itprotect

АТТЕСТАЦИЯ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

как не придумывать себе сложности а сэкономить время, деньги и нервы

Роман Писарев

Руководитель департамента
аудита и консалтинга iTPROTECT

Когда аттестация неизбежна?

1. Если это государственная информационная система
2. Если есть требования со стороны системы, к которой подключаетесь
3. Если есть требования со стороны головной компании
4. Если так решило руководство

itprotect

ОСОБЕННОСТИ
ПРИКАЗА ФСТЭК РОССИИ № 77

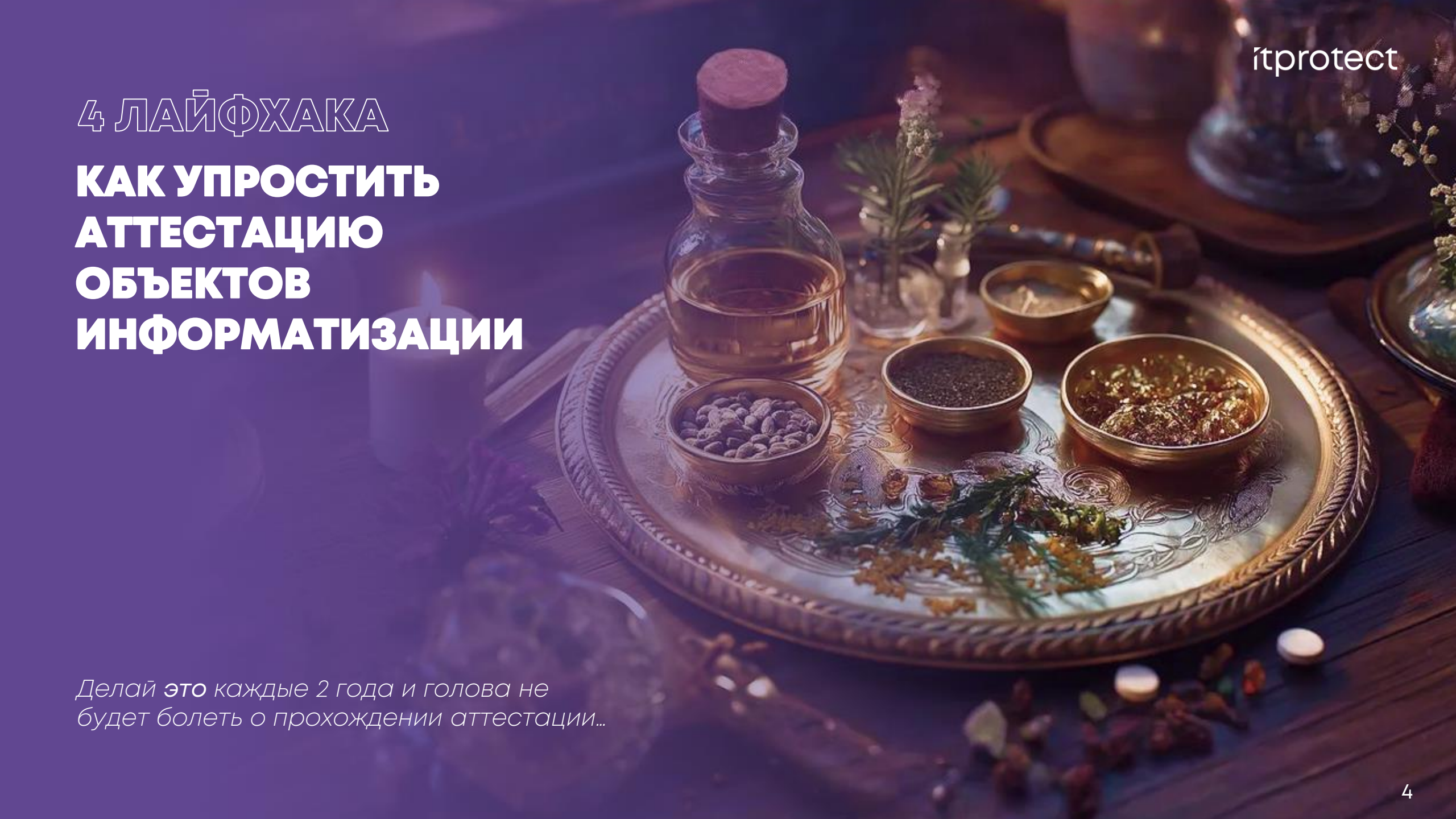
- ☑ Зафиксированы все признаки хорошего аудита:
  - ✓ Определена и подробно описана процедура аттестации
  - ✓ Определены роли участников и их обязанности
  - ✓ Определено содержание отчетных документов, утверждены формы некоторых из них
- ☑ Результат будет значимым
- ☑ Аттестаты действуют бессрочно

✗ Нужно отправлять информацию во ФСТЭК России

itprotect

4 ЛАЙФХАКА

КАК УПРОСТИТЬ АТТЕСТАЦИЮ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ



*Делай **это** каждые 2 года и голова не будет болеть о прохождении аттестации...*

ЛАЙФХАК №1

НЕ ГРУЗИТЕ ФСТЭК БУМАГОЙ

Если вы аттестовываете не ГИС, то отправки документов можно избежать

Настоящий Порядок распространяется на аттестацию на соответствие требованиям по защите информации (далее - аттестация) следующих объектов информатизации:

- ✓ **государственных и муниципальных информационных систем**, в том числе государственных, муниципальных информационных систем персональных данных;
- ✓ **информационных систем управления производством,** используемых организациями оборонно-промышленного комплекса, в том числе автоматизированных систем станков с числовым программным управлением;
- ✓ помещений, предназначенных для ведения конфиденциальных переговоров (далее - защищаемые помещения).

Настоящий Порядок применяется также для аттестации следующих объектов информатизации, для которых их владельцами установлено требование по проведению оценки соответствия систем защиты информации этих объектов требованиям по защите информации в форме аттестации:

- ✓ **значимых объектов критической информационной инфраструктуры** Российской Федерации;
- ✓ информационных **систем персональных данных** (за исключением государственных, муниципальных информационных систем персональных данных);
- ✓ **автоматизированных систем управления производственными и технологическими процессами** на критически важных объектах, потенциально опасных объектах, объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды.

itprotect

Если вы аттестовываете не ГИС, то отправки документов можно избежать

Требуется: Аттестовать несколько объектов (например, несколько ОКИИ)

Решение: Объединить ОКИИ в один ОИ и дать ему новое название (например, «Сегмент объектов КИИ»)

Выводы: Такой «объединенный» ОИ уже не будет ОКИИ, и перестает подпадать под требования по отправке документов во ФСТЭК

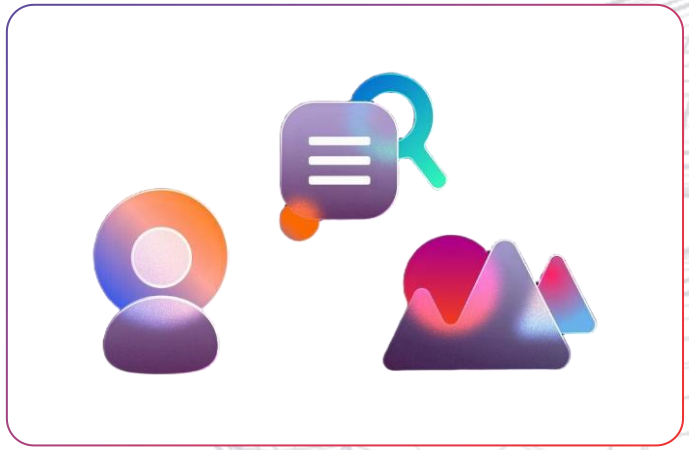
☑ Нужно отправлять документы во ФСТЭК

ОКИИ «Заводская лаборатория»

ОКИИ «Центр обработки данных»

ОКИИ «АСУ ТП производства»

✕ Не нужно отправлять документы во ФСТЭК



Сегмент объектов КИИ

itprotect

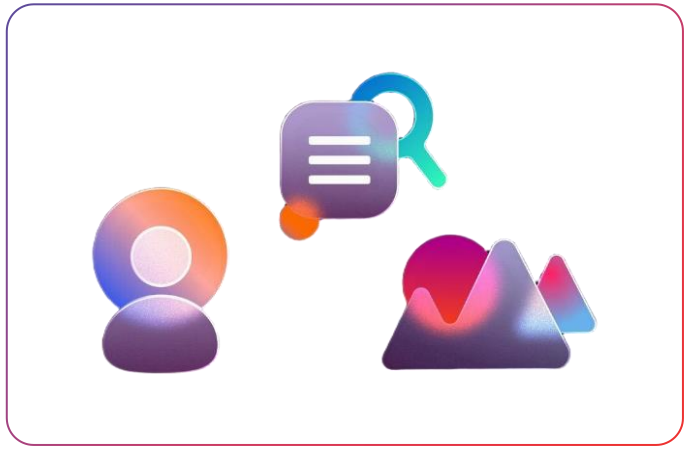
Если вы аттестовываете не ГИС, то отправки документов можно избежать

Требуется: АРМ для подключения к «чужому» ОКИИ или ГИС

Решение: Не классифицируйте (если это возможно) этот ОИ как ГИС или ОКИИ

Выводы: Такой ОИ будет «ненастоящим» ГИС или ОКИИ и перестает подпадать под требования по отправке документов во ФСТЭК

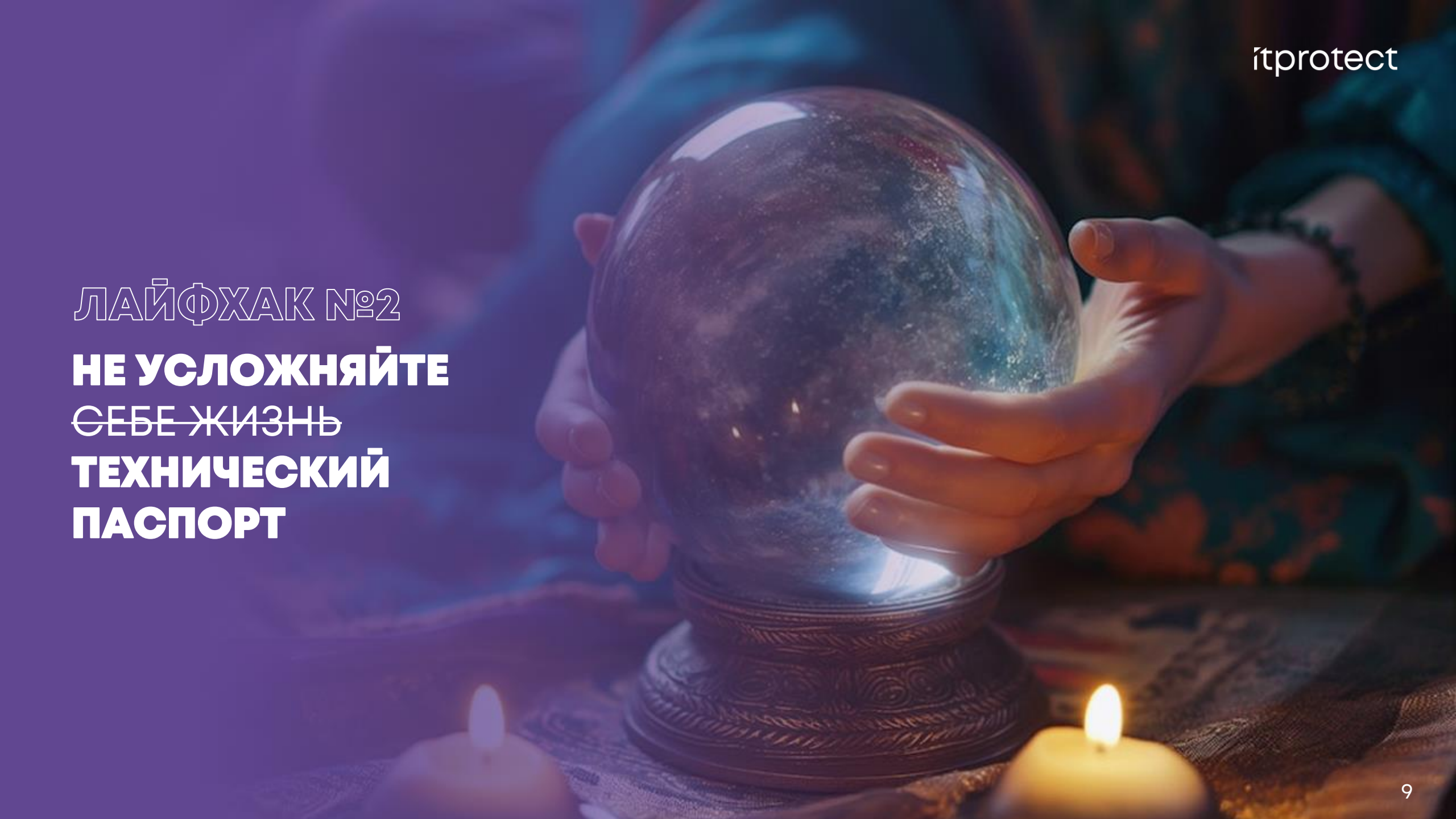
☑ Нужно отправлять документы во ФСТЭК



ГИС «АРМ для подключения к ГИС»

✕ Не нужно отправлять документы во ФСТЭК

ОИ «АРМ для подключения к ГИС»



itprotect

ЛАЙФХАК №2

НЕ УСЛОЖНЯЙТЕ ~~СЕБЕ ЖИЗНЬ~~ ТЕХНИЧЕСКИЙ ПАСПОРТ

Если внимательно прочитать приказ, то станет ясно, что не нужно отправлять лишнюю информацию

Можно не переписывать серийные заводские номера (серверов, мониторов, телефонов, принтеров, мышек и т.д.), не указывать места установки ПО и все остальное, что не требует форма тех. паспорта

3. Состав информационной (автоматизированной) системы.

3.1. Состав программно-технических средств информационной (автоматизированной) системы: _____.

(указываются типы технических средств, их наименования и модели)

3.2. Состав общесистемного и прикладного программного обеспечения информационной (автоматизированной) системы: _____.

(указываются типы программного обеспечения, их наименования и основные (мажорные) версии)

3.3. Состав телекоммуникационного оборудования информационной (автоматизированной) системы и используемые для передачи информации линии связи: _____.

(указываются типы оборудования, их наименования и основные (мажорные) версии)

3.4. Состав средств защиты информации, используемых в информационной (автоматизированной) системе: _____ _____.

(указываются типы средств, их наименования и основные (мажорные) версии, сведения о сертификатах соответствия)

Техпаспорт на ОИ оформляется по форме, согласно приложениям N 1, 2.
Для ОИ ИС:

itprotect

ЛАЙФХАК №3

БЕРЕГИТЕ ЛЕС!

itprotect

Обратите внимание, что часть документов отправляются «в случае разработки»

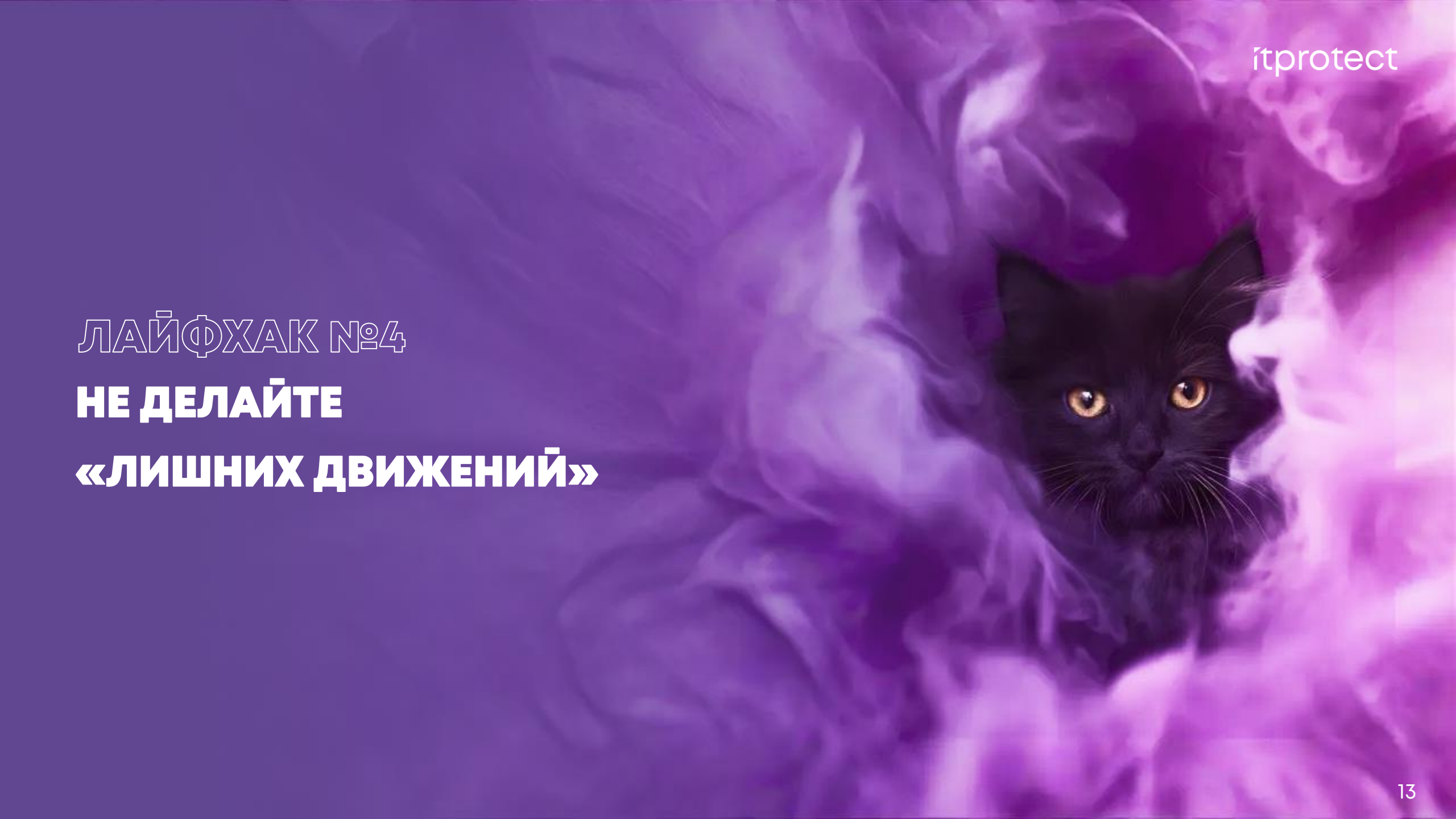
То есть, если у вас их нет, то и разрабатывать специально для аттестации не нужно

- технический паспорт на объект информатизации по форме согласно приложениям N 1, 2 к настоящему Порядку;
- акт классификации информационной (автоматизированной) системы по форме согласно приложению N 3 к настоящему Порядку, акт категорирования значимого объекта критической информационной инфраструктуры Российской Федерации (далее - акт категорирования значимого объекта);
- модель угроз безопасности информации (**в случае ее разработки** в соответствии с требованиями по защите информации);
- техническое задание на создание (развитие, модернизацию) объекта информатизации и (или) частное техническое задание на создание (развитие, модернизацию) системы защиты информации объекта информатизации (для объекта информатизации, входящего в состав объекта капитального строительства, задание на проектирование (реконструкцию) объекта капитального строительства) **(в случае их разработки** в ходе создания объекта информатизации);
- проектную документацию на систему защиты информации объекта информатизации (**в случае ее разработки** в ходе создания объекта информатизации);
- эксплуатационную документацию на систему защиты информации объекта информатизации и применяемые средства защиты информации;
- организационно-распорядительные документы по защите информации владельца объекта информатизации, регламентирующие защиту информации в ходе эксплуатации объекта информатизации, в том числе план мероприятий по защите информации на объекте информатизации, документы по порядку оценки угроз безопасности информации, управлению (администрированию) системой защиты информации, управлению конфигурацией объекта информатизации, реагированию на инциденты безопасности, информированию и обучению персонала, контролю за обеспечением уровня защищенности информации (далее - документы по защите информации владельца объекта информатизации);
- документы, содержащие результаты анализа уязвимостей объекта информатизации и приемочных испытаний системы защиты информации объекта информатизации (**в случае проведения анализа** и испытаний в ходе создания объекта информатизации).

itprotect

ЛАЙФХАК №4

НЕ ДЕЛАЙТЕ «ЛИШНИХ ДВИЖЕНИЙ»



В Приказе указано, что делать, когда у вас меняется аттестованный ОИ

Как выглядит п.33 в приказе:

33. В случае развития (модернизации) объекта информатизации, в ходе которого изменена конфигурация (параметры настройки) программных, программно-технических средств и средств защиты информации, исключены программные, программно-технические средства и средства защиты информации, дополнительно включены аналогичных средств или заменены на аналогичные средства проводятся дополнительные аттестационные испытания в соответствии с настоящим Порядком. Сведения об изменениях аттестованного объекта информатизации и проведенных при этом аттестационных испытаниях включаются владельцем объекта информатизации в технический паспорт. Действие аттестата соответствия не прекращается.

В случае развития (модернизации) объекта информатизации, приводящего к повышению класса защищенности (уровня защищенности, категории значимости) объекта информатизации и (или) к изменению архитектуры системы защиты информации объекта информатизации в части изменения видов и типов программных, программно-технических средств и средств защиты информации, изменения структуры системы защиты информации, состава и мест расположения объекта информатизации и его компонентов, проводится повторная аттестация в соответствии с настоящим Порядком.

В Приказе указано, что делать, когда у вас меняется аттестованный ОИ

Вот как нужно его трактовать:

33. В случае развития (модернизации) объекта информатизации, в ходе которого изменена
- ✓ конфигурация (параметры настройки) программных, программно-технических средств и средств защиты информации,
- ✓ исключены программные, программно-технические средства и средства защиты информации,
- ✓ дополнительно включены ~~аналогичные~~ средства или заменены на аналогичные средства

проводятся дополнительные аттестационные испытания в соответствии с настоящим Порядком.

В случае развития (модернизации) объекта информатизации, приводящего:

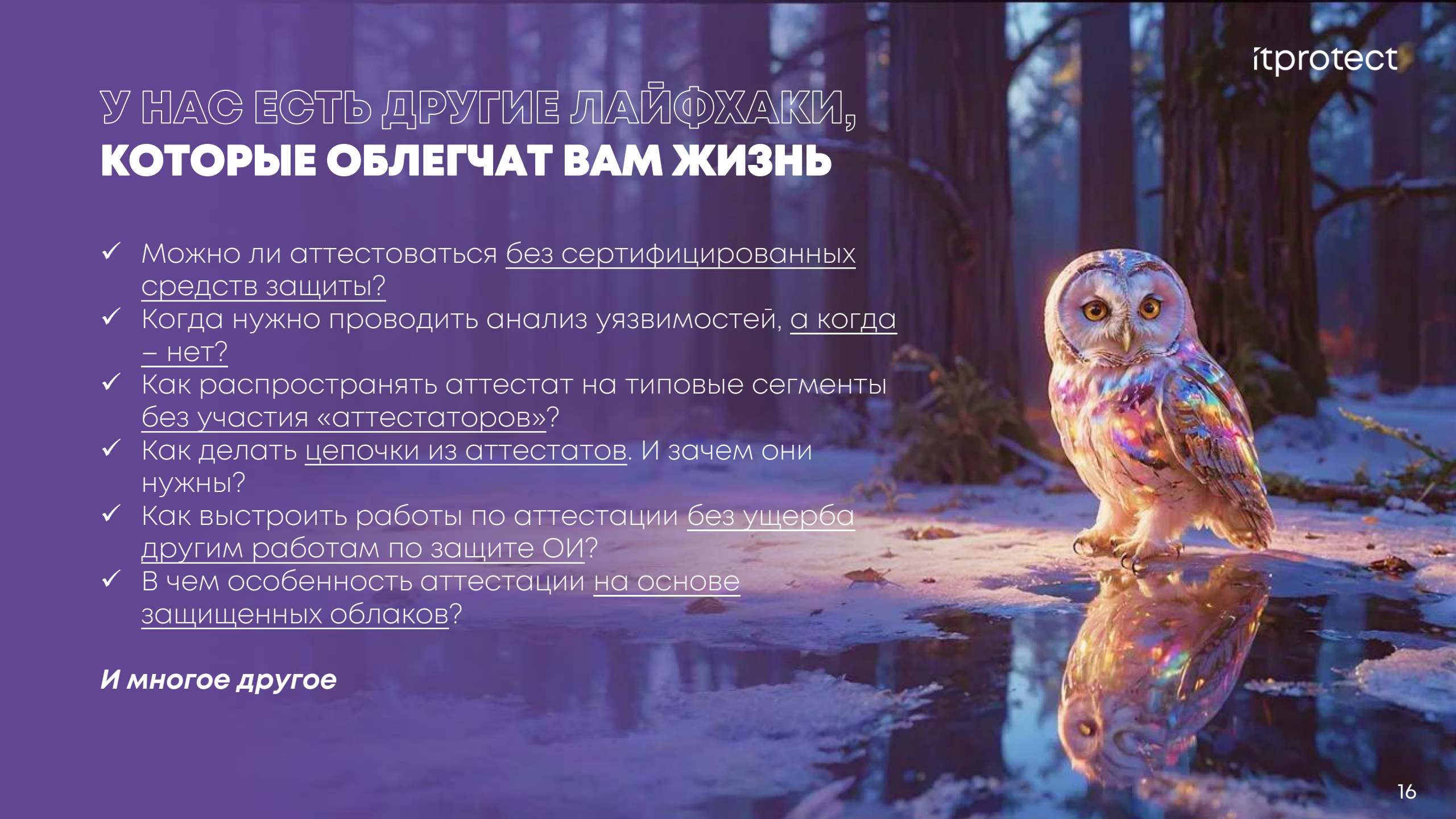
- ✓ к повышению класса защищенности (уровня защищенности, категории значимости) объекта информатизации;
- ✓ и (или) к изменению архитектуры системы защиты информации объекта информатизации в части:
  - изменения видов и типов программных, программно-технических средств и средств защиты информации,
  - изменения структуры системы защиты информации, состава и мест расположения объекта информатизации и его компонентов,

проводится повторная аттестация в соответствии с настоящим Порядком

У НАС ЕСТЬ ДРУГИЕ ЛАЙФХАКИ, **КОТОРЫЕ ОБЛЕГЧАТ ВАМ ЖИЗНЬ**

- ✓ Можно ли аттестоваться без сертифицированных средств защиты?
- ✓ Когда нужно проводить анализ уязвимостей, а когда – нет?
- ✓ Как распространять аттестат на типовые сегменты без участия «аттестаторов»?
- ✓ Как делать цепочки из аттестатов. И зачем они нужны?
- ✓ Как выстроить работы по аттестации без ущерба другим работам по защите ОИ?
- ✓ В чем особенность аттестации на основе защищенных облаков?

И многое другое



itprotect

ДЛЯ ВАШИХ ВОПРОСОВ:
EXPERT@ITPROTECT.RU

ИЛИ ОСТАВЬТЕ ЗАЯВКУ **НА БЕСПЛАТНУЮ КОНСУЛЬТАЦИЮ** НА САЙТЕ

И ПОДХОДИТЕ НА НАШ СТЕНД,
ОБСУДИМ ВАШИ ЗАДАЧИ