Ростелеком
Солар

Исследование «Молчание IdM, или Готовы ли российские компании решать задачи управления доступом?»

Май 2021 года

Содержание

0 Аналитический отчет 3

1 Введение 3

2 Ключевые цифры 4

3 Профиль респондентов, принявших участие в исследовании 5

4 Текущая ситуация с автоматизацией процессов управления доступом в российских компаниях 6

5 Готовность к автоматизации 8

6 Наличие инцидентов ИБ, связанных с правами доступа 10

7 Использование технологии DCAP и контроль неструктурированных данных 10

8 Выводы и рекомендации 14

9 О нас 15

0. Аналитический отчёт

В данном отчёте рассмотрим текущее состояние и перспективы развития отечественной отрасли управления доступом на основании аналитического исследования российских компаний, проведённого Центром компетенций управления доступом «Ростелеком-Солар».

1. Введение

Число пользователей в компаниях и организациях непрерывно растёт. Разрастается и модернизируется ИТ-ландшафт каждого предприятия. Этот рост вызван сочетанием различных факторов: от цифровой трансформации до изменения категорий пользователей и появления множества различных устройств, которые используются для доступа к ресурсам компании.

В то же время повышается и риск возникновения нарушений, связанных с управлением и предоставлением доступа к ресурсам и активам компании. Эти нарушения могут происходить на разных фронтах: не только через проникновения внешних злоумышленников во внутренний контур предприятия, но и через ошибки или злоупотребления правами доступа внутренних сотрудников компании. И от того, насколько компании готовы к вызовам – от разработки соответствующих политик и процедур, от технической реализации этих политик – зависит уровень рисков информационной безопасности компаний.

Целью исследования является определение уровня зрелости российских организаций в вопросах управления доступом, а также определение текущей готовности компаний к внедрению средств автоматизации, включая решения класса IdM.

2. Ключевые цифры

20% опрошенных компаний в 2020 году регистрировали инциденты, связанные с правами доступа. При этом 46% указали на их среднюю/высокую критичность.

Ни один респондент (!) не отметил наличия в компании полной автоматизации в системах управления доступом. Более 50% отметили наличие частичной автоматизации.

56% опрошенных высказали полную неудовлетворенность либо среднюю удовлетворенность существующей в компании системой управления доступом (58% в частных компаниях, 52% в государственных).

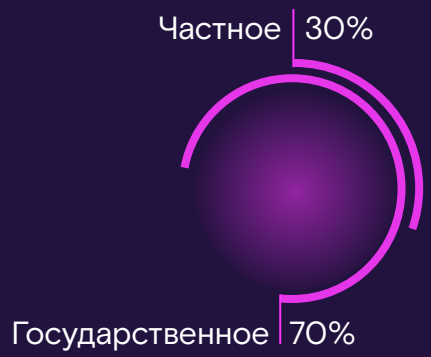
Среди основных причин низкой удовлетворенности существующей системой управления доступом отсутствие инструментов контроля (указали 66% недовольных текущей системой управления доступом) и высокая загрузка ИТ-персонала (отметили 40% недовольных).

Более 40% респондентов готовы автоматизировать процессы управления доступом, госструктуры выражают бОльшую готовность (47% vs 43% в коммерческом секторе)

3. Профиль респондентов, принявших участие в исследовании

По форме собственности респонденты разделились на частные и государственные организации в соотношении 70%/30% - с примерно аналогичным делением по отношению к субъектам КИИ (критической информационной инфраструктуры). Наибольший процент участников исследования был представлен отраслями: Информационных технологий и коммуникаций, Финансово-кредитными организациями, Промышленностью/Добычей полезных ископаемых/Энергетикой, Государственными организациями и Наукой/Образованием. Многие из них имеют развитую филиальную сеть. Примерно у половины опрошенных головной офис расположен в двух столицах, у остальных – в регионах. Размер организаций варьировался в пределах от 250 до 20000 рабочих станций (хостов).

Форма собственности



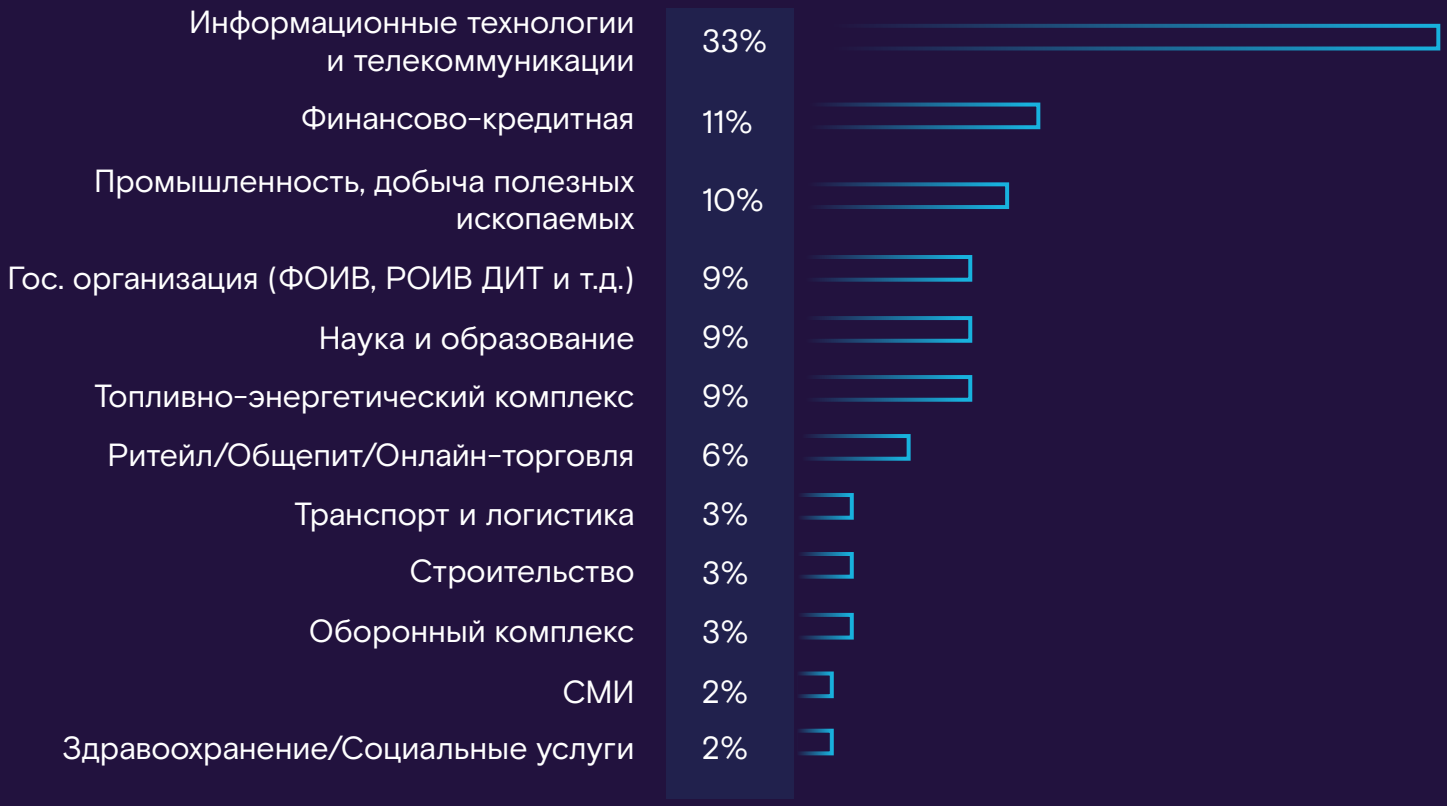
Количество филиалов

~10 среднее количество филиалов в компаниях респондентов

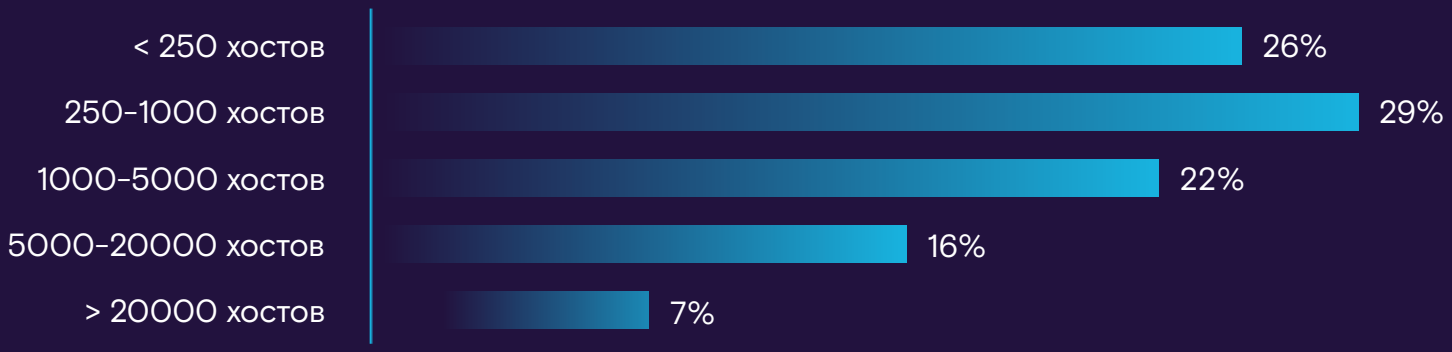
Город

Субъект КИИ

Отрасль организации



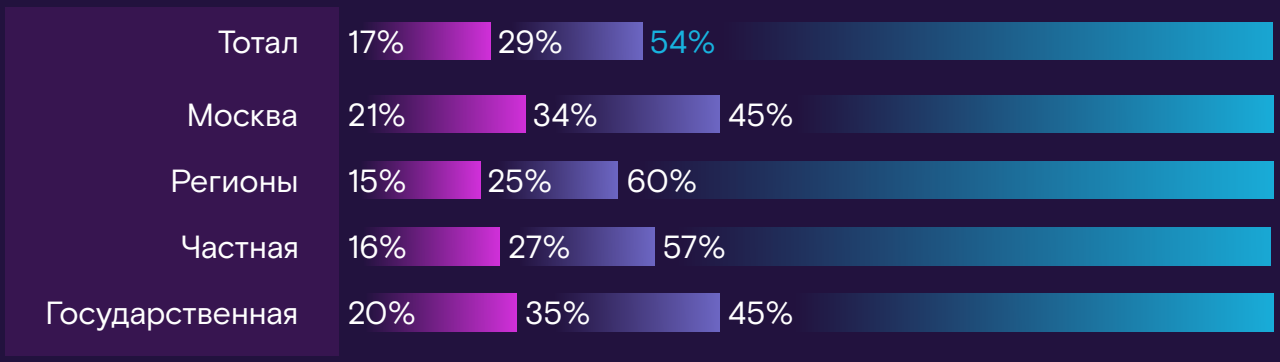
Размер организации



4. Текущая ситуация с автоматизацией процессов управления доступом в российских компаниях

Ни один из респондентов не отметил присутствие полной автоматизации в системах управления доступом. Более 50% отметили наличие в компании частичной автоматизации.

Система управления доступом в компании

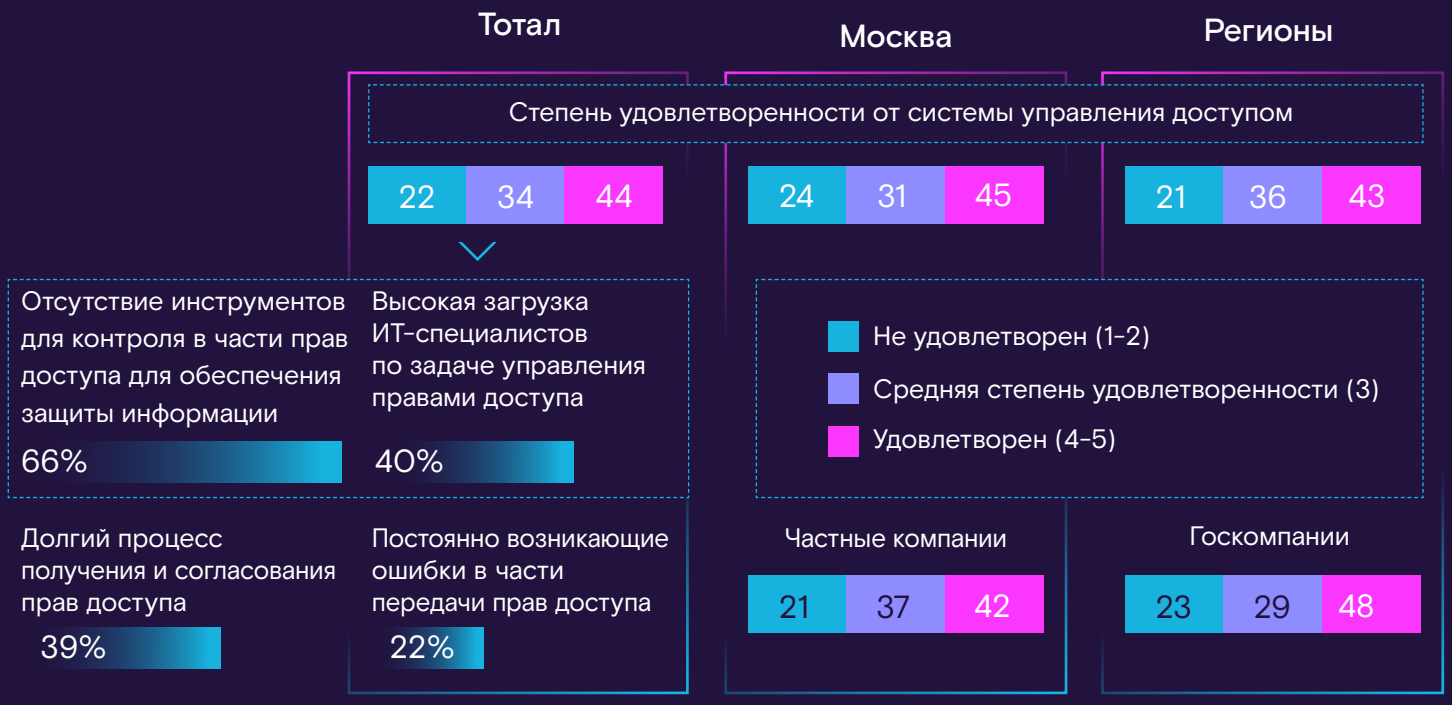


- Нет регламента (прописанных процессов выдачи прав доступа), а также аудита и контроля
- Есть регламент по правам доступа, нет технических средств его реализации (не автоматизированы процессы). Отсутствует аудит и контроль
- Есть регламент по правам доступа, частичная автоматизация непрофильными программными средствами. Отсутствует аудит и контроль

При этом 56% опрошенных высказали полную неудовлетворенность либо среднюю удовлетворенность существующей в компании системой управления доступом, причем этот показатель несколько выше в частных компаниях (58%), чем в государственных (52%).

Среди основных причин низкой удовлетворенности – отсутствие инструментов контроля (указали 66% недовольных текущей системой управления доступом) и высокая загрузка ИТ-персонала (отметили 40% недовольных).

Удовлетворенность текущей системой управления доступом

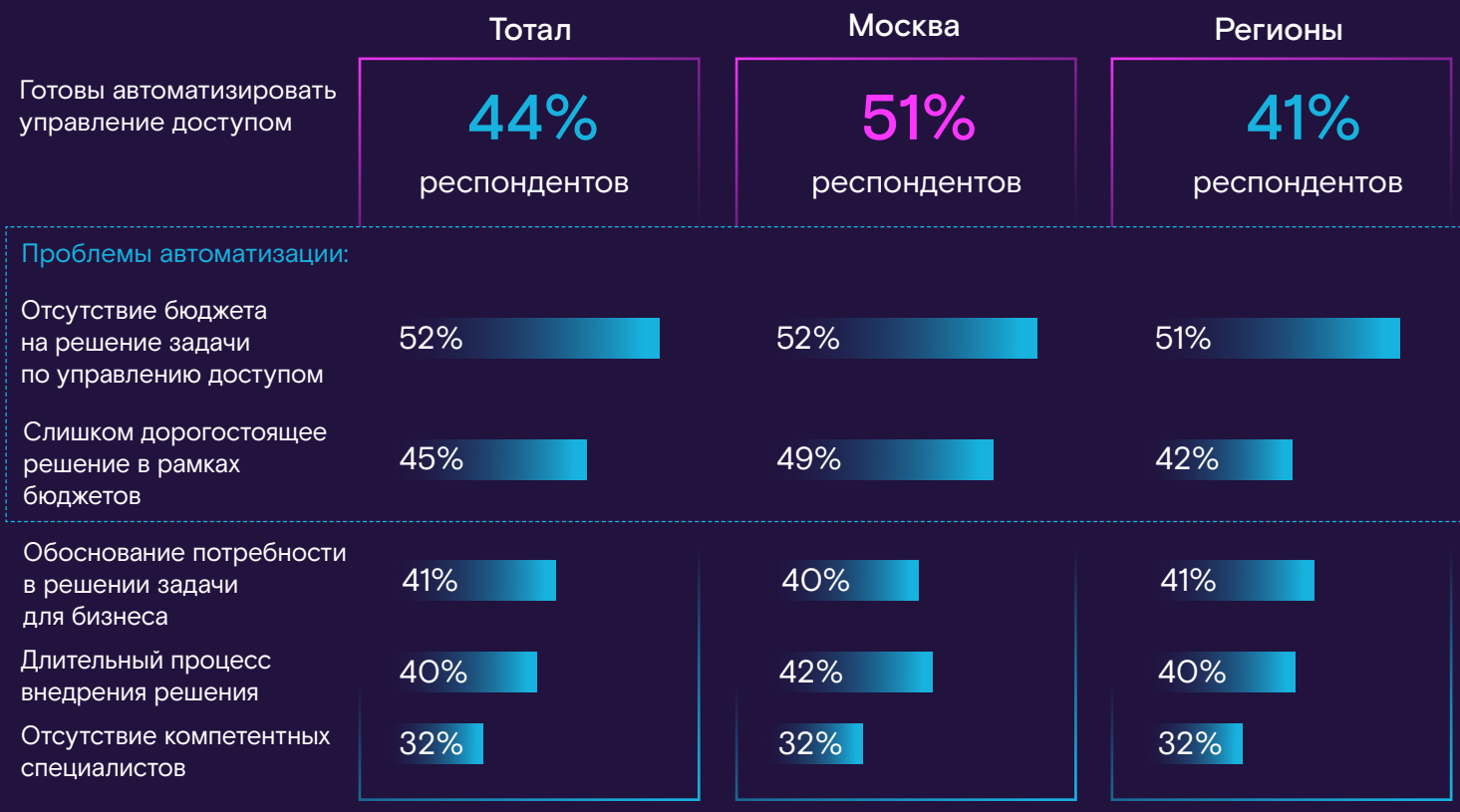


«Частичная автоматизация хоть и закрывает ряд задач, связанных с заменой ручного труда в процессах управления доступом, но не решает все проблемы для крупной компании с гибридной ИТ-архитектурой. Для осуществления полноценного контроля доступа необходим централизованный механизм, который объединит все разрозненные процессы, разные ИТ-системы и территориально распределённую структуру компании в единое целое. Централизованное решение по управлению доступом позволит обеспечить возможность внедрения общих политик и процедур для контроля всего ИТ-ландшафта компании», - комментирует директор Центра компетенций управления доступом Solar inRights компании «Ростелеком-Солар» Дмитрий Бондарь.

5. Готовность к автоматизации

Более 40% респондентов готовы автоматизировать процессы управления доступом (чаще в Москве – 51% опрошенных, чем в регионах – 41%). Среди основных проблем респонденты выделяют отсутствие бюджетов и высокую стоимость решений.

Готовность автоматизировать процессы управления доступом и барьеры при автоматизации



Респонденты из государственных компаний активнее выражают готовность автоматизировать процессы управления доступом (47% респондентов vs 43% в коммерческом секторе), при этом чаще отмечая проблематику долгого процесса внедрения.

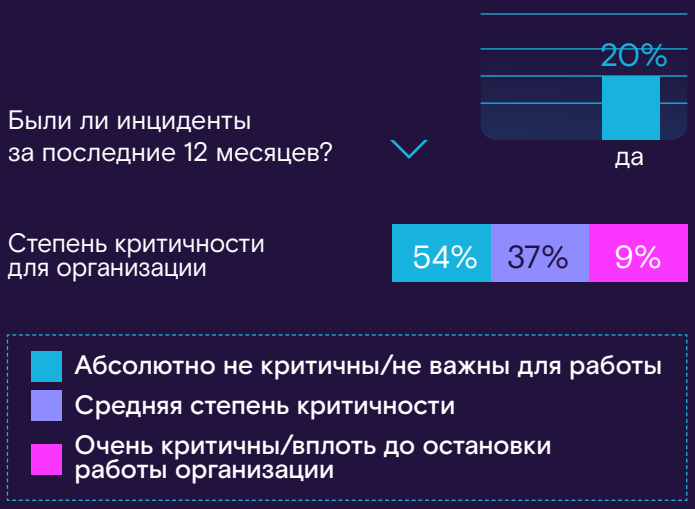
Готовность автоматизировать процессы управления доступом и барьеры при автоматизации

6. Наличие инцидентов ИБ, связанных с правами доступа

20% респондентов отметили, что в их компании за последний год были инциденты, связанные с правами доступа. При этом 46% указали на их среднюю/высокую степень критичности для работы организации.

Как отмечает директор Центра компетенций управления доступом Solar inRights компании «Ростелеком-Солар» Дмитрий Бондарь: «В большинстве случаев такие инциденты связаны с нарушением политик информационной безопасности, с накоплением излишних прав, отсутствием своевременной ресертификации, а также компрометацией учётных данных работников и халатным отношением к вопросам кибергигиены».

Инциденты с правами доступа и их критичность



7. Использование технологии DCAP и контроль неструктурированных данных

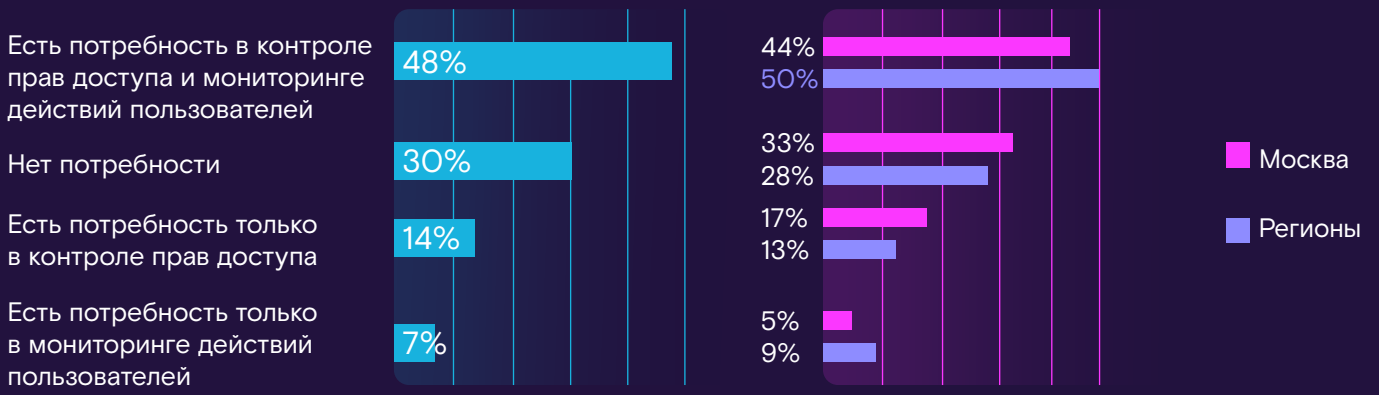
Проблема контроля конфиденциальных данных актуальна практически для всех предприятий. Помимо ключевых информационных систем данные хранятся в сетевых и облачных хранилищах, на корпоративных порталах, почтовых серверах и т.п. Кроме того, данные перемещаются и модифицируются, и необходим постоянный мониторинг и контроль за неструктурированным контентом. Поэтому решения для выявления, мониторинга и контроля использования неструктурированных данных – DCAP-системы (Data-Centric Audit and Protection) – востребованы сегодня, как никогда.

Директор Центра компетенций управления доступом Solar inRights компании «Ростелеком-Солар» Дмитрий Бондарь отмечает: «Совместное использование решений IdM и DCAP в связке даёт синергетический эффект и обеспечивает наиболее полный контроль над данными, тем самым минимизируя утечку конфиденциальной информации, где бы она ни хранилась и ни обрабатывалась.

Такие решения могут дополнять друг друга: появляется возможность работать не только с учетными записями и правами доступа в информационных системах, но и с конечными файлами, которые хранятся на сетевых и файловых ресурсах, обеспечивая разграничение и своевременное прекращение доступа к ним и контролируя операции, которые работники могут с ними выполнять».

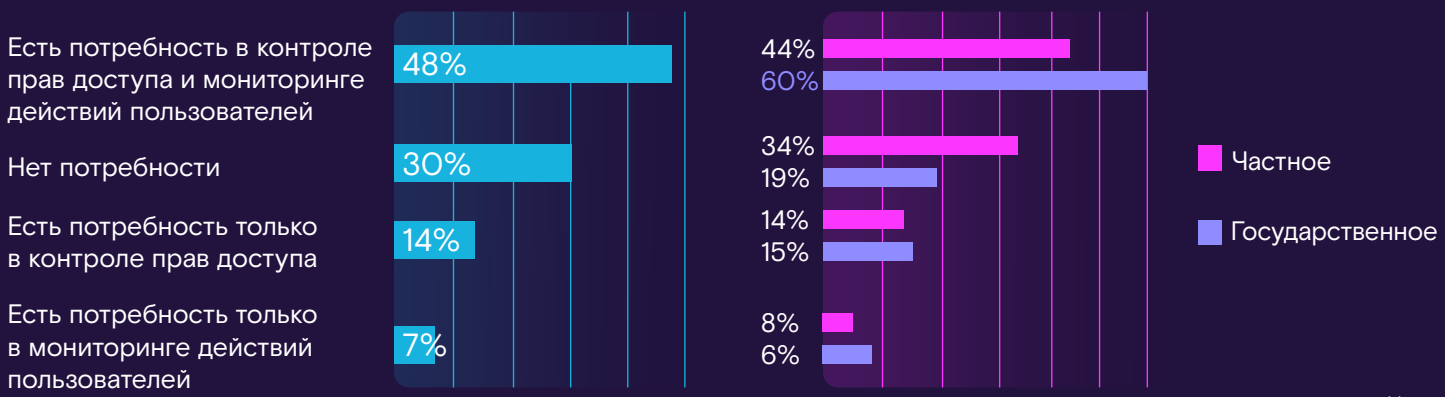
48% опрошенных компаний отметили потребность в DCAP, в регионах немного чаще, чем в Москве (50% vs 44% соответственно).

Тотал

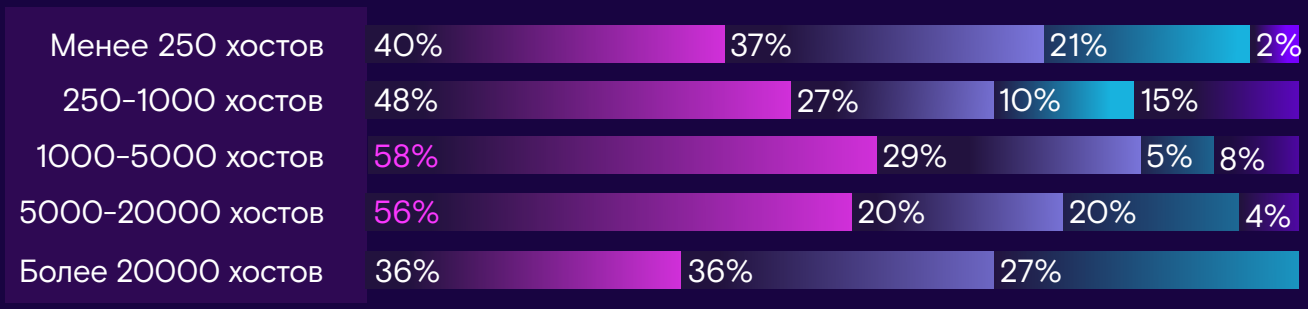


Респонденты из государственных предприятий значительно чаще отмечают интерес к DCAP-системам. По мнению авторов исследования, это может быть связано с тем, что госструктуры обрабатывают большие массивы персональных данных населения страны и осознают свою ответственность за сохранение их конфиденциальности.

Тотал



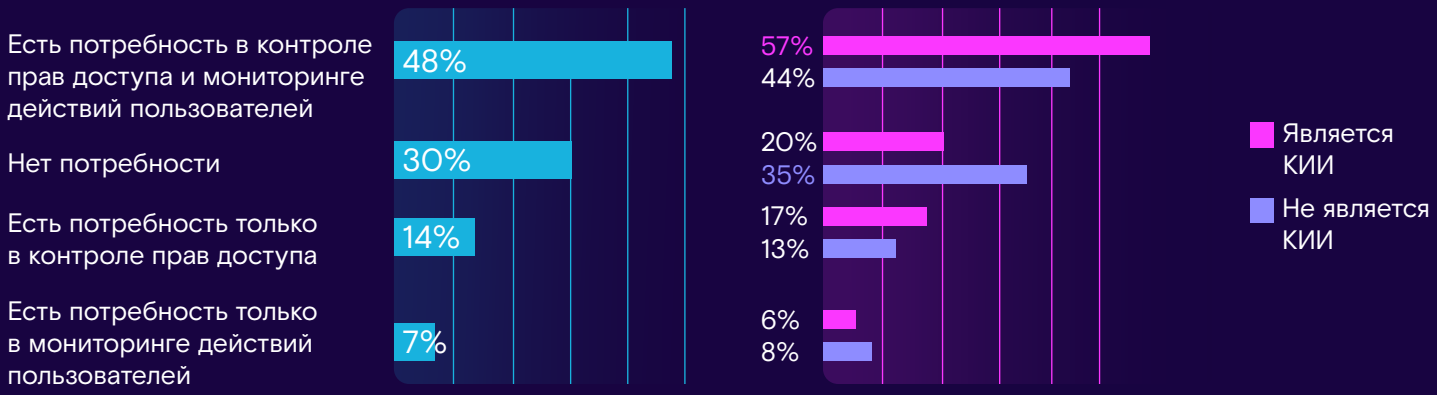
Респонденты с количеством рабочих станций от 1000 (крупные предприятия) чаще нуждаются в DCAP.



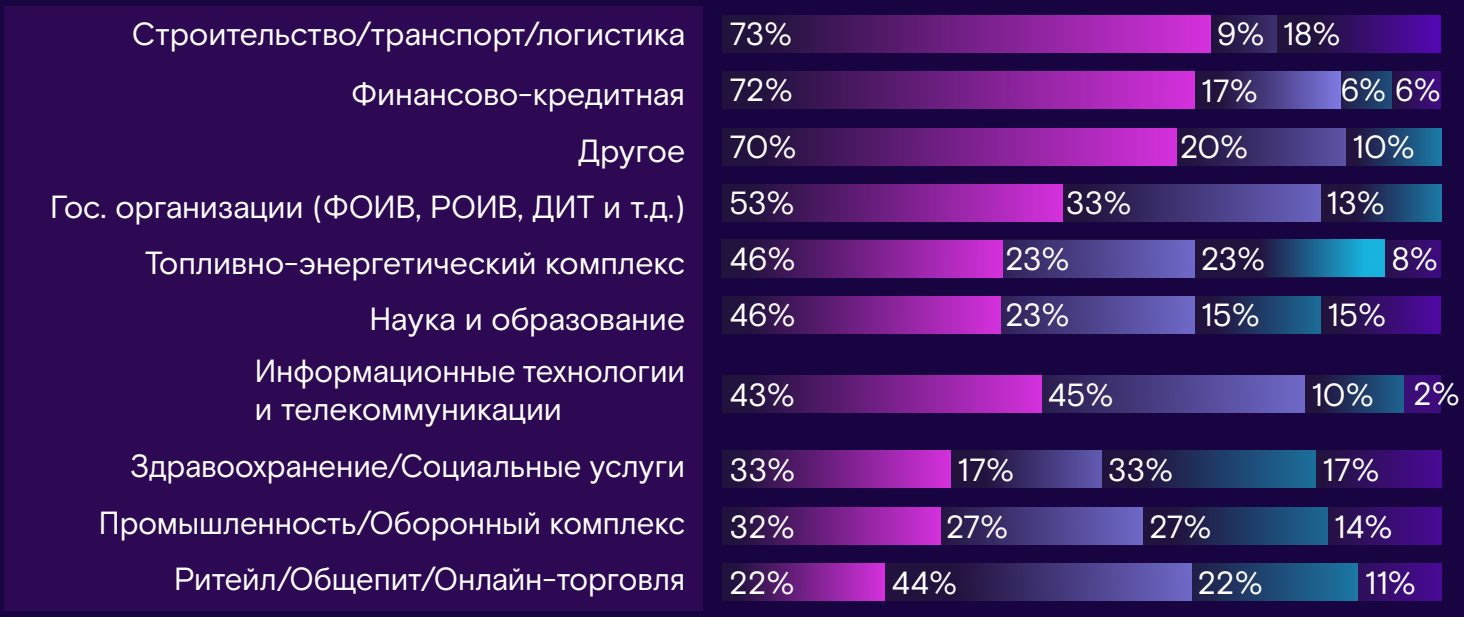
- Есть потребность в контроле прав доступа и мониторинге действий пользователей
- Есть потребность только в контроле прав доступа
- Нет потребности
- Есть потребность только в мониторинге действий пользователей

Представители предприятий, относящихся к объектам КИИ, чаще отмечают потребность в контроле прав доступа или мониторинге действий при использовании хранилища неструктурированных данных.

Тотал



Наиболее интересующиеся DCAP-решениями отрасли – строительство/транспорт/логистика и финансово-кредитная сфера.



- Есть потребность в контроле прав доступа и мониторинге действий пользователей
- Есть потребность только в контроле прав доступа
- Нет потребности
- Есть потребность только в мониторинге действий пользователей

8. Выводы и рекомендации

Сегодняшняя картина управления доступом в российских компаниях такова, что полностью автоматизированные процессы управления доступом пока являются стратегической целью для большинства отечественных организаций. Больше половины опрошенных предприятий уже встали на этот путь, но автоматизировали лишь часть процессов.

В целом, почти треть респондентов сошлась во мнении, что автоматизированные средства управления доступом и контроля работы пользователей уже сейчас помогают закрыть ряд задач и решить проблемы компании, даже если автоматизирована только часть процессов.

Однако более половины респондентов пока не готовы выделить средства на полную автоматизацию и опасаются, что потраченные средства не принесут выгоды в ближайшей перспективе из-за достаточно долгого срока внедрения решения по автоматизированному управлению доступом (IdM – Identity Management).

Эти данные говорят о том, что не все компании в настоящее время готовы выстроить внутри себя правильные и корректные процессы управления доступом, а их отсутствие осложняет внедрение автоматизации и требует достаточно много времени на подготовительный период.

Тем не менее вопрос внедрения соответствующих программных инструментов управления доступом стоит для российских компаний весьма остро, ведь чуть менее половины инцидентов информационной безопасности, связанных с правами доступа, являются высоко и среднекритичными для ряда компаний.

Наряду с необходимостью автоматизации процессов управления доступом в своих ключевых ИТ-системах почти половина опрошенных испытывают потребность навести порядок в использовании и контроле неструктурированных данных, хранящихся в компании. Компании хотят использовать DCAP (Data-Centric Audit and Protection) – современный подход к управлению безопасностью данных и контролю доступа пользователей к информационным ресурсам предприятия.

9 . О нас

«Ростелеком-Солар» – компания группы ПАО «Ростелеком», национальный провайдер сервисов и технологий для защиты информационных активов, целевого мониторинга и управления информационной безопасностью.

В основе наших технологий лежит понимание, что настоящая информационная безопасность возможна только через непрерывный мониторинг и удобное управление системами ИБ. Этот принцип реализован в продуктах и сервисах «Ростелеком-Солар».

Центр компетенций управления доступом Solar inRights «Ростелеком-Солар» – крупнейший в России по числу специалистов. Он объединяет экспертов с многолетним опытом управления доступом в ведущих компаниях России. Их понимание процессов крупного бизнеса и государственных организаций позволяют создавать высокотехнологичные продукты с учетом всей специфики отрасли и потребностей организаций. Миссия Центра - предоставление экспертизы, надежных решений по управлению доступом и построение долгосрочных партнерских отношений с заказчиками.

Ростелеком
Солар

rt.ru
rt-solar.ru

Info@rt-solar.ru
+7 (499) 755-07-70

Задать вопрос или
попробовать сервис

presale@rt-solar.ru