КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

Особенности применения СЗИ при выполнении требований приказа № 117 ФСТЭК России

Критерии выбора и комплексирования средств защиты информации

Евгения Кислицына

Заместитель коммерческого директора
Центра защиты информации
ГК «Конфидент»

EMAIL: ISC@CONFIDENT.RU

WEB: WWW.DALLASLOCK.RU

Почему 117-й приказ стал вызовом

Меняется область применения

- Распространяется на более широкий круг ИС
- Затрагивает не только отдельные сегменты, а инфраструктуру в целом
- Требует пересмотра уже реализованных подходов

Основные сложности применения

- Не всегда понятно, какие именно функции должны быть реализованы и какими средствами
- Возникают сложности при работе в гетерогенных средах и при невозможности полной замены платформ

Смещение фокуса с наличия средств на выполнение функций

- Недостаточно просто иметь СЗИ определённого класса, требуется обеспечить управляемость процессов
- Оценивается не продукт, а результат функционирования системы защиты

Рынок и приказ № 117: опрос

Мы провели короткий опрос, чтобы понять фактическую готовность рынка к требованиям приказа ФСТЭК России № 117. В него вошли 4 ключевых вопроса:

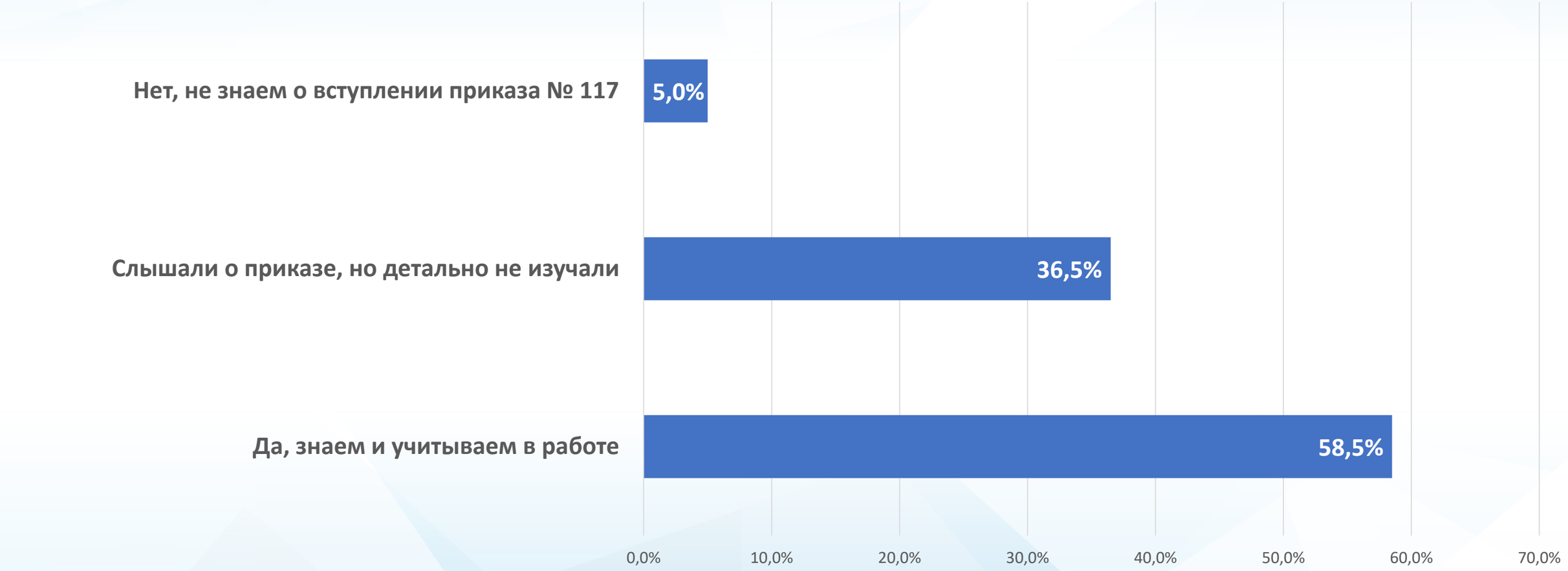
Знают ли организации о вступлении в силу приказа № 117?

Считают ли себя готовыми к его требованиям?

Каких классов СЗИ не хватает для соответствия приказу?

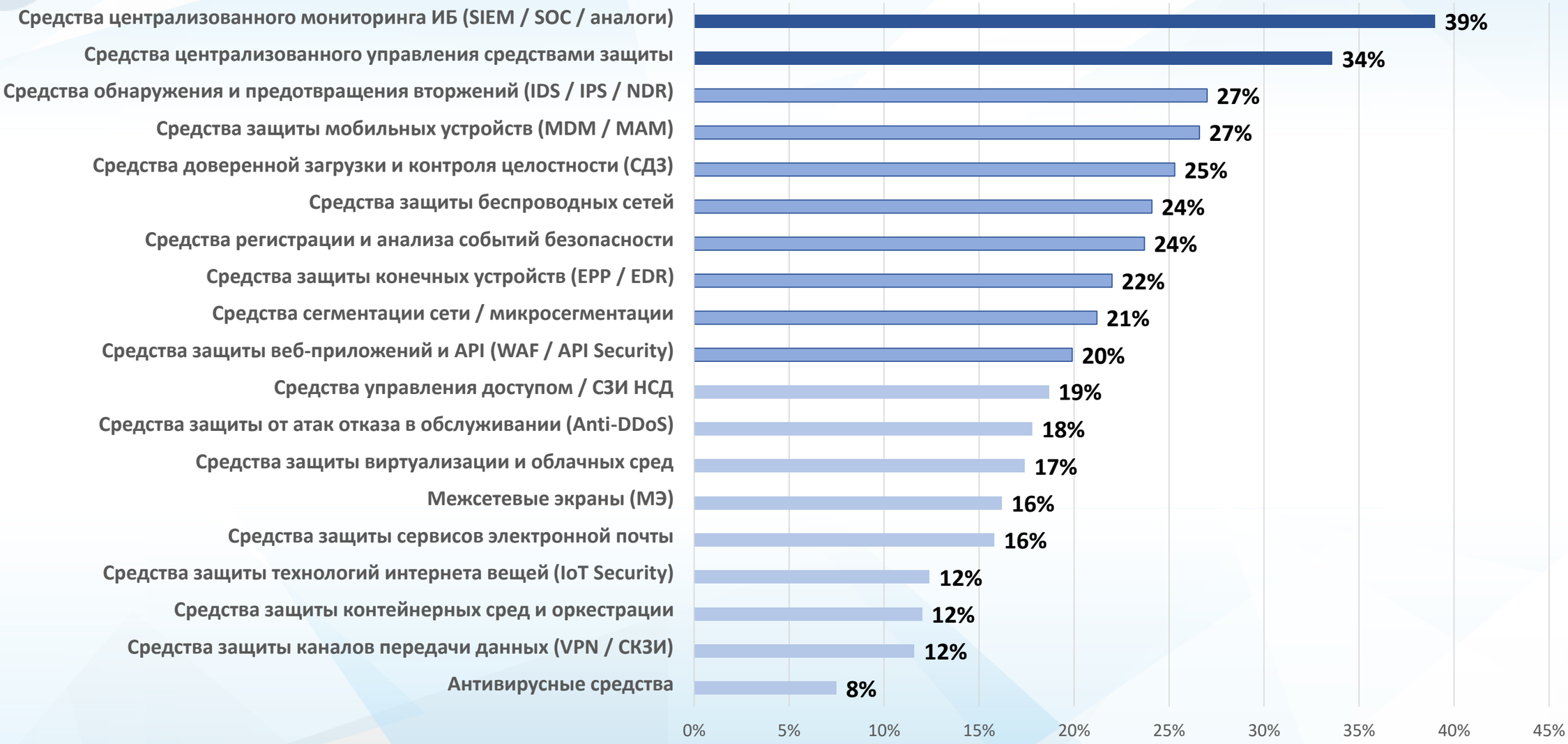
Используется ли централизованный мониторинг ИБ?

Знаете ли вы о вступлении в силу приказа ФСТЭК России № 117?

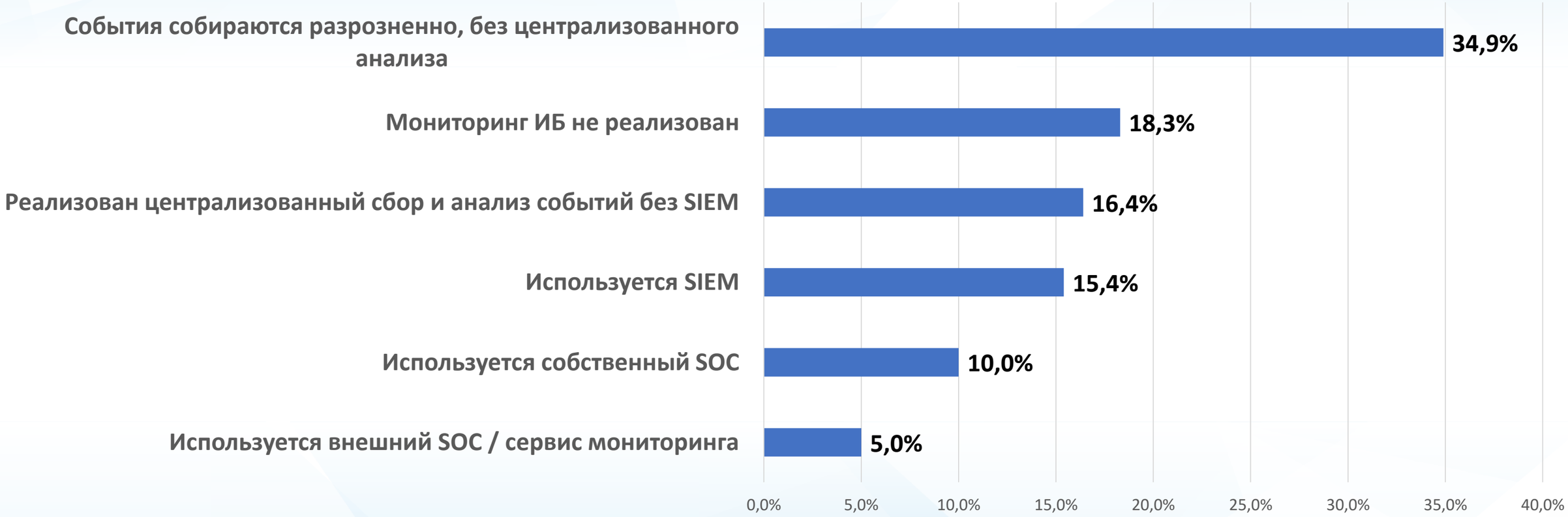


Считаете ли вы свою организацию готовой к выполнению требований приказа ФСТЭК России № 117?

Каких классов СЗИ не хватает для соответствия приказу?

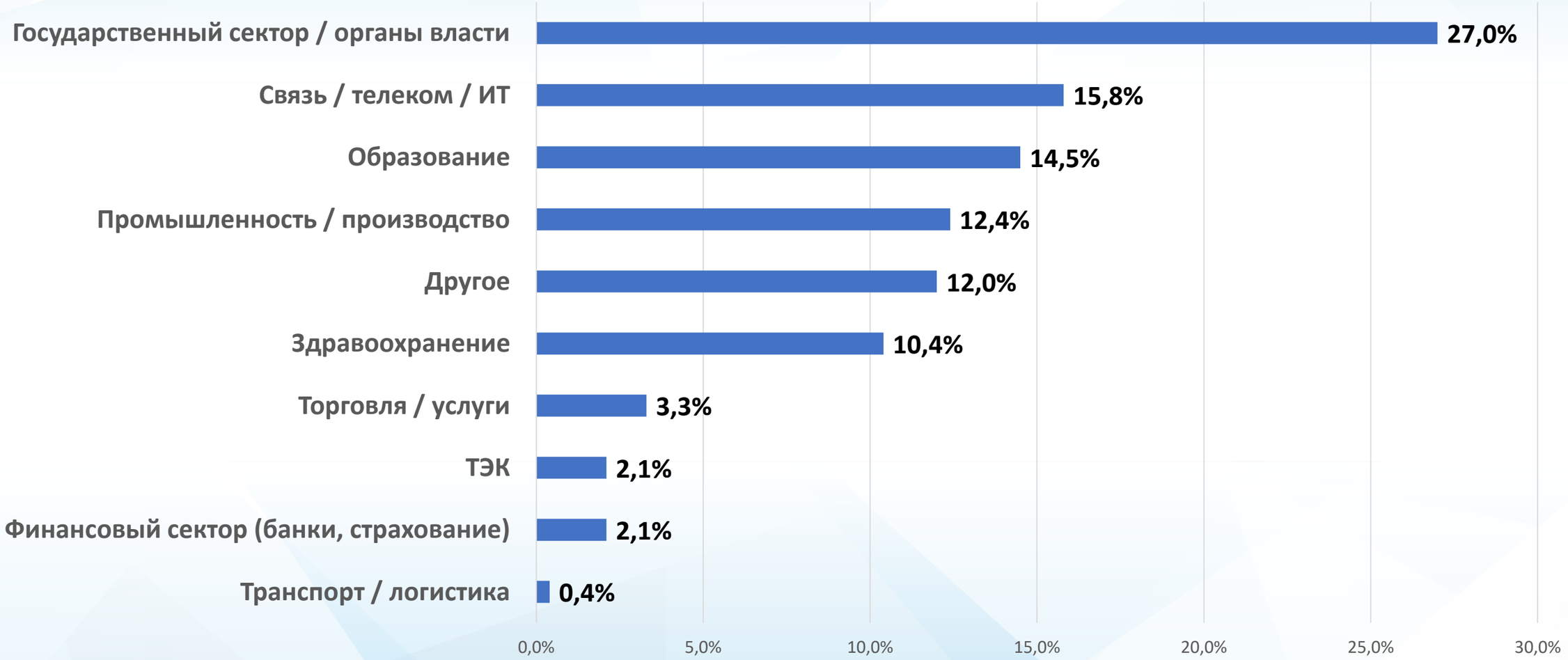


Каким образом в вашей организации реализован мониторинг информационной безопасности?

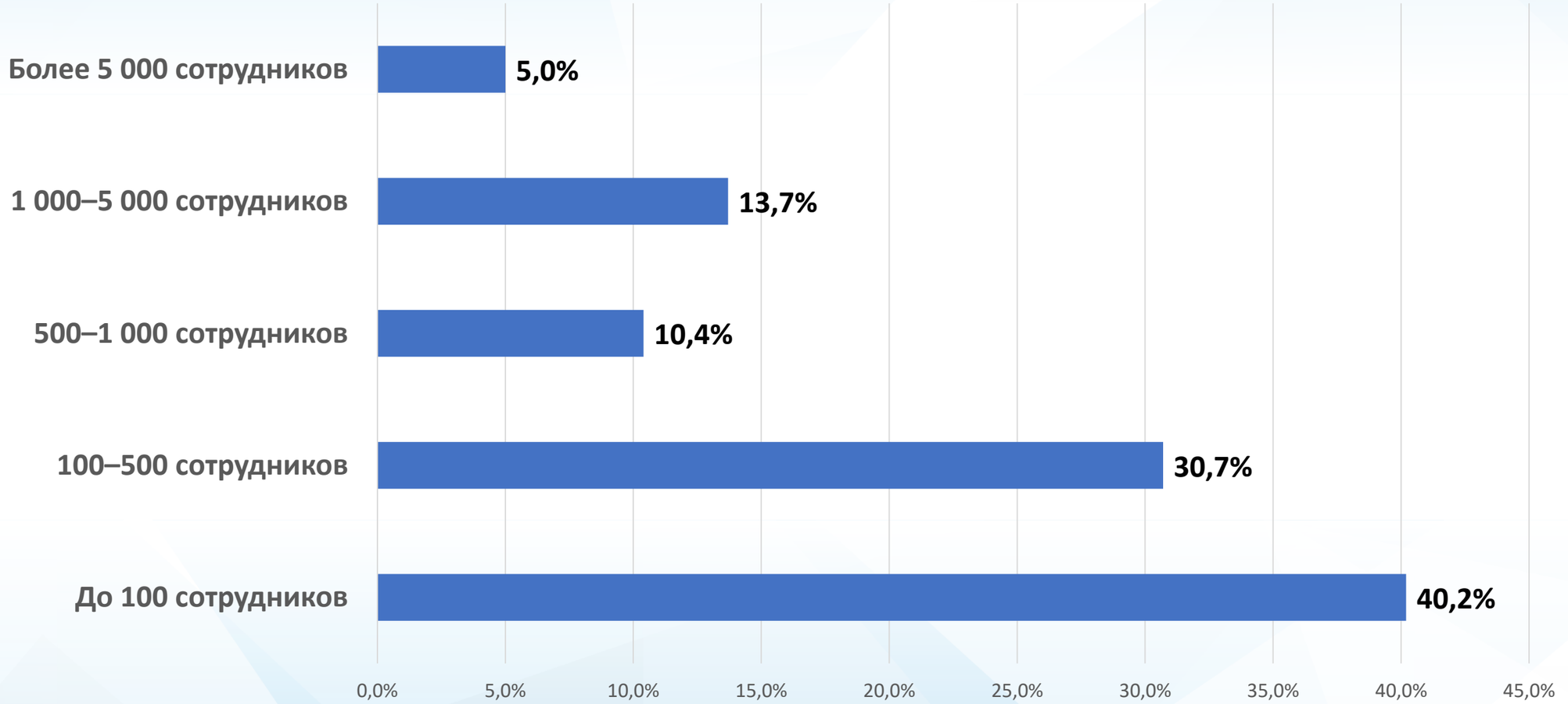


Используются ли ОС, которые невозможно заменить на сертифицированные в силу требований прикладного ПО или иных технологических/организационных ограничений?

Какую отрасль представляет ваша организация?



Какой размер вашей организации?



Что показал опрос

1. Рынок осведомлён о приказе № 117, но глубина понимания неоднородна. Значительная часть организаций пока находится на этапе первичного изучения требований.

2. Большинство организаций не готовы к выполнению требований № 117 «здесь и сейчас». Доминируют стадии анализа, проектирования и ожидания бюджета, а не внедрения.

3. Мониторинг ИБ реализован фрагментарно и не всегда соответствует требованиям системного уровня. SIEM и SOC используются ограниченно, часто отсутствует централизованный анализ событий.

4. Переход на сертифицированные ОС ограничен объективными факторами. Во многих ИС используются операционные системы, замена которых невозможна или существенно затруднена, что требует применения компенсационных и архитектурных мер защиты.

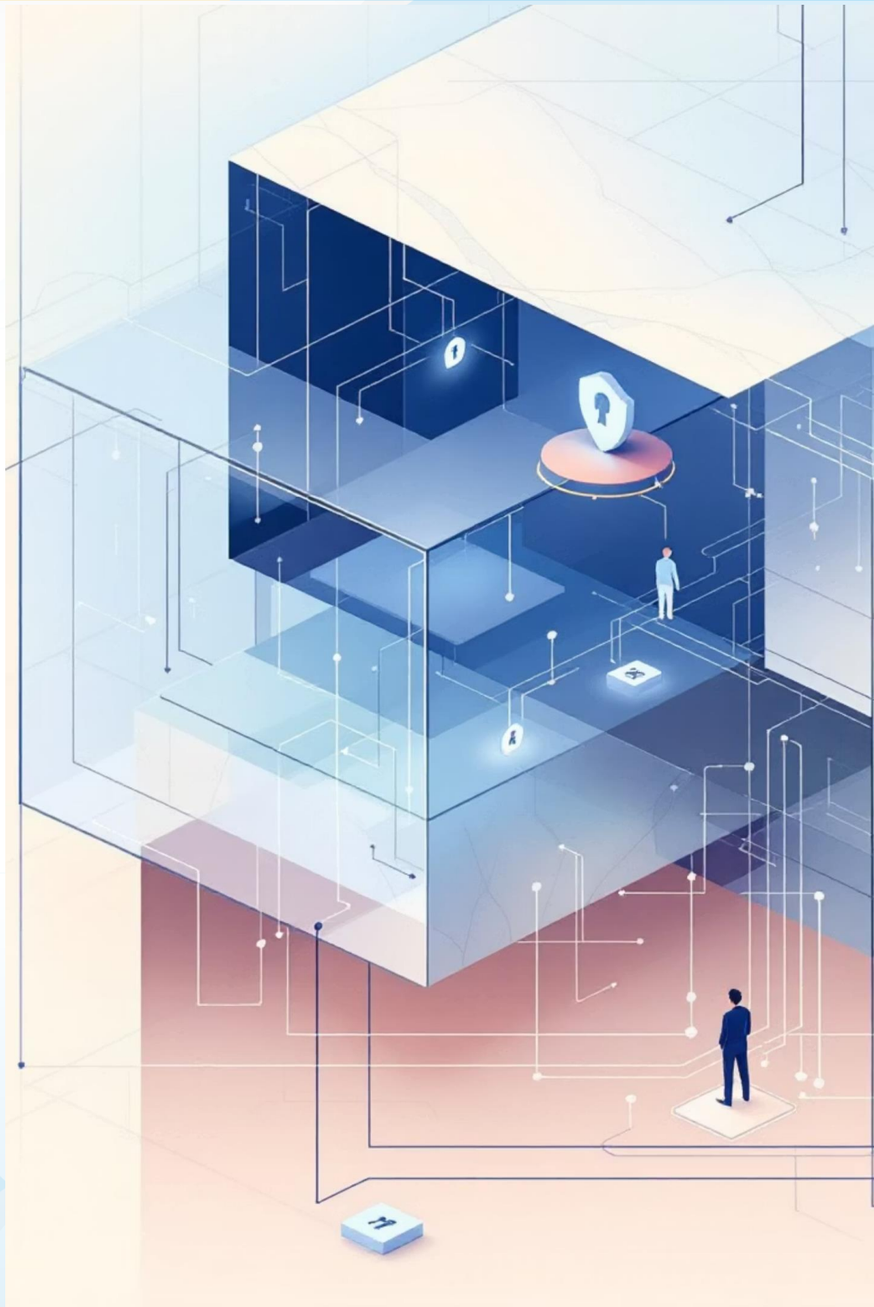
Как 117-й приказ формулирует требования

117-й приказ описывает защиту **через функции**, а не продукты:

- идентификация и аутентификация
- управление доступом (в т. ч. привилегированным)
- регистрация и анализ событий
- мониторинг ИБ
- защита конечных устройств
- защита сетевого взаимодействия
- управление уязвимостями и обновлениями

Необходима архитектура, а не набор решений.

Формальное наличие СЗИ ≠ выполнение требований приказа



Системный уровень НСД в контексте приказа № 117

НСД — это не только вход пользователя

Это весь жизненный цикл работы с ресурсами ИС

Требуется контроль:

- запуска ПО
- процессов
- доступа к данным
- привилегированных операций

При несогласованной реализации механизмов НСД:

- затрудняется централизованное управление
- усложняется подтверждение соответствия требованиям
- не формируется целостная картина состояния защиты

КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

НСД

СЗИ

МЭ, СКН, СОВ, СОР

EDR

НСД развивается как самостоятельное направление

- реализует функции управления доступом
- применяется при необходимости встроенного контроля
- не является обязательным для каждой ОС

Отдельные модули реализуют требуемые меры без конфликта с ОС

- разграничение и фильтрация сетевого трафика
- сегментация и изоляция сетевых зон
- выявление и блокирование сетевых атак
- контроль и анализ сетевого взаимодействия

- Обеспечивается реализация мер на разных уровнях ИС в соответствии с приказом № 117
- Исключается дублирование функций НСД
- За счет установки отдельных модулей безопасность не избыточна и обеспечивается в соответствии с заданной моделью угроз
- Упрощается подтверждение соответствия требованиям

КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

Совместимость с отечественными ОС

не замена платформ, а комплексирование решений

СЗИ Dallas Lock Linux

Поддержка отечественных ОС (в т. ч. Astra Linux)

Работа в среде **сертифицированных** отечественных операционных систем. Решение устанавливается без изменения архитектуры ОС и используется для защиты рабочих мест и серверов.

Отсутствие конфликтов и конкуренции за функции НСД

Механизмы защиты реализуются наложенным образом и корректно взаимодействуют с компонентами ОС, сохраняя целостность и управляемость системы.

Согласование архитектурных подходов с вендорами

Это обеспечивает предсказуемую интеграцию, корректную реализацию требований регулятора и возможность построения комплексной системы защиты без конфликтов между средствами.

ПОДРОБНАЯ ИНФОРМАЦИЯ
ДЕМОВЕРСИИ, БАЗА ЗНАНИЙ, НОВОСТИ
WWW.DALLASLOCK.RU

Мониторинг ИБ как обязательный инструмент

ЕЦУ Dallas Lock уже обеспечивает централизованный сбор и обработку событий безопасности из множества источников.

В соответствии с приказом ФСТЭК России № 117 мониторинг информационной безопасности является обязательной функцией системы защиты и должен включать **ряд функциональных задач:**

01

Постоянный мониторинг ИБ

Сбор, нормализация и хранение событий со всех продуктов и сторонних систем

02

Сбор и анализ событий

Механизм корреляции с правилами и аналитикой на базе ИИ для выявления сложных инцидентов

03

Выявление актуальных угроз

Система оповещений и визуализации для быстрого реагирования на угрозы

04

Формирование отчётности

Система оповещений и визуализации для быстрого реагирования на угрозы

Модуль COP для Windows, Linux и отечественных ОС

Решения **Dallas Lock 8.0** и **Dallas Lock Linux** используют механизмы обнаружения индикаторов компрометации – **IoC** (Indicator of Compromise)

Выявление признаков взлома

- сканирование системы
- управление базой IoC с возможностью добавления пользовательских индикаторов
- регулярное обновление базы индикаторов

Автоматическое реагирование

- блокировка IP-адреса атакующего
- блокировка учетной записи
- блокировка АРМ
- изоляция узла с ограничением сетевой активности
- завершение процесса или отключение АРМ

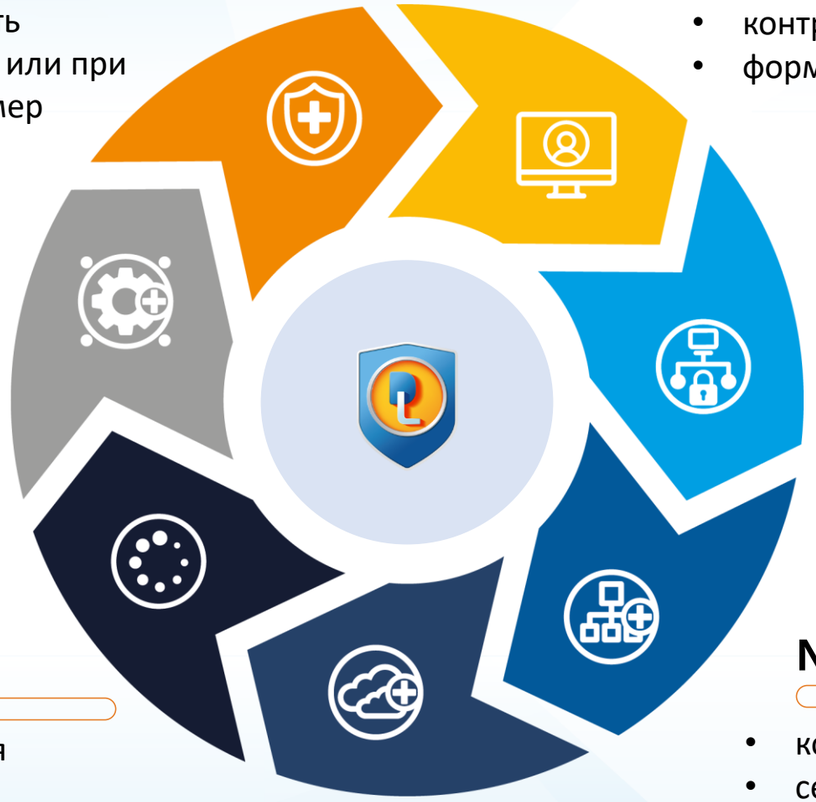
КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

СЗИ НСД

- требуется, когда нужно расширить функции ОС по управлению доступом и разграничению прав, обеспечить централизованное управление, или при реализации компенсирующих мер

Защита конечных устройств: МЭ, СОВ, СКН, СОР

- защита на уровне прикладной среды
- контроль сетевых соединений и процессов
- формирование событий для мониторинга



Единый центр управления

- централизованное управление политиками
- сбор и корреляция событий из разных источников
- выполнение требований № 117 по мониторингу

WAF

- защита веб-приложения и API
- контроль прикладного трафика
- источник событий для централизованного анализа

СДЗ Dallas Lock

- обеспечение доверенного состояния загрузки и функционирования ИС
- контроль целостности программной среды и конфигурации

NAC Dallas Lock

- контроль доступа устройств и пользователей
- сегментация и изоляция
- работа в смешанных средах

СЗИ ВИ Dallas Lock

- защита в виртуальных средах на базе oVirt, zVirt, РЕД Виртуализация, ROSA Virtualization, Альт Виртуализация и HOSTVM

КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

Приглашаем на сайт и в наш телеграм-канал!

Сайт

Телеграм

Евгения Кислицына

Заместитель коммерческого директора
Центра защиты информации
ГК «Конфидент»

EMAIL: ISC@CONFIDENT.RU

WEB: WWW.DALLASLOCK.RU