SEARCHINFORM

ЗАЩИТА ЗОКИИ ОТ ВНУТРЕННИХ УГРОЗ:

выполнение требований на практике

Алексей Парфентьев

Заместитель генерального директора
по инновационной деятельности
«СёрчИнформ»

РЕГУЛИРОВАНИЕ ЗАЩИТЫ КИИ: ТЕНДЕНЦИИ И НАПРАВЛЕНИЯ

С 01.09.2025 вступили в силу поправки в Закон о КИИ (58-ФЗ от 07.04.2025)

- Установлен порядок выявления ОКИИ на основе отраслевых перечней
- Объектов КИИ, в т.ч. значимых, станет больше
- Круг субъектов КИИ расширится, в т.ч. за счет бюджетных организаций и МСП

Направления защиты

по 239-му Приказу ФСТЭК

- Организационные меры защиты
- Технические меры защиты от внешних угроз
- Технические меры защиты от внутренних угроз
- Технические меры защиты от смешанных угроз

>50% состава мер

КАКИЕ ТРЕБОВАНИЯ ОТНОСЯТСЯ К ВНУТРЕННЕЙ ИБ?

SEARCHINFORM

Мера ИБ	Для каких ЗОКИИ обязательна?
ЗНИ. 5 Контроль использования интерфейсов ввода-вывода информации на съемные машинные носители	1-3 категории значимости
АУД.9 Анализ действий отдельных пользователей	1 категория значимости
ОЦЛ.4 Контроль данных, вводимых в ИС	1-2 уровень значимости

и более 20 других мер

ГОСКИИ
ДОПОЛНИТЕЛЬНЫЕ ТРЕБОВАНИЯ

SEARCHINFORM

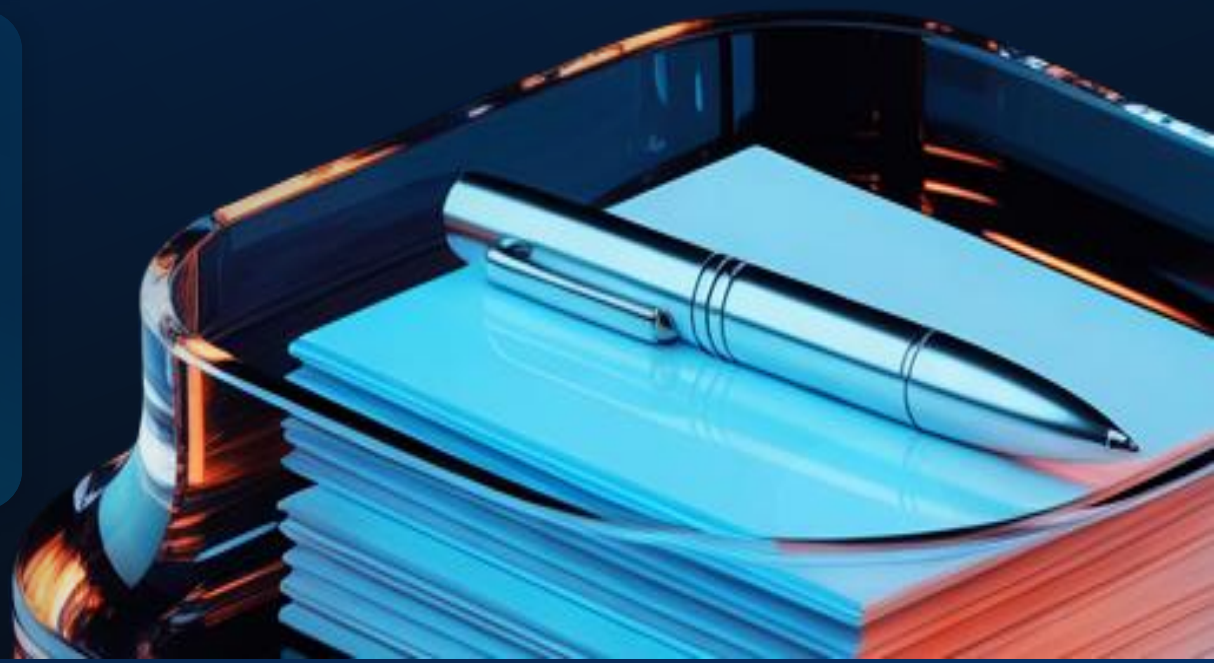
Приказ ФСТЭК № 117:

- Обязателен для ИС госсектора, отнесенных к ЗОКИИ в части, не противоречащей Приказу ФСТЭК № 239

6. В случае если информационная система является значимым объектом критической информационной инфраструктуры Российской Федерации, защита содержащейся в ней информации должна обеспечиваться в соответствии с нормативными правовыми актами, принятыми на основании статьи 6 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», и Требованиями.

Для государственных ЗОКИИ обязательны:

- Защита и контроль конечных точек
- Защита при передаче данных по e-mail
- Защита каналов передачи данных



КАКИЕ ОТРАСЛИ КИИ НАИБОЛЕЕ УЯЗВИМЫ ДЛЯ ВНУТРЕННИХ УГРОЗ?

Здравоохранение:
В **30%** организаций произошли внутренние ИБ-инциденты[1]

Финсектор
В **56%** организаций произошли внутренние ИБ-инциденты

Связь
В **43%** организаций произошли внутренние ИБ-инциденты

Транспорт
В **43%** организаций произошли внутренние ИБ-инциденты

- **«Пробив» данных о гражданах**
- **Выгрузка данных о деятельности организаций**
- **Внесение ложных сведений (например, о вакцинации, о заключении договоров)**

1 – Исследование уровня информационной безопасности в организациях России. Итоги 2024. ООО «СёрчИнформ»

ЧЕМ ВЫПОЛНЯТЬ ТРЕБОВАНИЯ?

ПРИКАЗ ФСТЭК № 239

- УПД.2 Реализация модели управления доступом
- ОПС.1 Управление запуском и обращениями компонентов ПО
- ЗНИ.5 Контроль использования интерфейсов ввода-вывода информации на съемные носители
- ЗНИ.6 Контроль ввода-вывода информации на съемные носители
- ЗНИ.7 Контроль подключения съемных носителей информации
- АУД.9 Анализ действий отдельных пользователей
- ОЦЛ.3 Ограничения по вводу информации в ИС
- ОЦЛ.4 Контроль данных, вводимых в ИС
- ЗИС.17 Защита информации от утечек

и более 30 других требований

ПРИКАЗ ФСТЭК № 117

- Защита конечных устройств
- Защита сервисов электронной почты
- Регистрация событий безопасности

и более 10 других требований

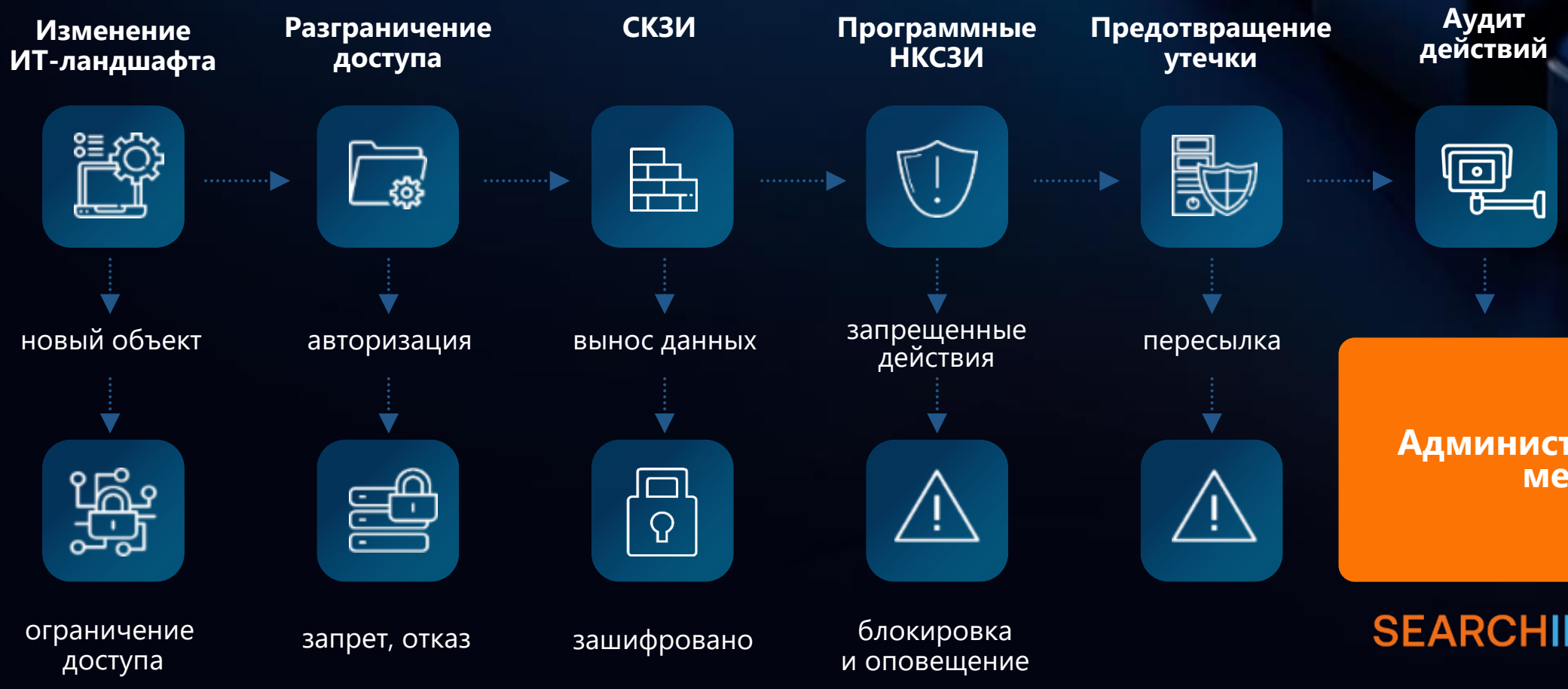
Выполняются полностью или в части с помощью

DCAP- и DLP-СИСТЕМ

SEARCHINFORM

DLP\DCAP ДЛЯ ЗАЩИТЫ КИИ:
ЗАДАЧИ ЗАЩИТЫ ДАННЫХ

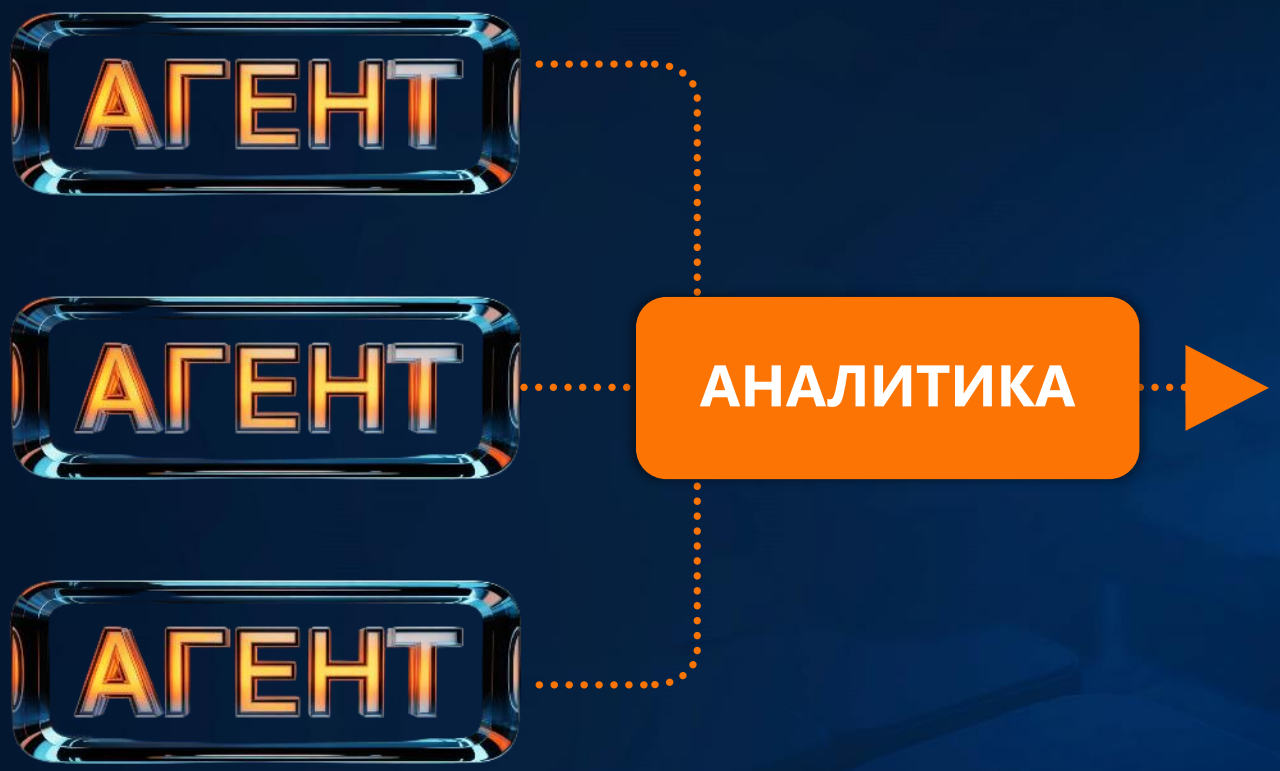
DLP И DCAP ДЛЯ ЗАЩИТЫ КИИ:
ЗАДАЧИ ЗАЩИТЫ ИНФРАСТРУКТУРЫ



SEARCHINFORM

DLP ДЛЯ ЗАЩИТЫ КИИ: ИНВЕНТАРИЗАЦИЯ ПО, АРМ И УЧЕТНЫХ ЗАПИСЕЙ

SEARCHINFORM



КАРТОЧКА ПОЛЬЗОВАТЕЛЯ

- Отчеты об установке и применении ПО, использовании сайтов
- Карта АРМ с расположением
- Все используемые учетки
- Отчет о логинах с корпоративными данными на посторонних сервисах

DLP ДЛЯ ЗАЩИТЫ КИИ:
РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ

- Графы по связям пользователей
- Отчеты о перемещении файлов
- Поиск по различным видам активности

SEARCHINFORM

DLP ДЛЯ ЗАЩИТЫ КИИ:
АУДИТ ХРАНЕНИЯ ДАННЫХ

SEARCHINFORM

НУЖНО ОПРЕДЕЛИТЬ:

- Категорию защищаемой информации
- Место хранения информации
- Кто имеет доступ к информации

НУЖНО ОБНАРУЖИВАТЬ И УЧИТЫВАТЬ:

- Факты доступа к данным
- Факты создания, изменения, перемещения, удаления, передачи данных

DLP ДЛЯ ЗАЩИТЫ КИИ:
ВОВЛЕЧЕНИЕ СОТРУДНИКОВ В ИБ

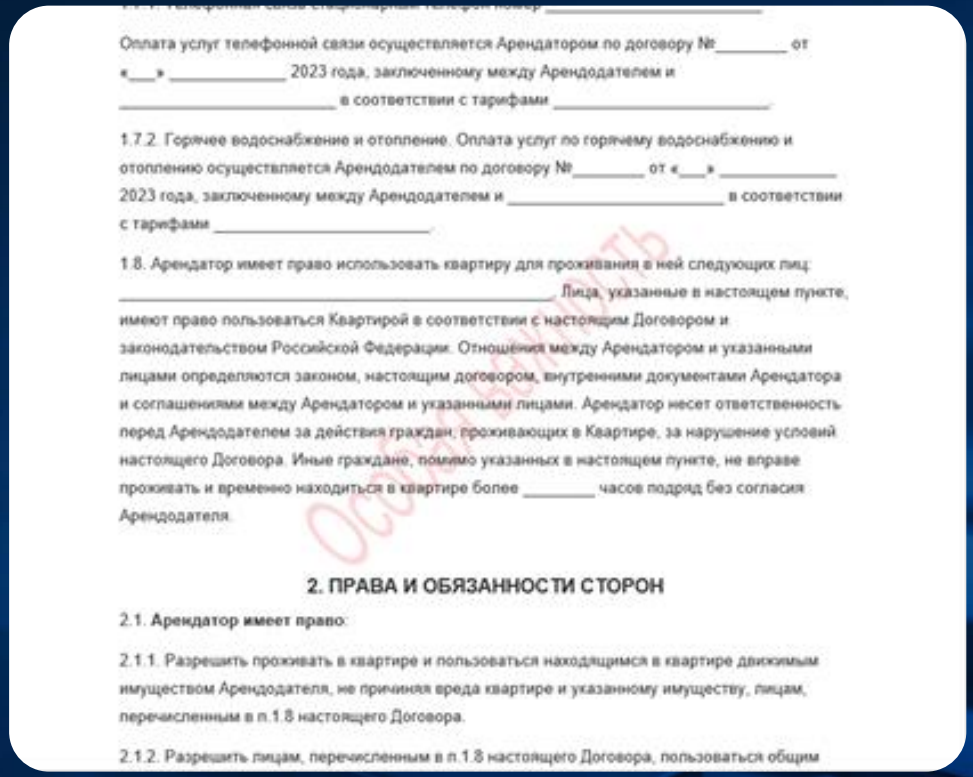
SEARCHINFORM

УВЕДОМЛЯЕМ ПОЛЬЗОВАТЕЛЯ:

- О срабатывании СЗИ
- О блокировке доступа

ПОЗВОЛЯЕМ ПОЛЬЗОВАТЕЛЮ:

- Общаться напрямую с ИБ-службой
- Указывать, какие данные требуют защиты
- Участвовать в категоризации данных



Оплата услуг телефонной связи осуществляется Арендатором по договору №_____ от «___» _____ 2023 года, заключенному между Арендодателем и _____ в соответствии с тарифами _____.

1.7.2. Горячее водоснабжение и отопление. Оплата услуг по горячему водоснабжению и отоплению осуществляется Арендодателем по договору №_____ от «___» _____ 2023 года, заключенному между Арендодателем и _____ в соответствии с тарифами _____.

1.8. Арендатор имеет право использовать квартиру для проживания в ней следующих лиц: _____. Лица, указанные в настоящем пункте, имеют право пользоваться Квартирой в соответствии с настоящим Договором и законодательством Российской Федерации. Отношения между Арендатором и указанными лицами определяются законом, настоящим договором, внутренними документами Арендатора и соглашениями между Арендатором и указанными лицами. Арендатор несет ответственность перед Арендодателем за действия граждан, проживающих в Квартире, за нарушение условий настоящего Договора. Иные граждане, помимо указанных в настоящем пункте, не вправе проживать и временно находиться в квартире более _____ часов подряд без согласия Арендодателя.

2. ПРАВА И ОБЯЗАННОСТИ СТОРОН

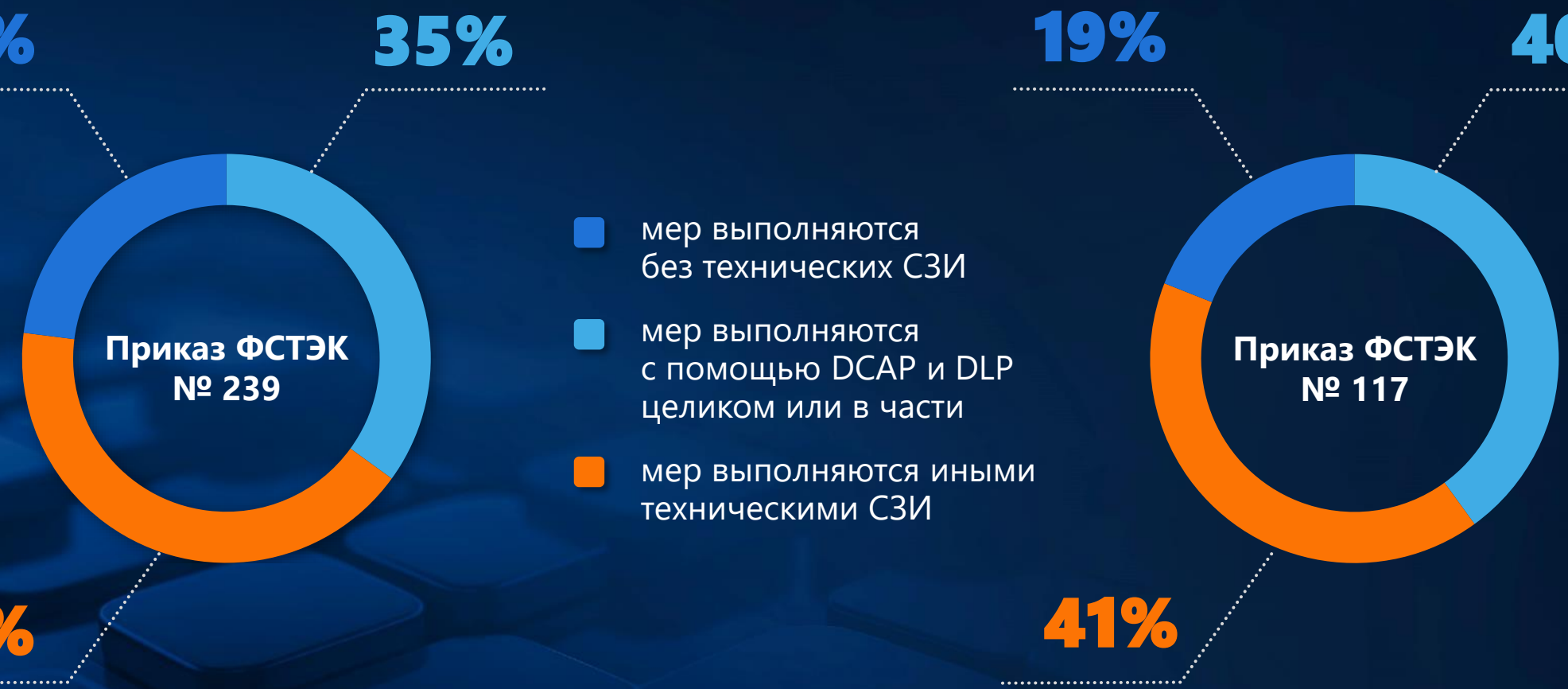
2.1. **Арендатор имеет право**:

2.1.1. Разрешить проживать в квартире и пользоваться находящимся в квартире движимым имуществом Арендодателя, не причиняя вреда квартире и указанному имуществу, лицам, перечисленным в п.1.8 настоящего Договора.

2.1.2. Разрешить лицам, перечисленным в п.1.8 настоящего Договора, пользоваться общим

DCAP И DLP ДЛЯ ЗАЩИТЫ КИИ: ИТОГИ

SEARCHINFORM



СПАСИБО ЗА ВНИМАНИЕ!

SEARCHINFORM

https://t.me/searchinform

https://vk.com/securityinform

ПРАКТИКА И АНАЛИТИКА

https://searchinform.ru/practice-and-analytics/