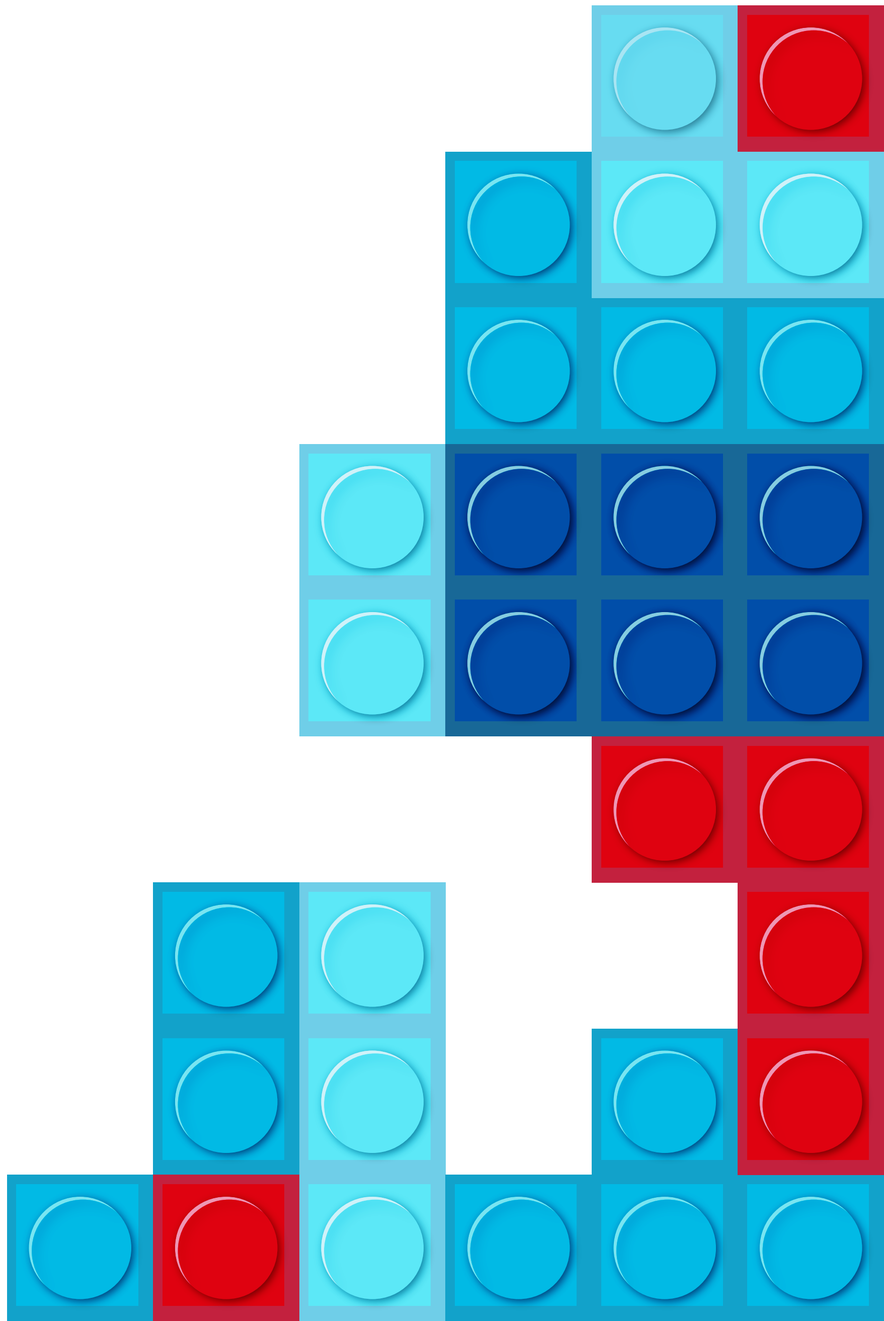
Модель угроз и никаких облаков

Конструктор–У



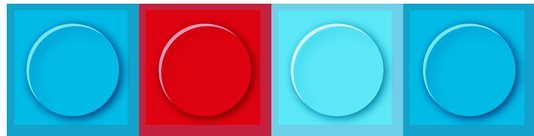
Спикер: Ковалько Владимир

Ведущий менеджер отдела комплексных предпродажных решений ARinteg

Компетенции

Много задач. Разные направления. Один исполнитель.

- Антивирусная защита
- Защита от несанкционированного доступа
- Межсетевое экранирование
- Мониторинг защищенности сетевых сервисов
- Управление учётными записями
- Построение защищенных каналов связи — VPN-систем
- Сканирование уязвимостей
- Управление уязвимостями
- Криптографическая защита информации
- Управление событиями информационной безопасности
- Защита конфиденциальной информации от утечки
- Защита виртуальной среды инфраструктуры
- Противодействие целевым атакам
- Защита почтового и веб-трафика
- Защита центров обработки данных
- Защита персональных данных (ПДн)
- Контроль привилегированных пользователей
- Аудит и консалтинг
- Видеонаблюдение и инженерные системы
- Безопасность корпоративных устройств
- Реализация серверных решений и СХД
- Разворачивание программных инфрастуктурных решений
- Реализация сетевых решений для инфраструктуры
- Поставка персональных систем для офиса и сопутствующей переферии



Сертификаты и лицензии

ЛИЦЕНЗИИ ФСТЭК

На деятельность по разработке и производству средств защиты конфиденциальной информации от 23 июня 2017 г. № 1764

На деятельность по технической защите конфиденциальной информации от 23 июня 2017 г. № 3319

ЛИЦЕНЗИЯ МЧС

МЧС по монтажу, техническому обслуживанию и ремонту средств обеспечения пожарной безопасности зданий и сооружений от 21 октября 2020 г. № 77-Б/08112

ЛИЦЕНЗИИ ФСБ

Лицензия УФСБ России на проведение работ, связанных с использованием сведений, составляющих государственную тайну от 05 февраля 2025 г. № 0136621

Лицензия ФСБ России на осуществление разработки, производства, распространения шифровальных средств от 18 декабря 2017 г. № 16355Н

СЕРТИФИКАТ

Соответствия системы менеджмента качества стандарту ISO 9001:2015 (ГОСТ Р ISO 9001-2015) от 26.10.2022 г. № СДС.ФМР.СМ000009-22

Собственные разработки

МОДЕЛЬ УГРОЗ
И НИКАКИХ ОБЛАКОВ

КОНСТРУКТОР
версия-у

ВКЛЮЧЕН В РЕЕСТР
ОТЕЧЕСТВЕННОГО ПО
№15721 от 05.12.2022 г.

ARZip
АРХИВАТОР

ВКЛЮЧЕН В РЕЕСТР
ОТЕЧЕСТВЕННОГО ПО
№16999 от 21.03.2023 г.

SAVA
СИСТЕМА МОНИТОРИНГА
СОБЫТИЙ ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

ВКЛЮЧЕН В РЕЕСТР
ОТЕЧЕСТВЕННОГО ПО
№10346 от 21.04.2021

Модуль «Учёт персональных данных»

Требования регуляторов по разработке «Модели угроз и нарушителя безопасности информации»

Модель угроз необходима для исполнения требований регуляторов в отношении:

- 187-ФЗ – значимых объектов критической информационной инфраструктуры
- 152-ФЗ – информационных систем персональных данных
- Приказа № 17 ФСТЭК России – государственных информационных систем

Организации в среднем необходимо от 5 Моделей угроз

Федеральный закон от 30.11.2024 г. №420-ФЗ

Неуведомление об утечке – штраф от 1 до 3 млн рублей

3-5 млн рублей – утечка данных 1-10 тыс. субъектов и/или 10-100 тыс. идентификаторов
...

15-20 млн рублей – утечка биометрических данных независимо от количества субъектов

Повторная утечка – 1-3% совокупной годовой выручки, но в пределах 20-500 млн рублей

Повторная утечка специальных/биометрических данных – 1-3% совокупной годовой выручки, но в пределах 25-500 млн рублей

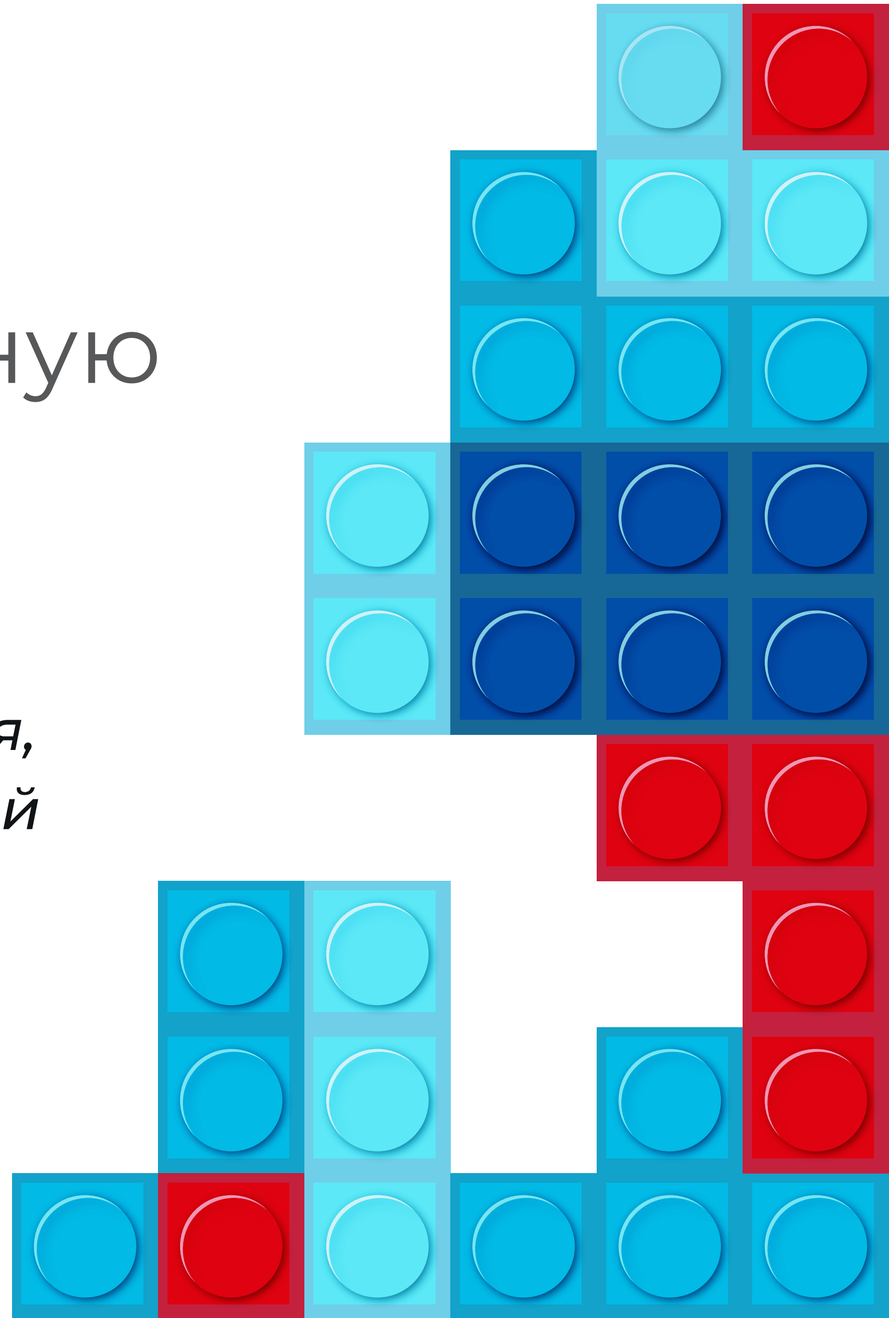
Штрафы за утечку вступили в силу с 30 мая 2025 г.

ЗАКОНОПРОЕКТ

УК РФ Статья 274.1.

Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации

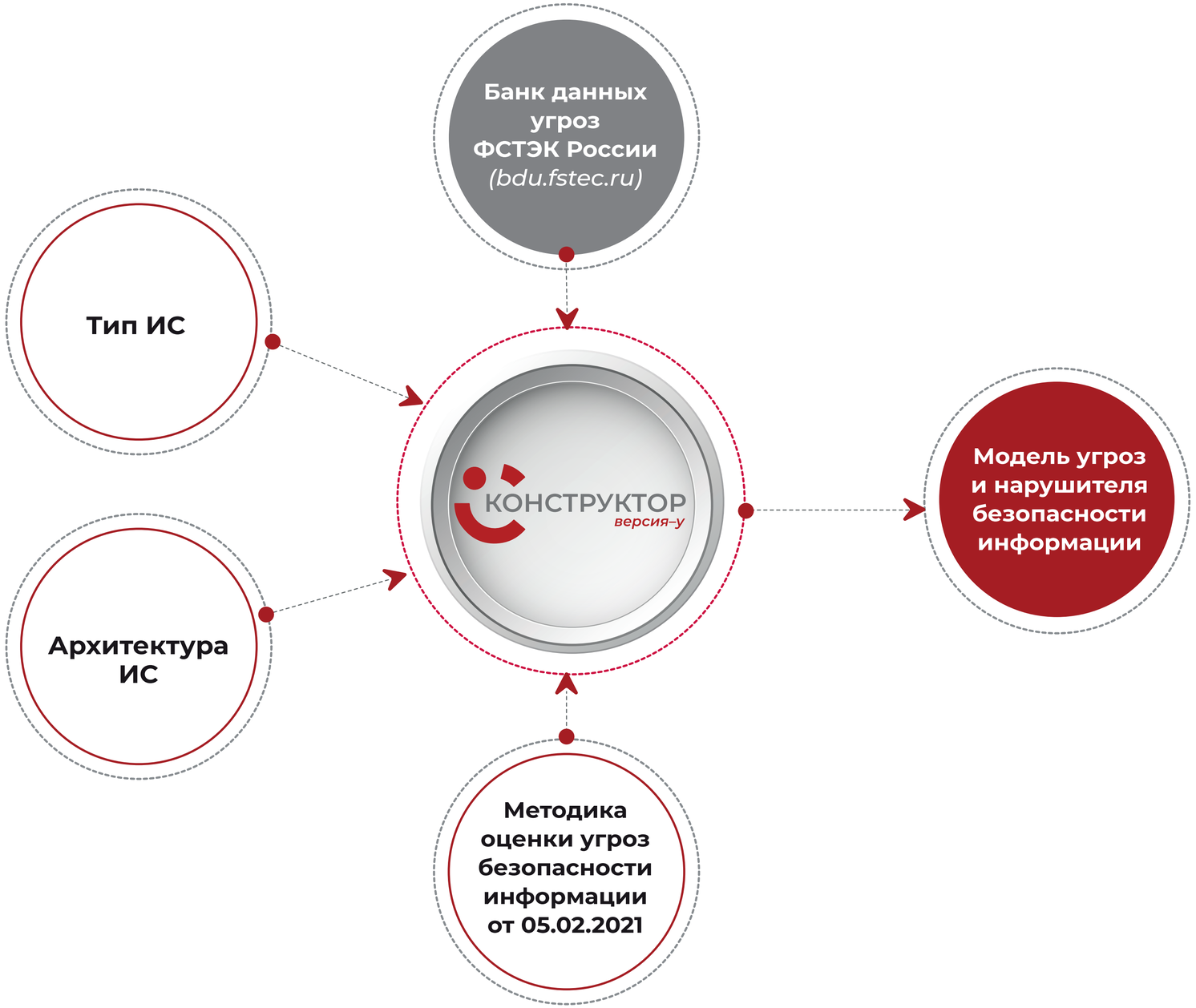
Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации .... ***наказываются лишением свободы на срок от 5 до 10 лет***



Конструктор–У позволяет разработать документ «Модель угроз и нарушителя безопасности информации». Для работы с ПО достаточно базовых знаний в области информационной безопасности

«Методический документ. Методика оценки угроз безопасности информации» (утв. ФСТЭК России 05.02.2021)

КОНСТРУКТОР версия–у



Разработка Модели угроз

Моделирование угроз проводится для 227 угроз из БДУ ФСТЭК России

Конструктор–У работает на ОС Windows и отечественных Linux платформах, в том числе в закрытом контуре

Алгоритм Конструктор-У

Негативные последствия

Возможные объекты воздействия

Потенциал нарушителя

Способы реализации угроз

Угрозы применительно к рассматриваемой инфраструктуре

Алгоритм методики ФСТЭК России

best practices в области ИБ

Исходные данные

Тип информационной системы

Информация об объекте защиты

В автоматизированный процесс создания документа можно вносить экспертные мнения специалистов компании

При внесении изменений в инфраструктуру ИС модель угроз автоматически актуализируется

Конструктор–У:

Позволяет самостоятельно подготовить документ – «Модель угроз и нарушителя безопасности информации» и оперативно его скорректировать при изменениях в инфраструктуре

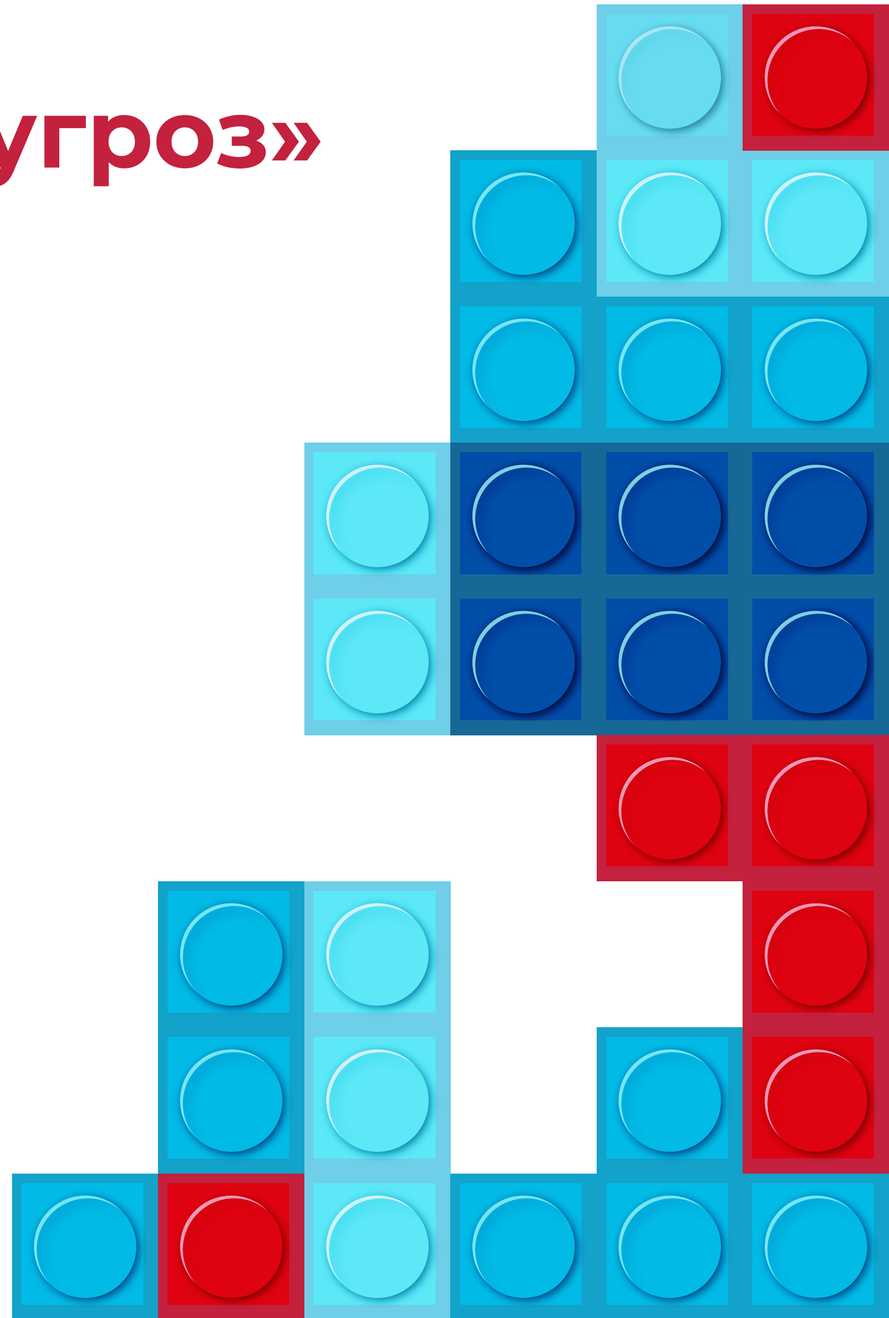
Упрощает сбор информации со всех подразделений организации (по всем ИС) за счет унификации

При изменении регуляторной базы позволяет получить бесплатные обновления в рамках техподдержки

Отсутствие избыточности функционала

При формировании «Модели угроз» Конструктор–У:

- Использует нормативную базу ФСТЭК России и best practices в области ИБ
- Позволяет вносить экспертные мнения специалистов компании в автоматизированный процесс создания документа
- **Работает в том числе в закрытом контуре**



Спасибо за внимание!

Подписывайтесь
на наш телеграм-канал