.

Секрет успешного внедрения IdM — «есть слона по частям»

Мы предприняли две попытки внедрения IdM. В первый заход мы попытались охватить все и сразу. Но когда запустили систему в эксплуатацию, все, что могло пойти не так, пошло не так. Ко второй попытке мы подошли более осмысленно. Мы выделили конкретные процессы, которые подлежат автоматизации, и проработали простые сценарии совместно с кадровой службой и ИТ. Выстроенные цепочки мы сразу запускали в прод, не дожидаясь завершения всего масштабного объема работ. Начав с простого процесса (увольнения), мы перешли к автоматизации управления практически всеми типами доступов. Раньше новый сотрудник мог ждать нужные доступы до двух недель. Сейчас мы можем выдавать доступы еще до выхода человека на работу. Теперь из сотен тысяч запросов доступов в месяц более 80% обрабатываются полностью в автоматическом режиме.

Антон Мелков,

Амбассадор Айдентити Клуба, Начальник управления крупного российского банка

Внедрение IdM должно начинаться с самых ценных процессов

До внедрения IdM создание учетной записи в ИТ занимало до трех дней, и это было слишком долго. Операционный персонал на складах и в ПВЗ приходит на рабочее место в семь утра, в восемь часов они начинают собирать заказы. Для бизнеса приоритетны непрерывность процессов и скорость выхода сотрудника на работу, а задача ИБ — обеспечить, чтобы доступы не только оперативно предоставлялись, но и своевременно отзывались. Когда стало очевидным, что скорость выдачи доступов напрямую влияет на бизнес-процессы и, соответственно, результат, руководство поддержало инвестиции и выделило ресурсы на развитие системы. На первом этапе мы настроили базовые процессы создания и блокировки учетных записей. Тогда кастомных сценариев почти не было, а уже сегодня в системе работает уже около 400 кастомных процессов.

Илья Кулешов,

Руководитель отдела развития информационной безопасности, Ламода Тех

До 30

забытых ТУЗ на сотрудника: как взять их под контроль

Контроль сервисных (технических) учетных записей (СУЗ/ТУЗ) эксперты называют главным вызовом, поскольку их количество в компаниях растет по экспоненте и значительно превышает число реальных сотрудников.

Привязка всех СУЗ/ТУЗ к кураторам (владельцам)

При инвентаризации легаси эффективна временная изоляция неидентифицированных ТУЗ — это мгновенно проявляет владельца процесса. Предотвратить появление новых неизвестных аккаунтов помогает жесткая регламентация: права, цели и сроки жизни ТУЗ должны фиксироваться еще при создании заявки.

Автоматический контроль паролей

Чтобы исключить человеческий фактор, IdM и PAM полностью берут под контроль сервисные пароли: они ротируют их в фоновом режиме и помещают в хранилище (Vault), закрывая доступ разработчикам к открытым секретам. Параллельно система отслеживает жизненный цикл ТУЗ и заблаговременно через мессенджер или почту уведомляет кураторов об истечении срока действия учетной записи.

Автоматическая переаттестация при увольнении куратора

Чтобы уход сотрудника не парализовал бизнес-процессы слепым отключением сервисных аккаунтов, IdM реагирует на увольнение автоматической переаттестацией, обязывая руководителя назначить нового владельца ТУЗ. Дополнительно система предлагает превентивное делегирование секретов: перед увольнением или отпуском логины, пароли и OTP-коды от общих кабинетов заранее передаются коллегам через менеджер паролей.

Раньше случались ситуации, когда за увольняющимся сотрудником числилось, условно, около 30 сервисных учеток. При уходе он мог вспомнить лишь часть из них и просто написать в письме: «Вот эти учетные записи я знаю, передайте их такому-то коллеге». Мы меняли владельцев вручную, сотрудник уходил, а оставшиеся учетные записи висели в «воздухе». Теперь при увольнении срабатывает механизм аттестации: IdM находит все оставшиеся аккаунты ушедшего работника и отправляет его руководителю уведомление: «За данным сотрудником числится еще 15 сервисных учетных записей, необходимо назначить нового владельца». Руководитель или новый ответственный сотрудник в IdM оформляют заявку на изменение владельца.

Николай Черенков,

Руководитель отдела сопровождения процессов информационной безопасности, Банк Синара

IdM — точка сборки процессов Identity Security

Эксперты сходятся во мнении, что управление доступом должно быть сквозным процессом, но на практике не могут его реализовать. Поворотным моментом становится внедрение в компании IdM, которое позволяет собрать большинство инструментов Identity Security под единым управлением.

IdM был стартовой точкой создания подразделения по управлению учетными записями

Мое подразделение находится в структуре подразделения безопасности, не ИТ. Появилось оно эволюционным путем: организация большая, и со временем накопились вопросы — процессы согласования тянулись долго, было много бумажек. Это вызывало много замечаний от регуляторов и рекомендаций аудиторов привести все в порядок. Все началось со становления системы IdM и налаживания базовых процессов совместно с ИТ и кадровой службой. По мере развития зона ответственности постепенно расширялась: добавлялись задачи по PAM, внедрению двухфакторной аутентификации. Когда накопился большой багаж специфических задач и процессов, наша команда окончательно сформировалась в отдельное подразделение.

Антон Мелков,

Амбассадор Айдентити Клуба, Начальник управления крупного российского банка

Разделение управления доступами между ИБ и ИТ

В первые годы в Ламода управление доступами находилось в зоне ответственности ИТ. Затем процесс выделили в отдельное направление внутри ИБ — и это абсолютно правильно — у ИТ и ИБ разные приоритеты. Такой подход позволил точнее учитывать риски при принятии решений. На первом этапе наша команда занималась преимущественно IdM, но постепенно зона ответственности расширялась: кто-то отвечал за архитектуру процессов, кто-то за настройку доступов, кто-то за кастомизацию пользовательского портала. Пять лет назад случилась трансформация: в департаменте ИБ сохранили только тот функционал IdM, который действительно требует экспертизы безопасника. Если операция сводится к механическому согласованию по инструкции без глубокого анализа рисков, она переходит обратно в ИТ. За счет высвободившихся ресурсов мы смогли сфокусировать команду IdM на развитии смежных, более сложных сервисов — таких как PAM, менеджеры секретов и хранилища паролей.

Илья Кулешов,

Руководитель отдела развития информационной безопасности, Ламода Тех

Своя разработка или коробка: главная дилемма IdM

Собственная разработка

- Максимальная гибкость и скорость изменений
- Экономическая выгода при наличии своего штата
- Глубокая интеграция со специфическими процессами

Покупка вендорского решения

- Наличие готовой базовой логики и стандартов
- Готовые сложные коннекторы
- Простота поиска кадров для сопровождения системы

На мой взгляд, сейчас главная проблема со всеми коммерческими продуктами заключается в том, что организация подсаживается на «иглу» конкретного вендора. Что касается IdM-систем: на данный момент я не знаю на российском рынке решений, которые позволяли бы так же гибко настраивать все самостоятельно. Чаще всего продаются хорошие, работающие решения «из коробки», но они абсолютно негибкие. То есть внедрение идет по стандартному проекту: расписывается ТЗ, фиксируются сетапы, и через год у тебя появляется готовый продукт, который начинает управлять доступами. Но затем возникают проблемы: любые доработки снова требуют полноценной проектной деятельности. В наших реалиях это превращается в бюрократию, которую невозможно провернуть достаточно быстро.

Игорь Зверев,

Руководитель отдела автоматизации и управления доступами, VK

Купить лицензии и развернуть продукт на сервере можно простым «Next, Next, Next». Самое интересное начинается дальше. Хаос автоматизировать нельзя — нужен порядок. В IdM необходимо завести роли и процессы: что, кому, куда и зачем предоставляется. А у нас четкого описания ролей пока нет. Права выдаются по запросу: я пришел и попросил то, что нужно, или шеф сказал доступы оформить. Здесь возникает главная сложность: либо наводить порядок своими силами (а это требует людских ресурсов и времени), либо нанимать подрядчиков.

Андрей Нуйкин,

Начальник отдела обеспечения безопасности информационных систем, Евраз

4–6

Запуск месяцев: вендоры упрощают IdM

Вендоры IdM стремятся избавиться от сложного кастомного кода, удешевить техподдержку и ускорить закрытие сделок. Для клиентов это означает кратное снижение стоимости продукта и работ, быстрый запуск в эксплуатацию за 4–6 месяцев и возможность оперативно продемонстрировать бизнесу окупаемость (ROI) для получения бюджетов на дальнейшее расширение системы.

IDM Base удешевляет внедрение и упрощает поддержку

IDM Base уже зарекомендовал себя в коммерческих внедрениях. По сути, это базовая конфигурация системы управления доступом (Identity Management) — тот самый правильный фундамент, который мы отточили до мелочей, и от которого действительно стоит отталкиваться для быстрого старта. Мы сейчас просто запретили своим инженерам брать что-либо другое в качестве основы в каждый новый проект. Это сильно облегчило нам возможности обновлений: где-то система встанет и будет работать «как есть», а где-то на ее базе сделают отдельные процессы или доработки. Если в продукте появляются новые API, позволяющие делать что-то более правильно, то и скрипты из этой конфигурации под них переписываются — пусть и с небольшим лагом в месяц-два. Но они переписываются, перетестируются и идут в качестве обновлений ко всем новым клиентам, а также к тем, кто остался на исходной конфигурации. В итоге это дает реальное сокращение стоимости нашей работы в проекте и существенное снижение затрат на техподдержку.

Александр Махновский,

Технический директор, Аванпост

Переход от внутреннего проекта к рыночному продукту занимает годы

Ankey IDM изначально разрабатывался для крупного якорного заказчика, что заложило мощную технологическую базу. Работа с холдингом предполагает сложные нестандартные требования и учит решать задачи, которых просто не возникает у более простых продуктов. Однако выход на открытый рынок изменил наш подход к продукту. Высокая технологичность сама по себе уже перестает быть преимуществом. Поэтому сейчас мы фокусируемся не только на новых функциях, но и на упрощении пользовательских сценариев, делая Ankey IDM интуитивно понятным даже для непрофильных специалистов. Более того, в ряде аспектов мы опередили время: поддержка контейнеризации была внедрена несколько лет назад, когда для многих заказчиков и интеграторов это еще не было привычной практикой. Сегодня этот задел превращается в реальное конкурентное преимущество.

Александр Давыдов,

Менеджер продукта Ankey IDM, Газинформсервис

Сегмент

MFA/ SSO/ IAM

Единый вход и управление доступом — самый медленный рост среди ключевых сегментов

3,1 **млрд ₽** размер рынка MFA/SSO/IAM в 2025 году

7% **темп роста** рынка MFA/SSO/IAM за 2025 год

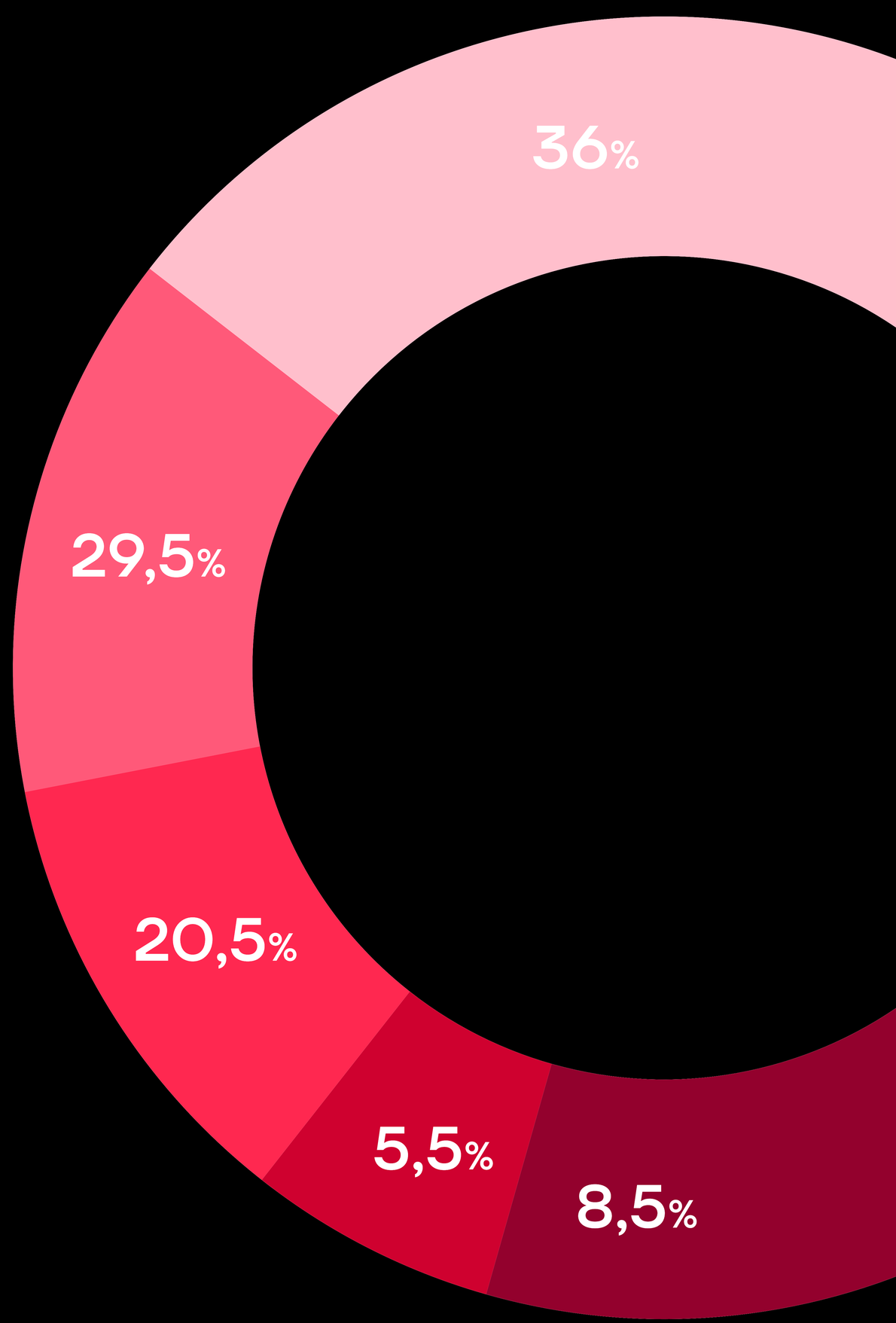
Топ-3 вендоров по выручке от продажи лицензий и техподдержки:

- Индид (Indeed AM)
- МУЛЬТИФАКТОР (Multifactor)
- Аванпост (Avanpost MFA+, FAM)

36% компаний покрыли MFA все системы

Насколько охвачена организация многофакторной аутентификацией (MFA)?

- **36%** Охвачены все сотрудники и системы
- **29,5%** Охвачены только критические системы
- **20,5%** Охвачены только для удаленного доступа
- **5,5%** Охвачены только администраторы
- **8,5%** Не внедрена MFA



+ Только в трети организаций MFA охвачены все сотрудники и системы.

Покупательские тренды

- Поиск решения проблемы доставки факторов (в условиях блокировки приложений и сбоев связи)
- Эксперименты с беспарольным входом и биометрией
- Интерес к адаптивной (контекстной, непрерывной) аутентификации

45,9% компаний располагают MFA на своих серверах

20% в облаке

Какие типы развертывания многофакторной аутентификации (MFA) используются в вашей организации?*

45,9% Локальное развертывание – решение полностью развернуто внутри защищенного контура организации на собственных серверах

38,3% Гибридное развертывание – комбинация компонентов: часть функционала (например, push-уведомления, доставка одноразового пароля) работает через облачные сервисы, а ядро – в локальной инфраструктуре**

25,7% MFA реализовано как встроенная функциональность в составе другой системы (IdM, PAM)

20,8% Облачное развертывание – решение предоставляется облачным провайдером, сервисы и данные размещаются вне инфраструктуры организации (например, в публичном облаке)

+ Почти в половине организаций MFA развернуто локально. Каждая пятая организация применяет облачное развертывание.

* Сумма превышает 100%, так как респонденты могли выбрать несколько вариантов ответа.
** Вендоры могут вкладывать разный смысл в термин «гибридное развертывание».

Блокировки затрудняют доставку второго фактора

Чтобы доставить второй фактор в условиях блокировок и сбоев связи, компании используют оффлайн-генераторы и PWA-приложения, проводную передачу на стационарные ПК, собственные сети Private LTE, а также экстренный сброс факторов через техподдержку.

Блокировка сторов и отсутствие интернета породило проблемы для MFA

Когда приложение, используемое в рамках процессов MFA, отсутствовало в сторах, мы были вынуждены оперативно перейти на альтернативные механизмы аутентификации и использовать доступные на тот момент приложения. Чтобы решить проблему с блокировкой приложений, мы прорабатываем возможность использования PWA-приложений. Но здесь возникает необходимость обеспечивать безопасное хранение секрета на устройстве пользователя. Другой важный момент, который требует проработки в текущих условиях — обеспечение работы MFA при отсутствии интернета, когда push-уведомления просто не доходят. Пуши — удобная опция для пользователей, но в случае блокировки приложений и ограничениях Интернета необходимо иметь четкий план действий.

Антон Мелков,

Амбассадор Айдентити Клуба, Начальник управления крупного российского банка

Устойчивость аутентификации при перебоях мобильной связи

Одна из недавних задач, с которой мы столкнулись, была связана с перебоями мобильной связи в некоторых регионах. Сотрудники, чья аутентификация была завязана на SMS, временно лишились возможности входить в рабочие системы. Поскольку бизнес работает по всей России и в разных часовых поясах, это повлияло на ряд операционных процессов: например, возникли задержки с отправкой некоторых фур, так как водители не могли войти в систему по SMS-коду. Нам пришлось оперативно менять и сбрасывать первый фактор аутентификации, что требует времени. Сотрудники находятся на смене, рядом не всегда есть ИТ-специалист, а самостоятельная установка и настройка приложения-аутентификатора может потребовать дополнительной поддержки.

Илья Кулешов,

Руководитель отдела развития информационной безопасности, Ламода Тех

FIDO2 и биометрия пока не заменяют пароль на рабочей станции

Для успешного внедрения беспарольной аутентификации следует использовать биометрию и стандарт FIDO2 посредством интеграции специализированных плагинов с провайдерами идентификации вроде ADFS. При этом важно учитывать платформенные ограничения (например, сложности совмещения с Windows Hello на ОС Windows в отличие от беспроблемной работы на macOS) и неизбежность сохранения классического пароля для первичного логина на рабочую станцию.

Внедрение биометрической аутентификации

Мы также развиваем биометрическую аутентификацию. Сейчас решение доступно не на всех устройствах и в основном используется на Mac. Для сотрудников этот способ удобнее, чем ввод кодов.
Мы интегрировали к ADFS найденный на GitHub плагин, который работает по протоколу FIDO2 и использует локальное защищенное хранилище устройства.

Илья Кулешов,

Руководитель отдела развития информационной безопасности, Ламода Тех

Банк стремится перейти на беспарольную аутентификацию, но не находит подходящих решений

Момент, который у меня вызывает профессиональный интерес, связан с безопасными сценариями беспарольной аутентификации. Внутри сети работают SSO и прокси-серверы, обеспечивающие сквозную аутентификацию. Но при входе на саму рабочую станцию пользователь все равно вынужден вводить логин и пароль. Достойных корпоративных альтернатив для входа на рабочую станцию (например, подтверждение входа через QR-код или через другое уже авторизованное устройство) мы пока не нашли. Мы регулярно мониторим эту тему в поисках решений, которые позволили бы сделать вход на рабочие станции одновременно более безопасным и удобным для пользователей.

Антон Мелков,

Амбассадор Айдентити Клуба, Начальник управления крупного российского банка

19%

компаний анализируют поведение в реальном времени

+ В организациях редко используется поведенческая аналитика в реальном времени. Чаще всего аномалии поведения анализируются постфактум через SIEM или DLP.

Используются ли решения для поведенческого анализа (UEBA и/или ITDR) в организации?

19%	Да, для выявления аномалий в реальном времени
34%	Данные анализируются постфактум через SIEM или DLP
26%	Анализируем аномалии только для высокорис-ковых операций (например, выгрузка баз ночью)
19%	Нет, но планируется внедрение
21%	Это нецелесообразно на текущем этапе

ITDR объединяет поведенческий анализ и другие механизмы защиты

Сегодня поведенческий анализ в реальном времени используют далеко не все компании, хотя именно он становится важной частью современного подхода к защите айдентити. Сам по себе этот механизм не решает задачу полностью — наибольший эффект он дает в связке с другими технологиями защиты. Аудит запросов доступа, минимизация разрешений, многофакторная аутентификация, обнаружение небезопасных конфигураций и анализ пользовательского поведения вместе формируют новый класс защиты Identity Threat Detection and Response (ITDR). В условиях, когда против бизнеса действуют организованные группы киберпреступников, отдельных мер защиты уже недостаточно: их сочетание позволяет оценивать риски в инфраструктуре айдентити, выявлять аномальную активность и своевременно реагировать на угрозы.

Лев Овчинников,

руководитель продукта
Indeed ITDR, Индид

От разового входа к непрерывной проверке сессии

Компании пока редко внедряют специализированные инструменты поведенческой аналитики для реагирования на компрометацию учетных данных. При этом они настраивают имеющиеся решения для закрытия этой задачи:

Создание «цифрового отпечатка»

Компании переходят от разовой аутентификации к непрерывной проверке легитимности сессии по комплексу косвенных признаков — IP-адресу, файлам cookies, GeoIP и параметрам устройства.

Профилирование на основе бизнес-логов

Компании анализируют активность пользователей непосредственно внутри прикладных систем (например, какие срезы отчетов в BI они открывают) и настраивают триггеры на критические аномалии — выгрузку баз данных ночью или авторизацию на устройствах, находящихся в километре друг от друга, в течение часа.

Главный тренд Identity Security для меня — Continuous Verification: мы стараемся постепенно уходить от модели, в которой доверие к пользователю устанавливается только в момент входа, к постоянной оценке контекста и риска в течение всей сессии. Для этого надо формировать контекстный профиль пользователя и смотреть, насколько текущая активность похожа на его обычную активность — условно, насколько мы можем доверять тому, что за экраном все еще тот же человек. Если уровень доверия к сессии снижается, система может запросить дополнительную аутентификацию. Мы в нашей компании тоже сейчас идем в сторону непрерывной верификации и постепенно применяем этот подход во внутренних сервисах для сотрудников.

Даниил Мирошник,

Руководитель направления SOC,
Домклик

Поведенческая аналитика — ответ на фишинг с ИИ

“

Полнота сбора данных и гибкий анализ паттернов поведения

Поведенческая аналитика уже используется в наших продуктах, но нам есть куда ее развивать. Наша задача — понимать, что происходит с учетной записью на всех этапах ее жизненного цикла. Здесь важны два аспекта. Первый — полнота данных. Необходимо видеть всю историю учетной записи: как она создается, к каким системам и данным получает доступ, как меняются способы аутентификации и привычное поведение, возникают ли аномалии и связана ли ее активность с другими учетными записями. Второй — анализ этих данных. Чем больше информации мы собираем, тем сложнее вручную выявлять значимые отклонения и взаимосвязи. При этом универсального набора признаков для всех компаний не существует: нормальное и подозрительное поведение зависит от инфраструктуры, процессов и ролей сотрудников. Поэтому инструменты аналитики должны позволять гибко настраивать сценарии и паттерны под конкретную организацию.

Евгений Плотников,

Менеджер сервиса двухфакторной аутентификации «ID от Контур.Эгиды», СКБ Контур

Поведенческий анализ — надежный барьер против умного фишинга

Использование искусственного интеллекта позволяет злоумышленникам создавать невероятно реалистичные сообщения и убедительно взаимодействовать с пользователем, вызывая полное доверие к собеседнику. В таких условиях шансы у нападающих объективно возрастают. Из технических средств эффективно сработают элементы поведенческого анализа — то есть непрерывный мониторинг действий сотрудников и использования их учетных записей. Внедрение поведенческого анализа в самые разные средства защиты — это единственный способ проактивно выявлять угрозы. Необходимо постоянно строить базовую линию поведения каждого пользователя и пристально анализировать любые отклонения: нетипичные точки подключения, нетипичное время, устройства, аномальные попытки доступа к ресурсам, а также отклонения поведения отдельного сотрудника от профиля и общей линии поведения всего его подразделения.

Андрей Лаптев,
Директор по продуктовому развитию, Индид

+ Вендоры проводят непрерывный сбор массивов данных о действиях учетных записей для построения базовой линии нормального поведения пользователя и анализа нетипичных паттернов, включая изменения геолокации, времени входа или используемых устройств. Чтобы автоматизировать выявление таких аномалий и проактивно реагировать на компрометацию, разработчики внедряют алгоритмы искусственного интеллекта непосредственно в свои продукты.

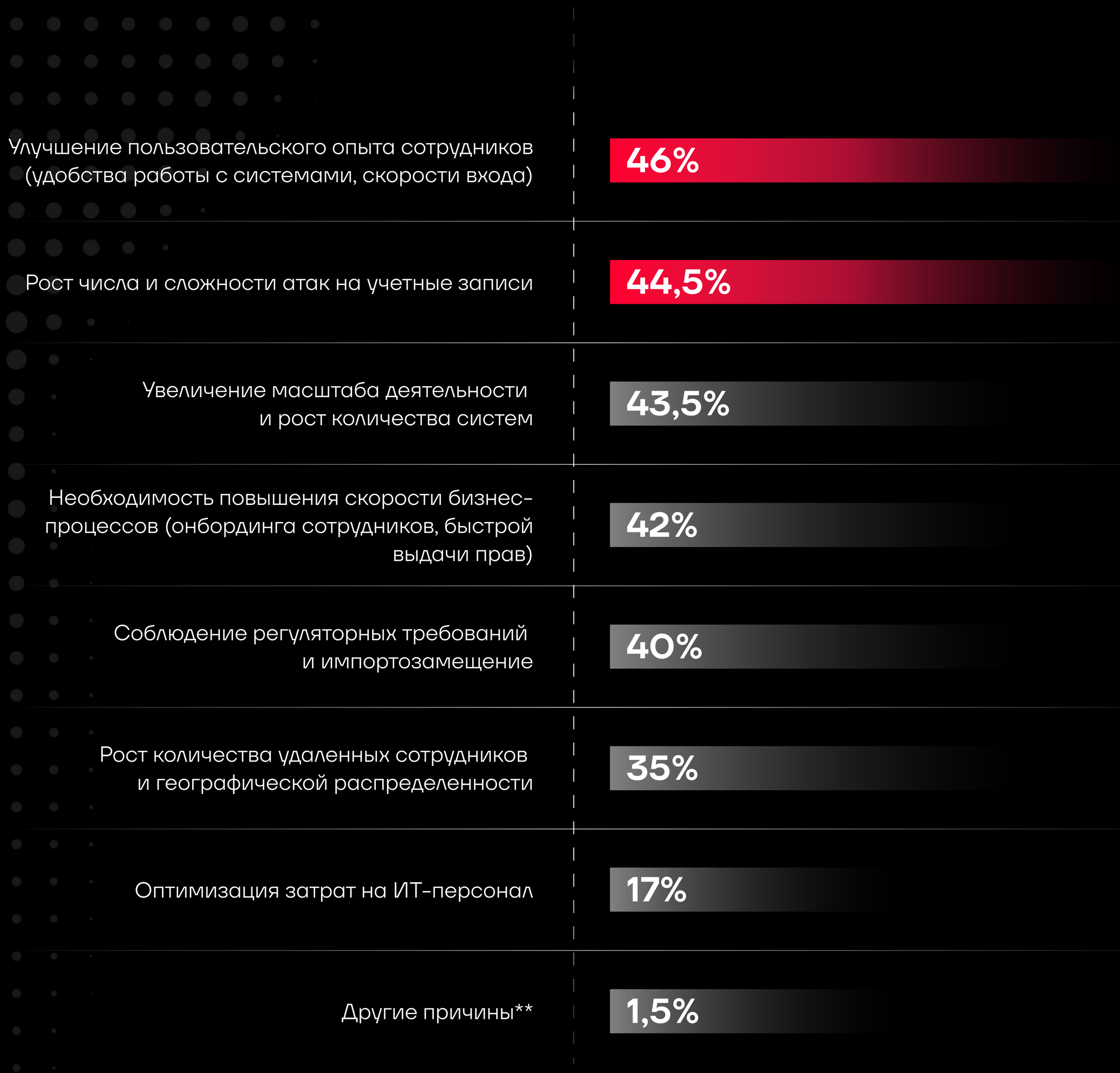
Задача 1:

Повышение удобства пользователей

46%

компаний внедряют Identity Security ради удобства сотрудников

Какие причины являются главными при внедрении систем управления и безопасности учетных записей? *



Удобство сотрудников — в тройке главных причин наравне с ростом атак (44,5%) и масштабом бизнеса (43,5%): разница между ними в пределах погрешности.

* Сумма превышает 100%, так как респонденты могли выбрать несколько вариантов ответа.
** В категорию «Другие причины» попали ответы: повышение информационной безопасности компании; требования департамента ИБ; стандарты AAA.

Удобный доступ проще контролировать: UX работает на безопасность

Эксперты сходятся во мнении, что удобство пользователей (User Experience, UX) критически важно для обеспечения безопасности, поскольку неудобные инструменты и процессы неизбежно ведут к саботажу и нарушению защищенности. Бесшовный для пользователей процесс доступа удобнее контролировать службе ИБ.

Важно мыслить категориями «процесс» и «сервис»

Мы с командой решили отказаться от оперирования понятием «система» — в стиле «где карту получали, туда и обращайтесь». Мы решили оперировать терминами «процесс» и «сервис». Если мы предоставляем некий сервис, то его потребителю абсолютно все равно, сколько за ним стоит систем — одна, две или десять. Ему не интересны внутренние механизмы. Человеку нужно просто получить учетную запись, сбросить забытый пароль, быстро подключить второй фактор, получить нужные доступы и не задумываться о том, как все устроено под капотом.

Антон Мелков,

Амбассадор Айдентити Клуба, Начальник управления крупного российского банка

User Experience важен и пользователю, и ИБ

Я абсолютно поддерживаю идею, что одним из ключевых факторов качественного IDM-решения является User Experience. Могу поделиться личным опытом: в 2023–2024 годах я работал SOC-аналитиком в одной из крупнейших нефтяных компаний России. Получение доступа в такой большой компании легко превращается в бюрократический квест. Но с точки зрения интерфейса и управления доступами все было реализовано здорово: понятное «единое окно», лаконичные инструкции, никакой путаницы. Человек всегда знал, куда нажать, а я как SOC-аналитик точно знал, где посмотреть выданные доступы, потому что система хранила все в одном месте, четко структурированном и стандартизированном виде. Это было одинаково удобно и пользователю, и команде безопасности.

Даниил Мирошник,

Руководитель направления SOC, Домклик

Идеальные PAM и MFA пользователь не замечает

Многие вендоры поддерживают идею, что идеальный пользовательский опыт систем управления доступом заключается в том, что работа с ними должна проходить просто и незаметно для пользователя.

MFA должна быть доступной для пользователя

Если смотреть с точки зрения пользователя, а их у нас почти миллион, гораздо больше, чем заказчиков, то для них мы предлагаем мобильное приложение, куда приходит push-уведомление, которое нужно просто подтвердить. По сути, это удобный второй фактор аутентификации.
В безопасности, помимо целостности и конфиденциальности, есть еще и доступность. К сожалению, многие специалисты по ИБ про доступность забывают. Решения, которые мы внедряем, точно не должны усложнять жизнь пользователям.

Валерий Аблеков,

Технический директор,
МУЛЬТИФАКТОР

Системы PAM должны быть незаметными для сотрудников

Идеальный пользовательский опыт выглядит так: специалист, начинающий работать через PAM, не должен ощущать никакой разницы по сравнению с работой без него. В первую очередь это касается количества этапов аутентификации. Если раньше человек заходил в систему буквально в два клика — условно, выбрал ресурс, ввел пароль и авторизовался, то с внедрением PAM все должно происходить точно так же легко. Не должно появляться никаких лишних промежуточных шагов, на которые тратится время. Второй ключевой момент — сохранность привычной функциональности.
Все задачи, которые пользователь выполнял до появления PAM, должны оставаться доступными и с ним. Любые возможности запуска автоматизаций и скриптов должны полноценно поддерживаться на уровне PAM-системы, а не ограничивать работу специалиста.

Артем Назаретян,

Руководитель
BI.ZONE PAM

Задача 2:

Контроль ИИ-агентов — вызов №1 для ИБ

Проблема управления доступом и идентификации ИИ-агентов является одним из самых обсуждаемых вызовов среди директоров по ИБ. Кроме того, что агенты наследуют классические «болячки» ТУЗов (технических учетных записей): сложность регулярной ротации паролей, отсутствие описаний, трудности с поиском реального владельца. Есть новые сложности: экспоненциальный рост агентов, недетерминированность поведения, размытие периметра ответственности и получение критических доступов, риск отказа в обслуживании и деградации систем, риск потери конфиденциальной информации.

> **Готовые стандарты контроля над ИИ-агентами на рынке отсутствуют**

Многие эксперты бьют тревогу и привлекают внимание к проблеме безопасности идентичности агентов. Мы в числе тех компаний, кто воспринимает этот вызов серьезно и ищет оптимальное решение. В плотном диалоге с командой ИТ по данному направлению мы прорабатываем возможные сценарии реализации аутентификации и управления Agentic Identities в связке с нашим Identity Provider, определяем область применения агентов, чтобы минимизировать потенциальный вред инфраструктуре. Однако необходимо в достаточно короткие сроки найти подходящее и технологичное решение для безопасного управления этим процессом, поскольку выгода для бизнеса от использования ИИ в ряде случаев достаточно ощутима. Связки систем IdP, IdM и IAM усложняются, и мы сейчас разрабатываем концептуальный подход к выстраиванию этих цепочек у себя.

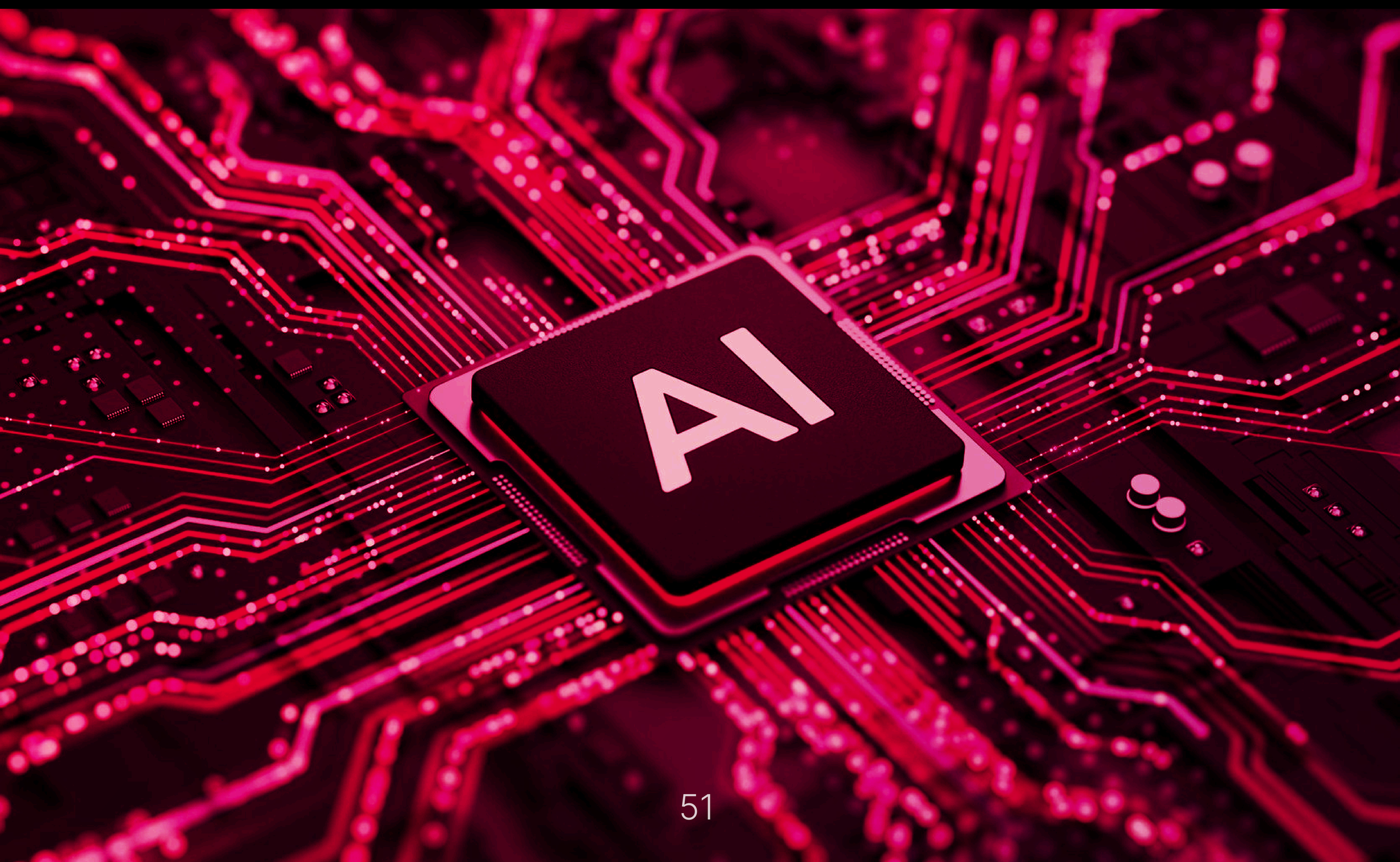
Антон Мелков,
Амбассадор Айдентити Клуба, Начальник управления крупного российского банка

ИИ-агенты при неверной настройке могут «задидосить» систему

Нам нужно рассматривать ИИ-агентов как еще одного полноценного сотрудника. Это один из самых серьезных рисков. Сейчас активно продвигаются low-code платформы и автоматизация рутины. Чтобы робот пошел, обработал или переложил данные в системах, ему нужны доступы. Сотрудники не находят ничего лучше, чем отдавать роботам свои личные учетные записи: «Он же просто имитирует мою деятельность». Есть серьезные риски неверной настройки. И речь даже не про ИБ, а про банальную производительность. У человека есть физическое ограничение по скорости работы. Робот делает запросы мгновенно и может «задидосить» целевую систему.

Андрей Нуйкин,

Начальник отдела обеспечения безопасности информационных систем, Евраз



39%

компаний на полюсах:

20%
запрещают ИИ-агентов

19%
не контролируют

Какой подход к контролю действий ИИ-агентов принят в организации?

Многие организации не выработали сбалансированного подхода к контролю ИИ-агентов. С одной стороны, в каждой пятой организации – полный запрет на использование, с другой – полная свобода. В трети компаний довлеет служба ИБ, требующая использовать ИИ-агентов в периметре.

* В категорию «Другое» попали ответы: не используются; только текстовые и бесплатные ИИ-агенты используются сотрудниками,
к остальным нет доступа; не запрещать ИИ-помощников полностью, так как они ускоряют рутинный анализ, но запрещать передавать чувствительные данные вовне и ограничивать использование облачных сервисов, логгировать все легитимные действия наравне с действиями сотрудников; отсутствует.

Корпоративный шлюз вместо запретов: как контролируют ИИ-агентов

Чтобы давать возможность сотрудникам безопасно использовать ИИ-агентов, компании контролируют конфиденциальность информации на сетевом шлюзе (подход Евраза), создают единый шлюз доступа и управление токенами (подход Домклика), ограничивают права (например, только на чтение или на ограниченный период времени).

Контроль конфиденциальности информации на сетевом шлюзе

К чему мы пришли на данный момент? Доступ к ИИ осуществляется строго через наш единый шлюз, где мы видим и контролируем весь трафик. У нас есть ИИ-подсказчик, обученный на наших ценных данных. Сотрудник может загрузить туда документ или текст запроса и узнать, содержится ли там конфиденциальная информация. Сейчас эту модель прикручивают прямо к прокси, чтобы все запросы пользователей автоматически проходили категоризацию и либо пропускали, либо предупреждали пользователя и т. д. Все идет к тому, что какие-то вещи будут отдаваться на откуп пользователям. Но разработчики настроены довольно жестко и не хотят отдавать создание агентов в «свободный полет». Их позиция — процесс должен напоминать установку софта на рабочий компьютер. Пользователь ведь не может сам установить приложение — он пишет заявку в техподдержку. С агентами хотят сделать так же: хочешь автоматизацию через агента — пиши заявку, и тебе дадут эту возможность.

Андрей Нуйкин,

Начальник отдела обеспечения безопасности информационных систем, Евраз

Чтобы контролировать ИИ-агентов, надо возглавить процесс их использования

Мы используем LiteLLM — это open-source решение, с помощью которого обеспечиваем доступ как к нейросетям, развернутым во внутренней инфраструктуре, так и к внешним коммерческим LLM-провайдерам. Для нас это основной элемент управления доступом в рамках Identity & Access Management в контексте работы сотрудников с ИИ-агентами и LLM. В этом решении контролируются токены доступа и определяется, к каким именно моделям конкретный человек имеет право подключаться. Пока идет борьба с теневым ИИ, главное, что мы можем сделать, — предложить сотрудникам максимально удобный корпоративный сервис. Лучше хранить один токен от корпоративного LLM-прокси, чем самостоятельно держать десятки ключей от разных сервисов. Через единую точку доступа сотрудник получает доступ к разрешенным ему внутренним моделям и моделям внешних коммерческих LLM-провайдеров. Мы транслируем пользователям простой месседж: «Зачем вам покупать что-то свое и применять Shadow AI? Мы уже все купили, настроили и развернули за вас». Около трети сотрудников в Домклик уже используют агентов на своем рабочем устройстве, и мы стараемся увеличивать эту долю.

Даниил Мирошник,

Руководитель направления SOC, Домклик

Учетка ИИ-агента — не ТУЗ: делегирование и доступ «на один запрос»

В отличие от классической сервисной учетной записи, учетная запись ИИ-агента предполагает делегирование полномочий инициатора, позволяя действовать от имени запустившего его человека. Кроме того, ИИ-агента невозможно зарегистрировать в системе заранее с постоянными правами — его авторизация и доступ происходят краткосрочно непосредственно в момент обращения.

Ключевой вызов — это контроль механизма делегирования полномочий

В чем принципиальное отличие учетной записи автономного ИИ-агента от обычной сервисной учетной записи? ИИ-агенту делегируются полномочия инициатора — человека, который его запускает, и агент начинает действовать от его имени. То есть в логике ИИ появляется элемент делегирования. Инструменты контроля должны развиваться в сторону управления частичным или полным делегированием полномочий. Нужна система, которая будет контролировать доступ агентов к ресурсам и данным в строгом соответствии с установленными политиками — невзирая на то, какими повышенными правами обладает сам человек. С ИИ-агентами есть и другая серьезная проблема. Работа агента автономна: он перерабатывает огромные объемы информации и может случайно найти реквизиты доступа внутри самих данных. Это создает риск того, что агент попытается ими воспользоваться и выйдет за рамки предусмотренной «песочницы».

Андрей Лаптев,
Директор по продуктовому развитию, Индид

Динамическая авторизация и управление согласиями

Ключевые отличия здесь уже понятны. В традиционном IAM для людей система заранее знает, какие приложения с ней взаимодействуют. В случае с ИИ-агентами история совершенно другая. Мы не можем полагаться на то, что для каждого такого агента будут выделяться индивидуальные секреты, которые потом придется обновлять и поддерживать в актуальном состоянии. Агента нужно регистрировать фактически в момент его обращения, а само взаимодействие с ним носит краткосрочный характер. Второй важный момент касается управления согласиями (consent management). Если сейчас пользователь вошел в систему и мы считаем, что все дальнейшие действия совершает именно он (а приложение может иметь даже некоторый избыток полномочий), то с агентами эта логика рушится. Из-за того, что ИИ-агенты могут галлюцинировать и делать чуть больше, чем от них ожидает человек, гранулярное управление разрешениями становится критически важным.

Михаил Ванин,
Генеральный директор, Identity Blitz

IAM для агентов и Just-in-Time: что готовят вендоры

Вендоры планируют контролировать ИИ-агентов с помощью специализированных шлюзов (AI-proxy/Credential Broker), которые скрывают постоянные ключи доступа, ведут сквозное логирование и привязывают агента к человеку-куратору с возможностью экстренной блокировки. Также предлагается полностью отказаться от постоянных полномочий в пользу динамического (Just-in-Time) выделения минимальных краткосрочных прав под конкретную операцию с их мгновенным уничтожением.

Принцип наименьших привилегий для ИИ-агентов

С нашей стороны в части Identity Security ключевая задача — четко понимать, в чьих интересах работает конкретный агент, и ограничить его в правах уровнем не выше, чем у запустившего его лица или группы лиц. При этом критически важно сделать так, чтобы агент не мог использовать полученный доступ повторно вне рамок текущей задачи. По сути, речь идет о краткоживущих цифровых идентичностях с on-demand provisioning — динамическим созданием самого идентификатора и необходимых прав доступа под конкретную задачу. Наша основная рекомендация: агенты не должны иметь постоянных идентичностей и накапливать права. Они должны получать доступ строго в рамках полномочий запустившего их субъекта, и в идеале именно этот субъект должен определять границы прав агента.

Александр Махновский,

Технический директор,
Аванпост

IAM/IGA для ИИ-агентов

Сейчас инженерная мысль крутится вокруг ИИ-прокси — это инструменты от разработчиков для разработчиков. Но рынку нужен инструмент, задающий правила игры между безопасниками, бизнес-пользователями и самими агентами. Управление доступом агентов взлетит только тогда, когда появится полноценный IAM для агентов. Что он собой представляет? Для безопасности это рабочее место, где виден полный реестр агентов, статус их одобрения, маршруты, а также реализовано управление доступом агентов к MCP-серверам и инференсу. У специалиста по безопасности есть отчеты, интеграция с SIEM и DLP (где в логах фиксируется идентичность как агента, так и его куратора) и «стоп-кран» для моментальной блокировки любого агента. Для бизнеса и разработки это понятный реестр одобренных ИБ агентов-субъектов и ресурсов (модели, MCP, тулы).

Алексей Хмельницкий,

Генеральный директор,
RooX

Задача 3:

Организация процесса управления доступом

Кто в вашей организации является основным владельцем процесса управления доступом (учетными записями)?

Владельцем процесса управления доступом может быть примерно в равной степени как департамент ИТ, так и ИБ.

* В категорию «Другой вариант» попал ответ: бухгалтерия.

80%

компаний закрепили управление доступом **за ИБ (40,5%) или ИТ (39,5%)**

ИБ — методолог ИТ — исполнитель: как разделить процесс

Эксперты подчеркивают, что процесс управления доступами должен быть разделен между подразделениями ради общей эффективности.

Разделение контроля и исполнения

Как отмечают руководители, ИБ должна выступать методологом и заказчиком процесса, а ИТ-служба — владельцем и исполнителем на уровне систем. Также заказчиками могут быть бизнес-подразделения, а исполнителем – подразделение в HR-отделе, связанное с HR Tech.

Разделение прикладного и сетевого уровня

Подготовка универсальных ИБ-специалистов, которые одинаково хорошо ориентируются в бизнес-ролях систем и сетевых протоколах, требует значительных ресурсов. На практике эффективнее распределять эти задачи между специалистами с разными профилями компетенций.

Мы находимся в блоке пользовательского опыта сотрудников и делаем сервисы и продукты именно для внутреннего использования. До этого я работал в ритейл-компании, и там все было сконцентрировано внутри нашей команды ИБ: мы сами формулировали требования, разрабатывали и все согласовывали. Такая схема вполне жизнеспособна, но в VK она неактуальна. Если мы станем сами ИБ-специалистами, то потеряем внешнего заказчика и начнем делать продукт «для самих себя». А значит, уйдет главная идея — выполнение реальных требований безопасности, приходящих к нам извне.

Игорь Зверев,

Руководитель отдела автоматизации и управления доступами, VK

У нас есть пользовательский доступ на прикладном уровне (права в приложениях, роли администратора или сопровождения), а есть сетевой доступ (порты, протоколы, маршрутизация «точка-точка»). Этим занимаются два разных подразделения. Раньше я хотел их объединить в одно, потому что была следующая проблема. Устраивается, например, аналитик. Ему нужен доступ к базам. Он создает заявку, мы ее согласуем. Человек пытается зайти в систему — и не может, потому что сетевого доступа нет. Он идет во второе подразделение, где ему задают вопросы о портах и протоколах подключения, но у пользователя может не быть таких технических знаний. Но если объединять этих специалистов в одну роль, мы столкнемся с тем, что грамотный специалист обойдется слишком дорого. Человеку, понимающему сетевые протоколы и читающему кипы документов по безопасности, будет неинтересно согласовывать обычные роли пользователей.

Николай Черенков,

Руководитель отдела сопровождения процессов информационной безопасности, Банк Синара

Минус один согласующий:

решение о доступе — за владельцем системы

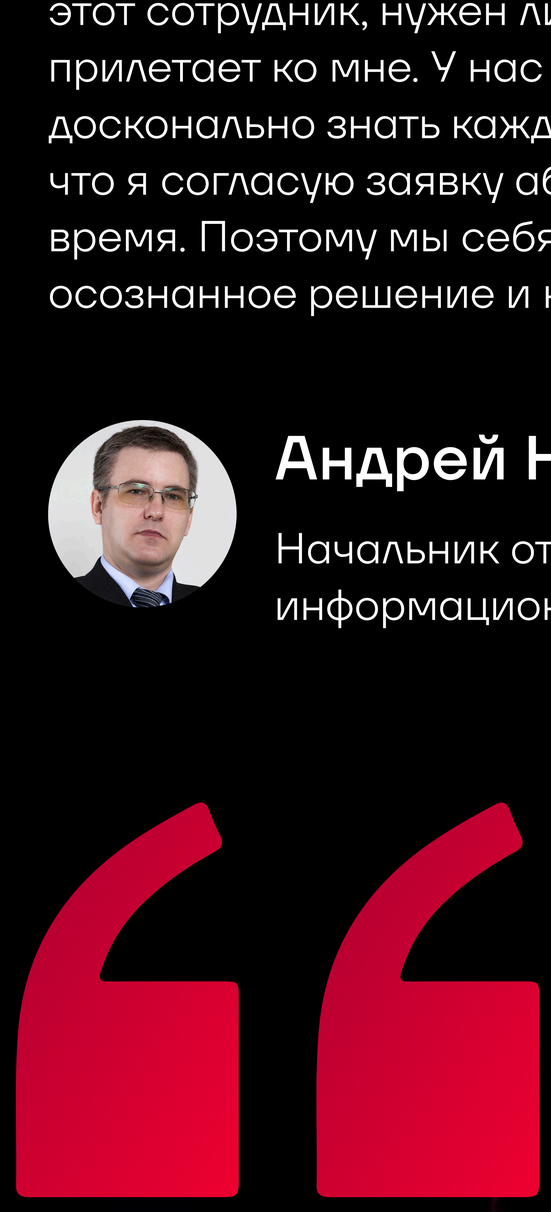
Решение о предоставлении конкретных прав внутри приложения должен принимать исключительно владелец этого бизнес-ресурса (или непосредственный руководитель сотрудника), который понимает реальный контекст и обязанности пользователя

Сотрудники ИБ физически не могут знать внутреннюю архитектуру сотен прикладных систем компании (таких как 1С или SAP) и определять критичность каждого действия внутри них. Согласование заявок безопасниками «вслепую» лишь создает иллюзию контроля и размывает ответственность.

У нас в какой-то момент в цепочке согласования доступов были и служба безопасности, и ИБ, и владельцы систем, и прямые начальники. Но когда мы начали глубоко погружаться в этот процесс, возникли логичные вопросы. Например, человек запрашивает доступ в SAP, чтобы что-то посмотреть. Есть владелец этой системы или конкретного модуля. Когда к нему приходит заявка, он понимает, кто этот сотрудник, нужен ли ему доступ и можно ли его туда пускать — здесь логика есть. Затем заявка прилетает ко мне. У нас огромная инфраструктура, сотни систем — естественно, я не могу досконально знать каждую из них и понимать, где там ценные данные, а где нет. В итоге получается, что я согласую заявку абсолютно вслепую. Зачем? Это просто лишний шаг, который растягивает время. Поэтому мы себя из этой цепочки убрали. Остался владелец системы, который принимает осознанное решение и несет за него ответственность.

Андрей Нуйкин,

Начальник отдела обеспечения безопасности информационных систем, Евраз



52,5%

компаний считают себя зрелыми но быстро выдают права лишь **28,5%**

Как вы оцениваете уровень зрелости организации с точки зрения безопасности учетных записей?

12%

Начальный:

пароли записаны на стикерах, права выдаются по звонку администратору, учетки уволенных сотрудников остаются в системе месяцами

35,5%

Базовый:

появился MFA на внешнем контуре, подключен PAM для контроля администраторов и подрядчиков, есть базовые регламенты

46,5%

Стандартизированный:

процессы автоматизированы, права выдаются по ролям, работает единый вход (SSO)

6%

Стратегический:

реализована концепция нулевого доверия (Zero Trust), решения принимаются автоматически на основе контекста и искусственного интеллекта

Почти половина респондентов оценивают зрелость защиты учетных записей в своих организациях выше среднего, что закономерно при оценке собственной компании.

1,5–2

часа на онбординг — ориентир зрелой компании

Уровень зрелости оценивается также с помощью объективных метрик. Ключевая из них, с точки зрения экспертов, это время онбординга сотрудника. Как мы видели ранее, у большинства компаний оно занимает более одного дня, а не 1,5–2 часа.

01
Скорость и операционная эффективность

- Время онбординга и скорость предоставления доступа (1,5–2 часа)
- Своевременность отзыва прав
- Соблюдение SLA

02
Экономические результаты

- Снижение нагрузки на ИТ-службу
- ROI: сопоставление затрат на собственную разработку или покупку решения с выгодами от ускорения бизнес-процессов

03
Покрытие бизнес-процессов

- Процент покрытия бизнес-ролями VS количество заявок
- Автоматизация – процент учетных записей, созданных или заблокированных без участия администраторов

04
Показатели безопасности

- Отсутствие инцидентов
- Количество «бесхозных» учетных записей: активных аккаунтов, не имеющих владельца или не используемых долгое время (например, более 3 дней)
- Результаты пентестов и аудитов
- Минимизация избыточных прав

05
Качество процессов

- Поведенческий анализ – способность детектировать аномалии
- Регулярность инвентаризации
- Контроль привилегированных пользователей по Just-in-Time (JIT)

Задача 4:

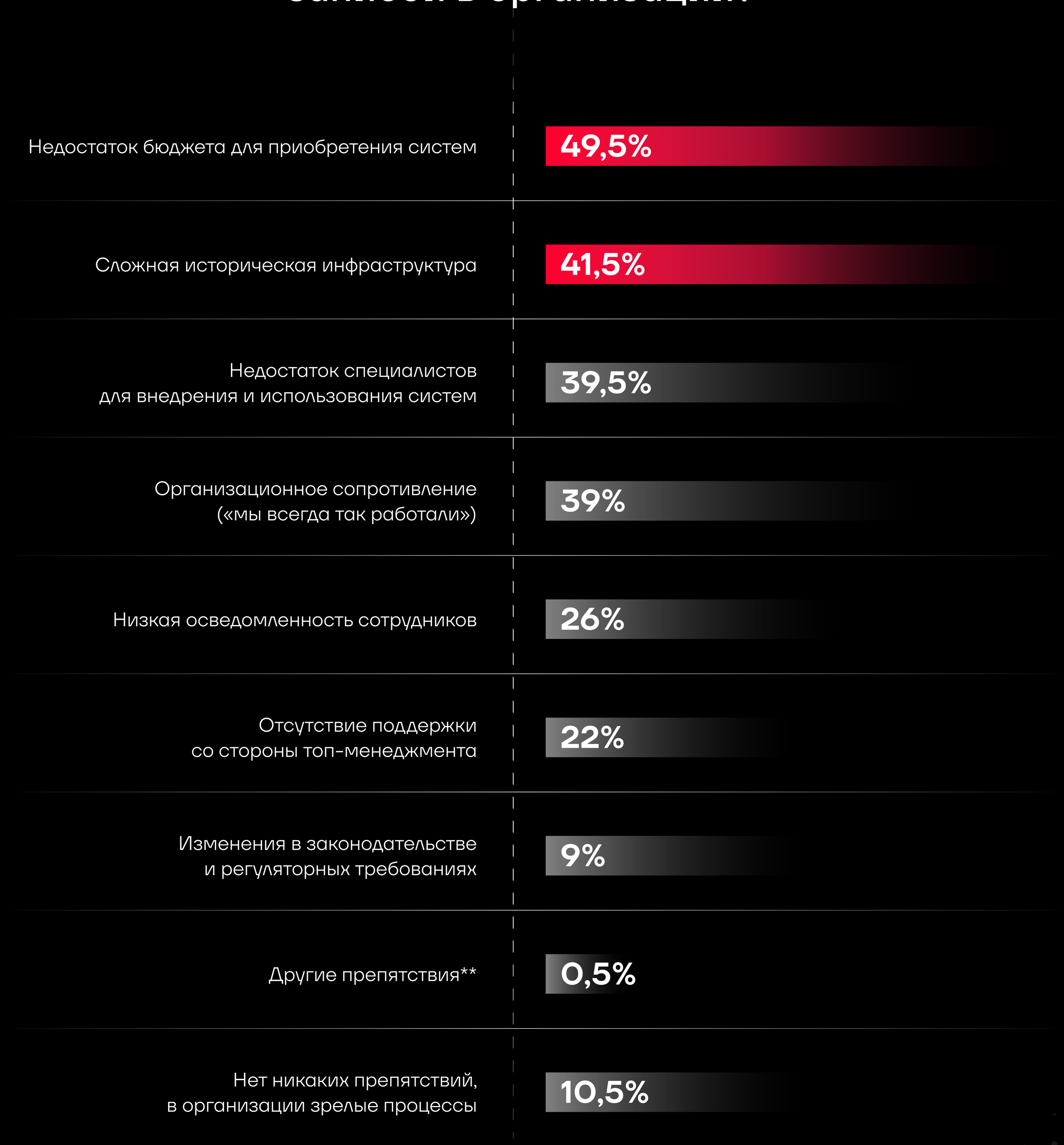
Рост эффективности затрат

49,5%

компаний упираются в бюджет — главный барьер зрелости

Недостаток финансов – ключевой барьер для повышения зрелости управления учетными записями. Также критичными являются сложность инфраструктуры, недостаток специалистов и организационное сопротивление.

Что является главными барьерами для повышения зрелости управления и безопасности учетных записей в организации?*



* Сумма превышает 100%, так как респонденты могли выбрать несколько вариантов ответа.
** В категорию «Другие препятствия» попал ответ: недостаточная автоматизация JML и ролевой модели, слабая интеграция IdM с HR-системами и другими источниками данных, отсутствие системного подхода к управлению привилегированными доступами.

Дорого, долго, неудобно: барьеры даже у лидеров рынка

Эксперты из крупных компаний называют такие же барьеры: высокая стоимость решений, исторически накопленный хаос в правах и инфраструктуре, дефицит компетенций, сопротивление ИТ-служб и культурные барьеры пользователей.

Барьеры внедрения IdM — недостаток денег и времени на описание процессов

Полноценного IdM у нас нет. У нас внедрены отдельные связанные процессы: например, тот же MIM, который рулит созданием и блокировкой учетных записей. Учетные записи создаются по заявкам, права меняются и согласуются точно так же через заявки.
К внедрению IdM мы двигаемся, но очень медленно. Причина простая: IdM — это долго, дорого и сложно. Купить лицензию и развернуть сервер — это элементарно. Самое интересное начинается потом, когда нужно заводить и описывать процессы. Тут возникают два пути: наводить порядок в системах и разрабатывать ролевую модель своими силами или нанимать интегратора, который сделает это за нас (а это стоит денег). Мы осознаем, что система нам нужна и она действительно полезна, но пока думаем, по какому пути идти.

Андрей Нуйкин,
Начальник отдела обеспечения безопасности информационных систем, Евраз

Основным препятствием внедрению PAM стала корпоративная культура

Первая проблема — стоимость. По мере внедрения PAM растет не только стоимость инфраструктуры: при сессионной модели лицензирования увеличение числа одновременных подключений означает и необходимость регулярно докупать concurrent-лицензии. Вторая проблема — нагрузка на инфраструктуру. С ростом числа пользователей качественно и количественно выросла нагрузка на саму систему. Решение приходится масштабировать, а это снова означает дополнительные расходы и увеличение инфраструктуры, которую нужно поддерживать. Третья проблема — корпоративная культура и изменение привычек пользователей. Пользователи оказались совершенно не готовы к тому, что их прямое сетевое подключение «зарежут» и заставят ходить строго через PAM. Мы осмелились принять это решение — полностью забрать прямой доступ и перевести всех в PAM. Но если людям неудобно, они всегда будут искать обходные пути, обманывать систему и пытаться вернуться к привычным сценариям работы. Поэтому мало просто технически закрыть прямой доступ — нужно еще сделать так, чтобы новый сценарий работы был понятным и удобным.

Даниил Мирошник,
Руководитель направления SOC, Домклик

48,5%

недовольны ценой отечественных решений

Что вас больше всего не устраивает в отечественных решениях?*

48,5%	Высокая стоимость
36%	Недостаток технических специалистов, разбирающихся в решениях
35,5%	Незрелость новых версий
34%	Низкая гибкость и сложность кастомизации
31,5%	Долгая обратная связь и проблемы со скоростью техподдержки
24,5%	Несоответствие реальным нагрузкам enterprise-уровня
18,5%	Отсутствие готовых коннекторов
1%	Другое**
7%	Все устраивает

\+ Высокая стоимость является главной претензией специалистов организаций к решениям отечественных вендоров.

* Сумма превышает 100%, так как респонденты могли выбрать несколько вариантов ответа.
** В категорию «Другое» попал ответ: не всегда есть «обратная совместимость» с уже внедренными зарубежными решениями.

57%

респондентов оценивают
российские продукты на уровне зарубежных или выше

Как вы оцениваете качество отечественных решений для безопасности учетных записей относительно зарубежных аналогов?

52,5%
Примерно на одном уровне с зарубежными решениями

41,5%
Уступает качеству зарубежных решений

4,5%
Превышает качество зарубежных решений

1,5%
Другое*

* В категорию «Другое» попали ответы: не знаю (2 ответа); дорого.

1–3 года

Окупаемость и как обосновать бюджет

Самым популярным способом обоснования покупки решений является привязка к обязательным требованиям регуляторов. Компании, которые уже обеспечили базовую защиту, используют также:

Апелляция к бизнес-целям и решение реальных «болей» бизнеса

Бизнесу нецелесообразно продавать «абстрактную безопасность» — ему нужно предлагать скорость, стабильность и повышение производительности труда. Обосновать покупку легче, если показать, что инвестиции помогут бизнесу быстрее запускать новые точки, склады или нанимать персонал (как в Ламода).

Финансовый расчет окупаемости (ROI)

Компании рассчитывают окупаемость систем, переводя время простоя сотрудников в конкретные финансовые потери. Если компания выбирает между покупкой готового решения и собственной разработкой, проводится детальный расчет совокупной стоимости владения. Окупаемость инвестиций в покупку или доработку обычно рассчитывается на горизонте от 1 до 3 лет.

Мы ежегодно рассчитываем время с момента трудоустройства сотрудника до момента получения им доступов. Если IdM интегрирован с целевой системой, он моментально определяет положенный по бизнес-роли доступ и в течение нескольких минут автоматически предоставляет его, отправляя уведомление. Это первый вектор. Второй вектор — это когда IdM не интегрирован с системой, но есть заявка. Сюда входит время, которое пользователь тратит на то, чтобы разобраться с IdM, найти нужные доступы, оформить заявку и дождаться ее согласования администраторами. Кроме того, мы закладывали в оценку окупаемости IdM и клиентские риски. Если операционист сидит в офисе, а перед ним стоит клиент, пока сотрудник мается с оформлением заявки и не может зайти в систему — банк несет прямые репутационные и финансовые риски.

Николай Черенков,

Руководитель отдела сопровождения процессов информационной безопасности, Банк Синара

«Лайт»-версии, SaaS, новая архитектура: как вендоры снижают цену

Для решения проблемы высокой стоимости вендоры предлагают продукты только с ключевыми функциями, запускают облачные SaaS-модели, упрощают интеграционную архитектуру.

Вместо масштабирования PAM можно купить менеджер паролей

PAM-система обходится намного дороже, чем менеджер паролей. Даже если расширять уже существующую PAM-систему, это все равно потребует несоизмеримо больших денег по сравнению с покупкой менеджера паролей. По своей сути менеджер паролей — это лишь одна из составных частей PAM-системы. Поводом серьезно задуматься о внедрении менеджера паролей часто становятся выявленные, в том числе представителями регуляторов, замечания в соблюдении парольной политики. При этом 100% покрытие сотрудников компании — довольно редкая история. Как правило, менеджеры паролей внедряют не на всех офисных сотрудников подряд, а фокусируются в первую очередь на ИТ-специалистах и административном персонале.

Вячеслав Макович,

Директор по маркетингу
и развитию, АБП2Б

Более низкой цены можно добиться за счет иной архитектуры решения

Иногда дешевле сделать не ту же систему с меньшим количеством функций, а вообще по-другому ее спроектировать. Например, мы объединили IAM и IDM в одной платформе, вместо того чтобы строить два отдельных контура и затем синхронизировать их между собой. Такой архитектурный подход позволяет убрать часть сложных интеграций и снизить совокупную стоимость решения без отказа от ключевой функциональности. При этом мы сознательно отказались от части функций, которые есть в классических IDM-системах, но используются далеко не всеми заказчиками. В результате наше решение действительно не во всем похоже на традиционный IDM — и это как раз принципиальный момент. Мы не пытались воспроизвести классический IDM со всеми его возможностями.
Мы переосмыслили архитектуру и оставили то, что действительно нужно заказчику для управления доступом.

Алексей Хмельницкий,

Генеральный директор,
RooX

Быстрый результат по ROI: начинать с критичных систем

Автоматизируя самые критичные системы на первом этапе, CISO может быстро показать руководству реальную экономию («быстрый результат на ROI») и под этот доказанный эффект получить бюджет на масштабирование проекта. ROI-подход может использоваться не только для обоснования покупки IdM, но и других продуктов управления доступом.

Использование международного опыта для оценки ROI

Для CISO важно получить измеримый результат уже на первом этапе проекта. Поэтому мы используем расчет ROI: сначала автоматизируем наиболее критичные системы, а затем показываем бизнесу экономический эффект. Когда результат выражен не только в повышении безопасности, но и в конкретной экономии времени и ресурсов, значительно проще обосновать дальнейшее развитие IDM. Наша методика опирается на международный опыт оценки эффективности подобных проектов. Мы оцениваем трудозатраты на ручное управление доступом, стоимость рабочего времени сотрудников, затраты на создание и изменение учетных записей, а также риски, связанные с соблюдением комплаенс-требований. Затем сравниваем эти показатели с автоматизированным процессом. Например, если раньше выдача учетной записи занимала час, а после автоматизации — несколько минут, эту разницу можно перевести в стоимость рабочего времени. Дополнительно рассчитывается совокупная стоимость владения (TCO) на горизонте 3–5 лет. В итоге заказчик получает наглядную экономическую модель и может оценить срок окупаемости проекта.

Александр Давыдов,

Менеджер продукта Ankey IDM,
Газинформсервис

ИБ-специалисты должны говорить на языке бизнеса

ИБ исторически всегда была отделена от ИТ. Но на самом деле любое ИТ-решение изначально должно подразумевать безопасность. Это разделение искусственно и давно должно быть стерто: если мы умеем считать эффективность ИТ-решений, то с тем же успехом можем оценивать средства ИБ в совокупности с ИТ, оптимизируя бизнес-процессы и снижая риски. Главная задача современного CISO это уметь считать собственный ROI и общаться с бизнесом на его языке. Он приходит и говорит: «Нам необходимо 50 миллионов, и все будет хорошо». — «А что именно будет хорошо?» — «Ну, ничего не упадет». — «А оно сейчас падает?» — «Нет, не падает». — «Зачем тогда 50 миллионов?» Любое средство ИБ это не что-то «сбоку», а часть единого ИТ-подхода, инструмент, который хоть и не зарабатывает деньги бизнесу напрямую, но отлично их экономит. И именно это надо научиться считать современному CISO.

Константин Родин,

Заместитель директора
по развитию бизнеса,
АйТи Бастион

От продуктов к экосистеме: как сократить отставание

Российские вендоры признают частичное отставание от западных решений в развитии облачных сценариев, глобальных стандартов и комплексных продуктовых экосистем, связывая это с тем, что отечественные разработчики не находятся на международном технологическом фронтире. В то же время они подчеркивают, что в локальном сегменте российские продукты не уступают западным.

Изоляция от мирового рынка является возможностью для закрытия уникальных локальных потребностей

С одной стороны, наши решения отчасти отстают, потому что нужно признать: мы не находимся на мировом технологическом фронтире. Мы массово не участвуем в международных комитетах, которые разрабатывают глобальные стандарты и спецификации для мировых вендоров. С другой стороны, российский рынок информационной безопасности довольно изолирован, и у него есть своя уникальная специфика. В зарубежных продуктах наши локальные требования изначально не поддерживаются — для глобального рынка они просто неактуальны или там привыкли решать подобные задачи иначе. В этом отношении отечественные продукты часто оказываются даже более развитыми. Мы можем сразу, «из коробки», учесть специфические потребности российского бизнеса: от интеграции с ЕСИА и Госуслугами до поддержки отечественной криптографии.

Михаил Ванин,

Генеральный директор, Identity Blitz

От отдельных решений — к целостной экосистеме продуктов

Я вижу тренд развития российских решений в сторону экосистемы, и мы двигаемся в том же направлении. У нас есть свой флагманский продукт. Если сравнивать наш модуль 2FA с зарубежными аналогами, то функционально они более-менее равны. Но если сравнивать нас в масштабе целостной экосистемы с Microsoft Azure или Cisco Duo, то это пока немного разные миры. Зарубежные решения работают в комплексе, и это именно то, к чему мы стремимся. Нашей основой должна стать служба каталогов MULTIDIRECTORY. Она станет центром, вокруг которого будут объединяться остальные продукты. В первую очередь это SSO — функциональность, которую заказчики очень часто запрашивают, но пока по каким-то причинам опасаются внедрять. Мы хотим дать рынку единую точку управления пользователями и удобный вход во все корпоративные системы.

Валерий Аблеков,

Технический директор, МУЛЬТИФАКТОР

15 ключевых фактов Identity Security

Рынок и технологии

17 Млрд ₽
объем рынка Identity Security в 2025 году

34,6%
рынка приходится на PAM — крупнейший сегмент

+16%
рост IdM/IGA — самый быстрый среди PAM, IdM и MFA

69,5%
компаний используют MFA

36%
покрыли MFA всех сотрудников и системы

64,5%
контролируют администраторов регламентами, а не PAM

45,5%
выдают права бессрочно

24%
используют специализированную IdM

2026

Процессы и барьеры

71,5%
выдают права новичку рабочий день и дольше

87,5%
сталкивались с инцидентами вокруг учетных записей

43,5%
пострадали от ошибок администраторов — инцидент №1

39%
либо запрещают ИИ-агентов, либо не контролируют их

80%
закрепили управление доступом за ИБ или ИТ

49,5%
называют главным барьером нехватку бюджета

57%
оценивают российские решения не ниже зарубежных

Индид × Айдентити Клуб

Исследование проведено компанией «Индид» совместно с Айдентити Клубом при участии представителей российских компаний и экспертов в области информационной безопасности.

Благодарим всех участников исследования за вклад в формирование целостного представления о сегменте Identity Security в России.

© 2026 Индид. Все права защищены.