Ростелеком
Солар

Системы контроля действий привилегированных пользователей (PAM)

Группа исследований рынка

rt-solar.ru

Оглавление

Цели, задачи и методология

Цели и задачи

- Выявить проблематику PAM, определить, как ее видят пользователи
- Выявить ситуации, которые являются наиболее сложными при эксплуатации решений PAM

Данные исследования

Проект был реализован методом количественного опроса
(силами «Ростелеком-Солар» без привлечения сторонних агентств)

1

Целевая аудитория

Сотрудники компаний, отвечающие за выбор и внедрение продуктов и сервисов по тематике «Информационная безопасность»

Компании распределены по сегментам: B2G, B2E, B2B верхний, B2B средний, B2SMB

2

География

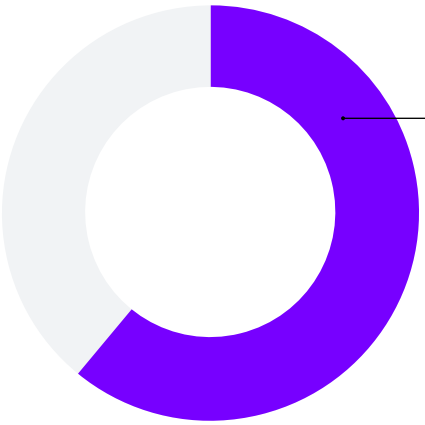
Москва, Санкт-Петербург, города 1 млн+
и 500 000+ жителей

3

Выборка

n = 104 интервью с представителями целевой аудитории

Выводы и рекомендации



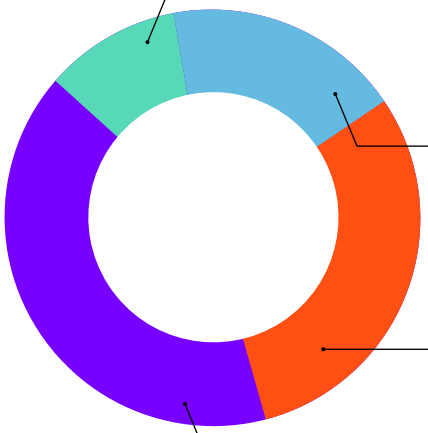
61%

Проблематика угроз в связи с использованием привилегированного доступа является актуальной, — примерно 61% опрошенных сталкиваются с ней раз в месяц и чаще.

Основные «боли» для респондентов:

- Любые нарушения, связанные с паролями
- Скачивание запрещенного контента
- Обход политик безопасности в личных целях

Также больше половины респондентов опасаются увеличения обезличенных и неуправляемых учетных записей и отсутствия централизованной видимости всех привилегированных пользователей.



10%

Используют полноценное решение PAM

19%

Не управляют привилегированным доступом

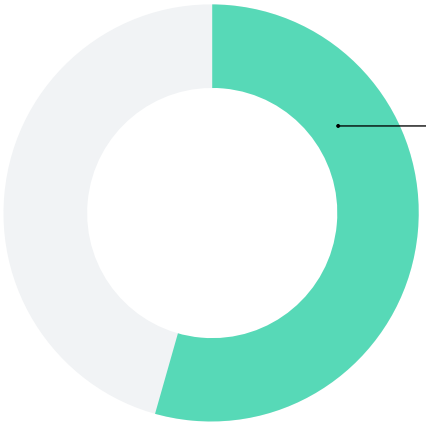
30%

Применяют непрофильные решения (ряд автоматизированных средств)

41%

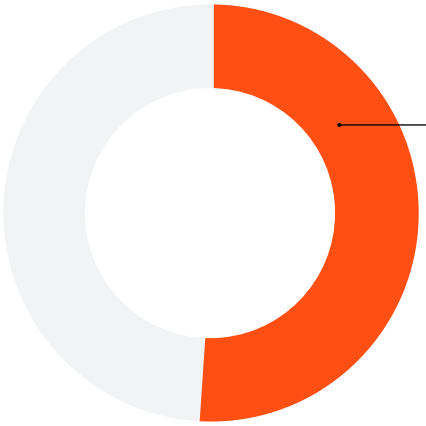
Управляют доступом вручную

Основные задачи, которые пользователи хотят решить посредством PAM:



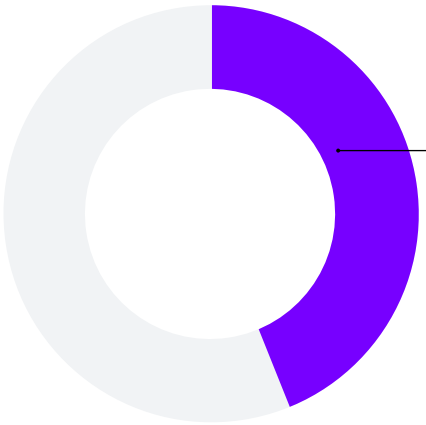
58%

Защита всех привилегированных учетных данных / достижение более высокого уровня безопасности



51%

Полная прозрачность и подконтрольность действий внешних поставщиков/контрагентов/ подрядчиков, имеющих доступ к ресурсам компании

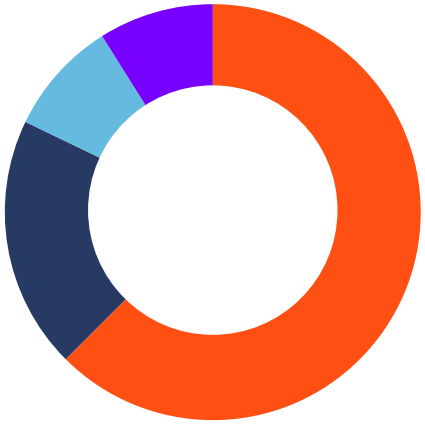


44%

Снижение затрат на соблюдение требований ИБ

Профиль респондентов

Сфера деятельности



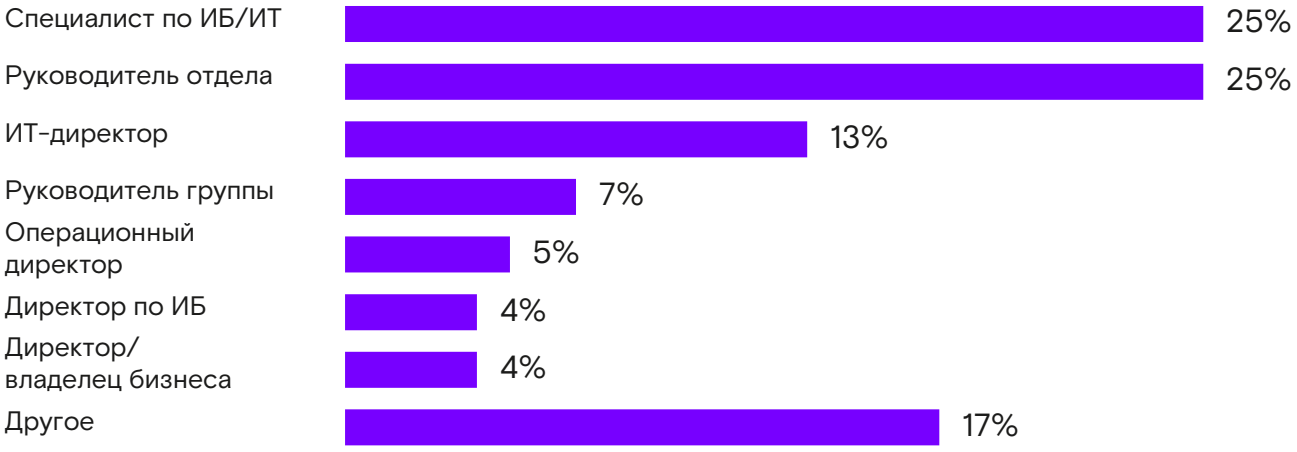
9% ФОИВ

62% Коммерческая организация

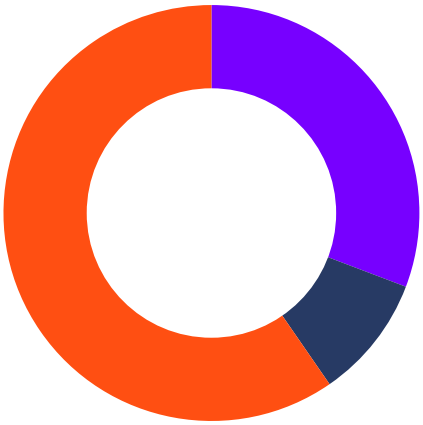
9% РОИВ

20% Компания с госучастием

Должности респондентов



Город/Сектор



60%
Москва

30%
Регионы

10%
Санкт-Петербург

36%
SMB

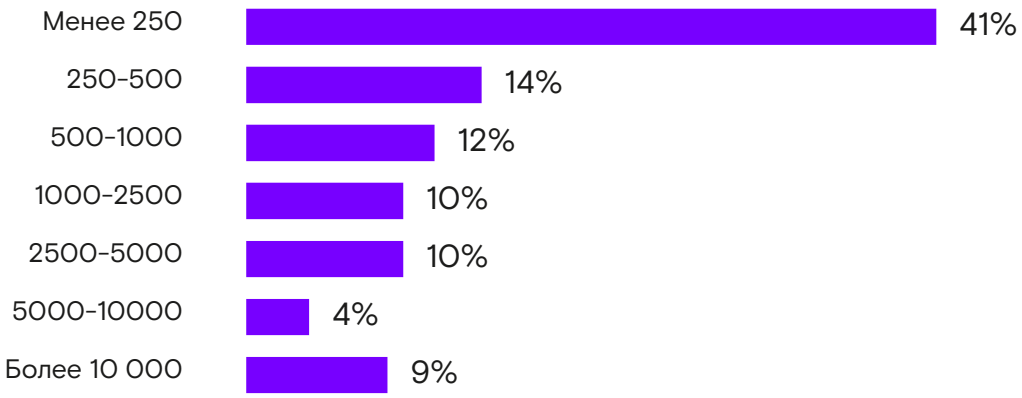
33%
B2B средний*

18%
B2G

13%
B2E/B2B старший**

* B2E/B2B старший - компании с выручкой от 5 млрд рублей в год
** B2B средний - компании с выручкой от 800 млн до 5 млрд рублей в год

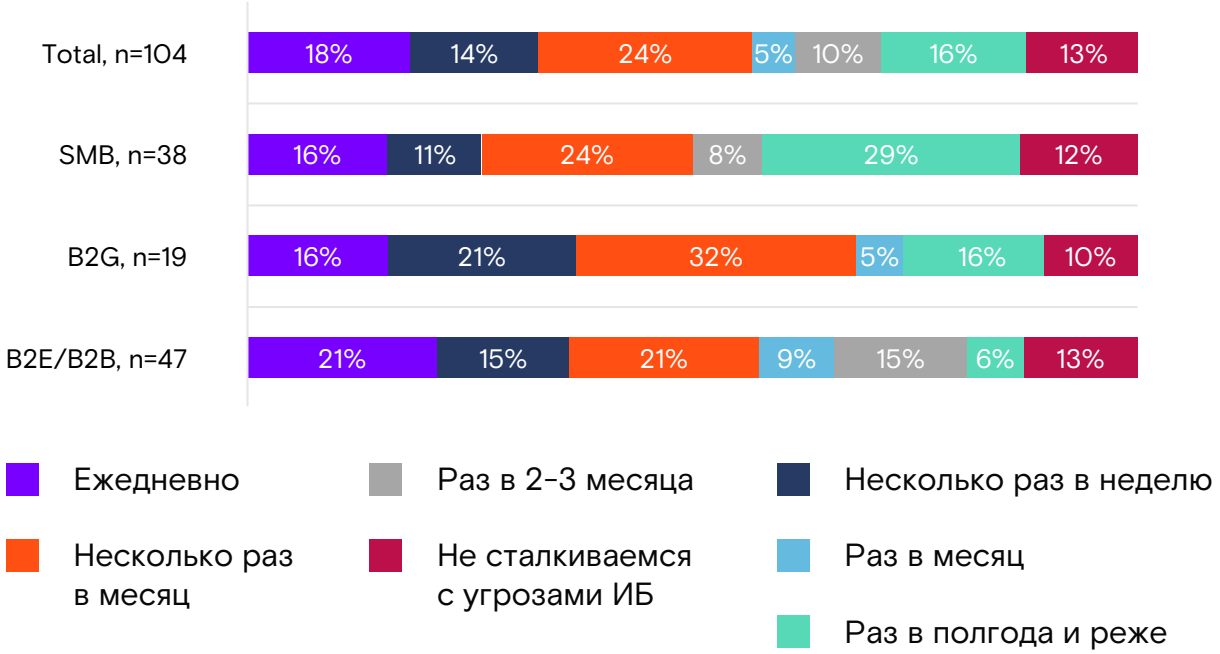
Размер организации по кол-ву сотрудников



Результаты

В среднем примерно 1/3 респондентов сталкиваются с угрозами в ИБ несколько раз в неделю и чаще, в-основном, с вредоносным ПО и DDos-атаками.

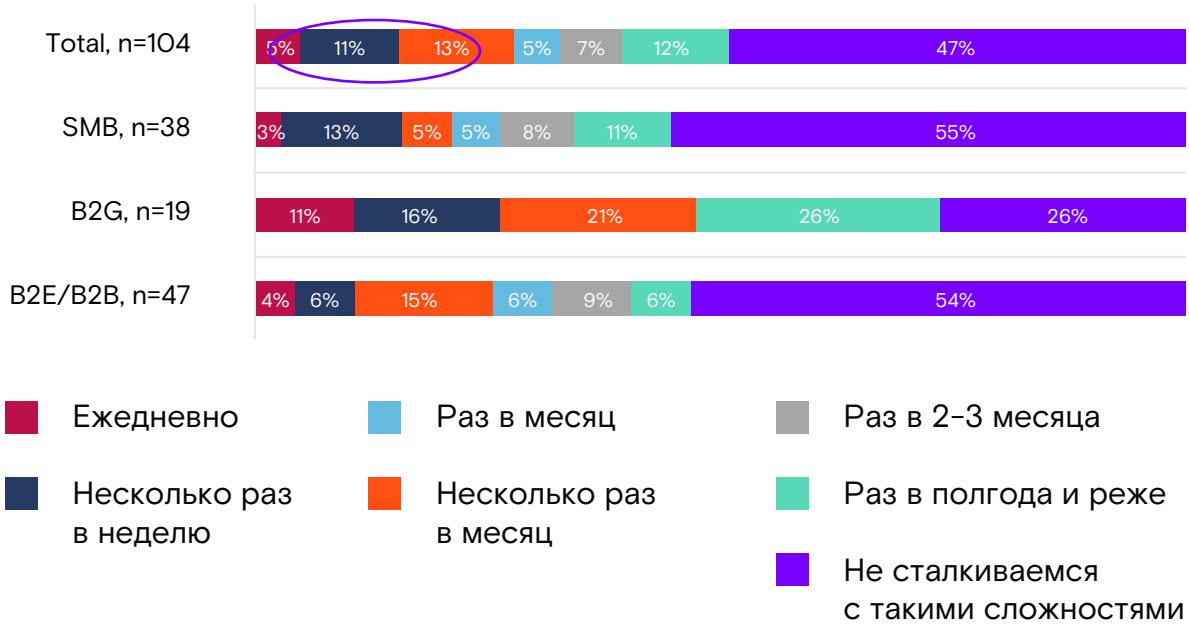
Форма собственности



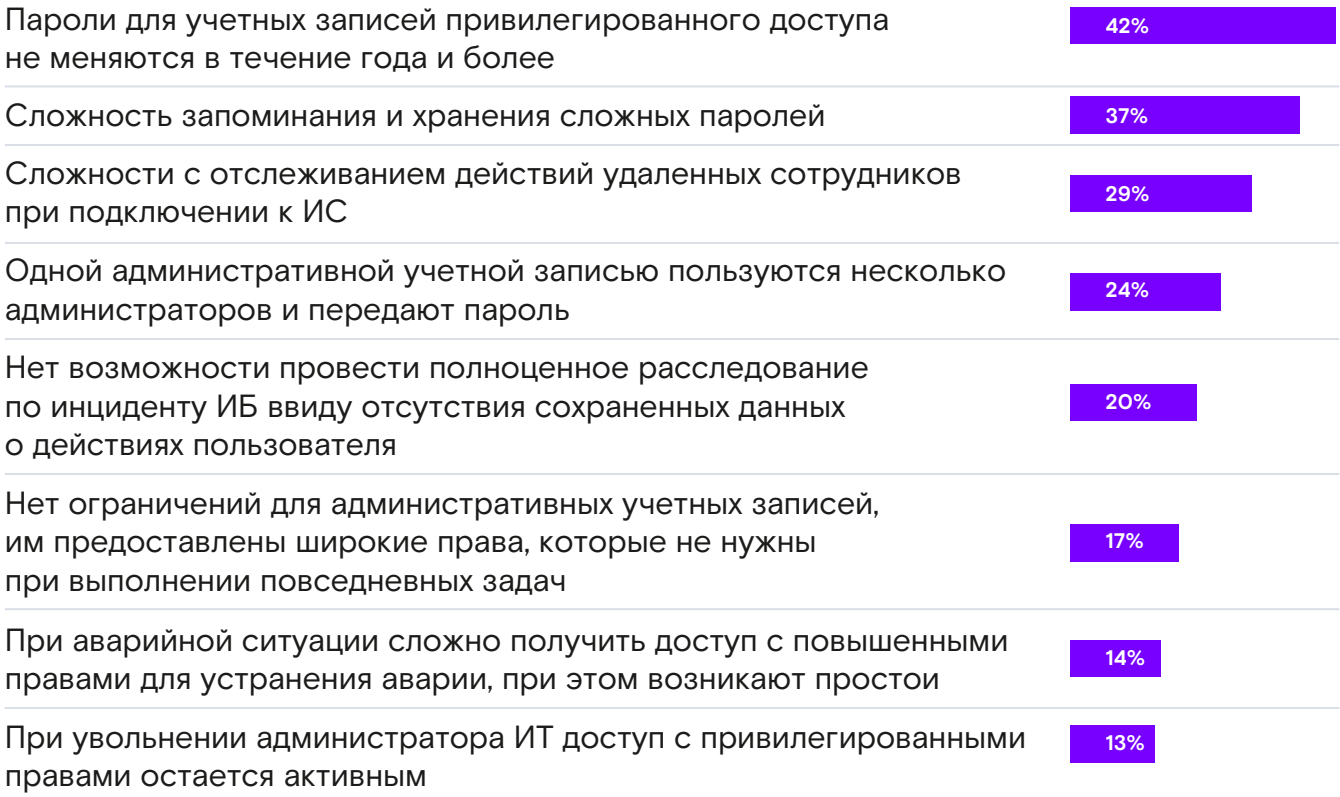
Типы угроз, с которыми сталкивается компания

~ 29% респондентов сталкиваются с угрозами в части привилегированного доступа несколько раз в месяц и чаще, наиболее часто — с нарушениями в части паролей (изменение и хранение). В свою очередь, почти половина респондентов не имеет таких проблем.

Угрозы в связи с использованием привилегированного доступа

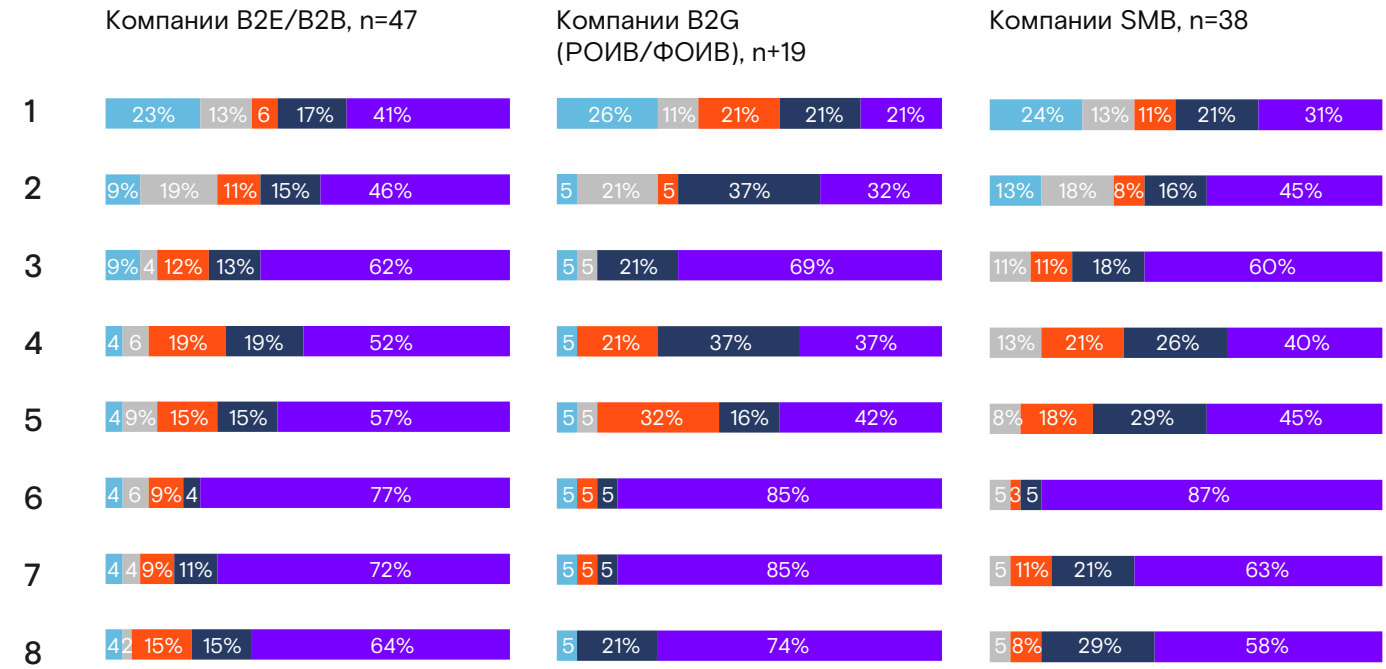


Типы угроз, с которыми сталкивается компания



Скачивание запрещенного контента и обход политик безопасности – наиболее часто встречающиеся нарушения при использовании доступа во всех сегментах.

Угрозы в связи с использованием привилегированного доступа

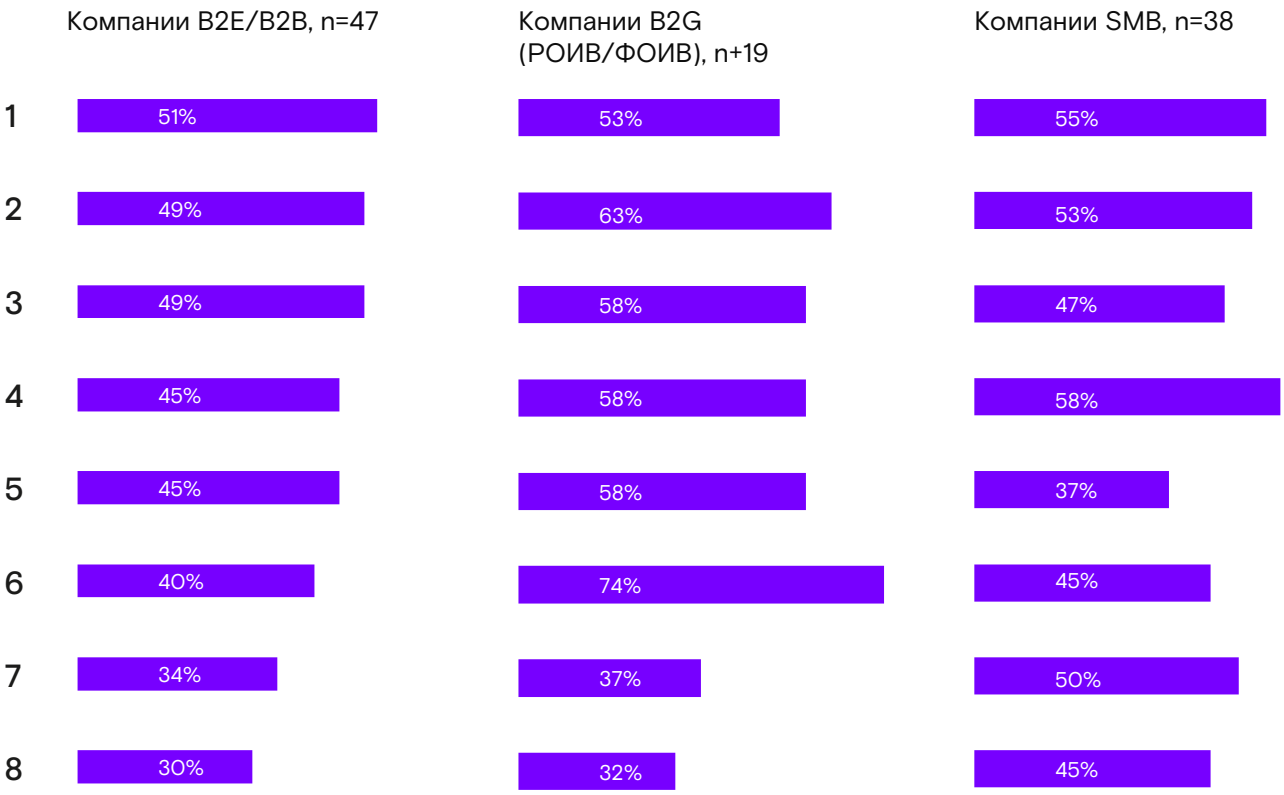


- Ежедневно / несколько раз в неделю
- Несколько раз / раз в месяц
- Раз в 2-3 месяца
- Раз в полгода и реже
- Не сталкиваемся

1. Скачивание запрещенного контента
2. Обход политики безопасности в личных целях
3. Использование обезличенных учеток для несанкционированного доступа в ИС
4. Несанкционированное скачивание конфиденциальной информации
5. Несанкционированное использование повышенных прав для доступа к корпоративным данным
6. Несанкционированные финансовые операции
7. Удаление / изменение логов / журнальных файлов для скрытия неправомерных действий
8. Злонамеренное изменение конфигурации ИС или повреждение/удаление данных

Увеличение обезличенных и неуправляемых учетных записей, по мнению респондентов сегментов B2E / B2B, в большей степени способно усложнить процесс работы, тогда как B2G отмечают отсутствие отчетности.

Что усложнит процесс работы



1. Увеличение обезличенных и неуправляемых учетных записей

2. Отсутствие централизованной видимости всех привилегированных пользователей и их деятельности

3. Атаки на привилегированных пользователей

4. Трудности с проверкой привилегированных пользователей на соответствие политикам безопасности

5. Увеличение разных типов привилегированных пользователей (облако, секреты DevOps)

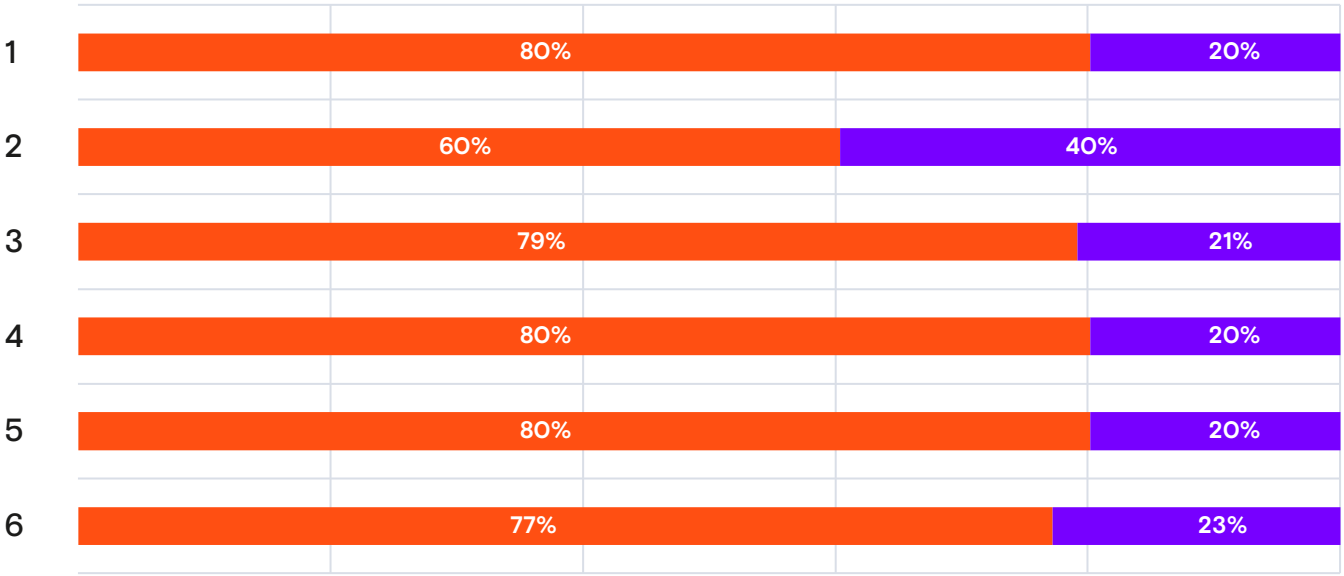
6. Отсутствие отчетности о привилегированных учетных записях и их деятельности

7. Увеличение количества прав, необходимых для привилегированных пользователей

8. Увеличение числа привилегированных пользователей

В подавляющем большинстве респонденты отмечают все указанные проблемы в большей степени для сотрудников, работающих удаленно.

Что усложнит процесс работы



Удаленные сотрудники

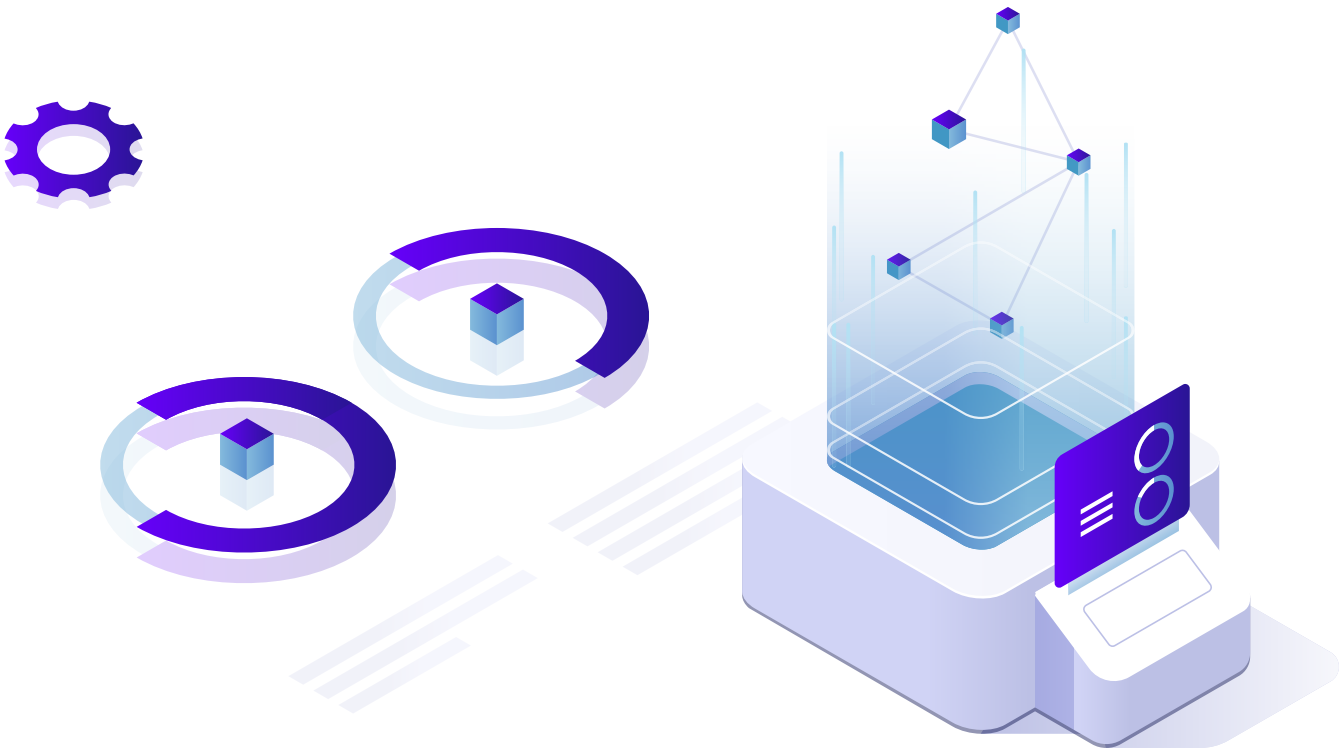
Офисные сотрудники

1. Сложнее определить, произошла ли компрометация учетных данных
2. Более высокая частота обращений в справочную службу
3. Пользователям сложно получить доступ к системам для выполнения своей работы
4. Много пользователей, использующих BYOD (собственное устройство для работы)
5. У пользователей возникают проблемы с аутентификацией (пароли, 2FA...)
6. Пользователи более подвержены фишингу, мошенничеству и социальной инженерии

Защита / достижение более высокого уровня безопасности и полная прозрачность действий внешних игроков — задачи, которые респонденты чаще других хотели бы решить посредством PAM.

Какие задачи хотите решить посредством PAM

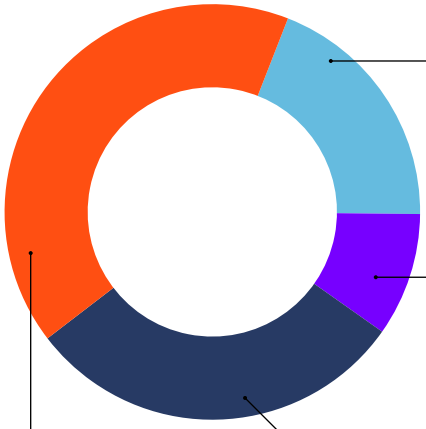
Защита всех привилегированных учетных данных / достижение более высокого уровня безопасности	58%
Полная прозрачность и подконтрольность действий внешних поставщиков/контрагентов/подрядчиков, имеющих доступ к ресурсам компании	51%
Снижение затрат на соблюдение требований ИБ	44%
Обеспечение соблюдения принципа наименьших привилегий (минимальный доступ, только на необходимый срок)	41%
Интеграция управления привилегированным доступом в общую концепцию управления ИТ-услугами/изменениями	39%
Удаление излишнего административного доступа на серверах	39%
Прохождение аудитов на соответствие внешним и внутренним требованиям	36%
Обнаружение всех привилегированных учетных записей	33%



Лишь 10% респондентов используют полноценное решение PAM, большинство применяют непрофильные решения (ряд автоматизированных средств) или управляют доступом вручную.

Как выстроена работа с привилегированным доступом сейчас

Total, n=104



19%

Не управляют привилегированным доступом

10%

Используют полноценное решение по управлению привилегированным доступом PAM (Privileged Access Managment)

30%

Применяют непрофильные решения (ряд автоматизированных средств, которые частично закрывают потребности в управлении/контроле привилегированного доступа

41%

Управляют привилегированным доступом вручную

Ростелеком
Солар

rt.ru

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