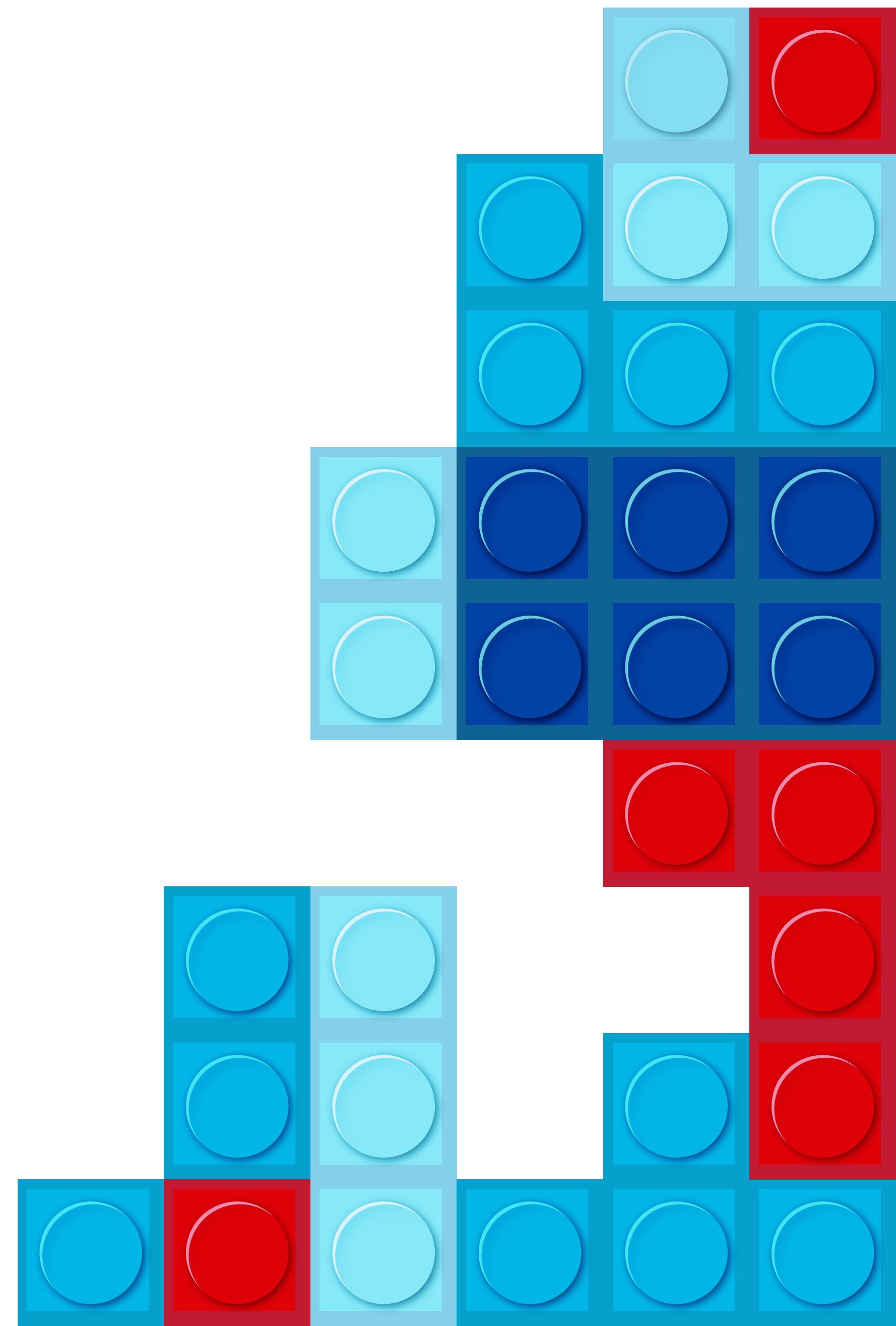


Модель угроз и никаких облаков

Конструктор-У



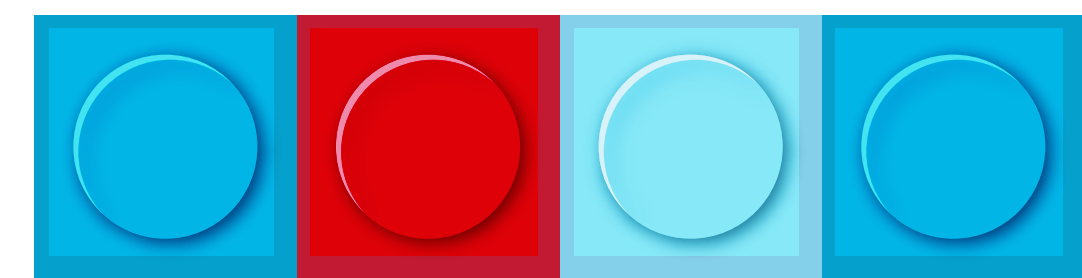
Дмитрий Слободенюк
коммерческий директор ARinteg



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



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



ЛИЦЕНЗИИ ФСБ

Лицензия УФСБ России на проведение работ, связанных с использованием сведений, составляющих государственную тайну



ЛИЦЕНЗИЯ МЧС

МЧС по монтажу, техническому обслуживанию и ремонту средств обеспечения пожарной безопасности зданий и сооружений



СЕРТИФИКАТ

Соответствия системы менеджмента качества стандарту ISO 9001:2015 (ГОСТ Р ISO 9001-2015)



ЛИЦЕНЗИЯ МИНОБОРОНЫ РОССИИ

Наши партнёры

The image displays a collection of logos for various technology and security partners. The logos are arranged in a grid-like fashion within a light blue rounded rectangle. The partners include:

- kaspersky
- positive technologies
- INFOWATCH
- ИНДИД
- ideco
- Security Vision
- АЙТИБАСТИОН
- APPSEC SOLUTIONS
- Аладдин
- с-терра
- СПЕЦИАЛЬНАЯ ИНТЕГРАЦИЯ
- ZECURION
- infotecs
- DDOS-GUARD
- Dr.WEB
- SMART-SOFT
- ASTRA LINUX
- Эшелон комплексная безопасность
- МТC RED
- phishman
- express
- AVANPOST
- Вебмониторэкс защита веб-приложений и API
- КОД безопасности
- perimetrix
- PRO32
- SEARCHINFORM INFORMATION SECURITY
- КИБЕРПРОТЕКТ
- FUTURE CREW
- basealt
- РЕДСОФТ
- EDGE ЦЕНТР
- Р7-ОФИС
- Контур staffcop
- МойОфис
- AQUARIUS
- CONTENT AI
- РОСА
- udv|group
- solidwall
- ГАРДА
- МАКVES
- Стахановец
- ASCCON
- КОНФИДЕНТ
- СИСТЕМЫ ЗАЩИТЫ ДАННЫХ
- UserGate
- КОМПАНИЯ АКТИВ
- РУТОКЕН
- SOLAR
- RUSIEM
- R-Vision
- ЦИФРОВЫЕ РЕШЕНИЯ
- xello
- САТЕЛ
- КРИПТОПРО
- SecretTechnologies
- Цифровые технологии
- ГИС ГАЗИНФОРМ СЕРВИС
- DEPO [computers]
- servicepipe

Собственные разработки

ВКЛЮЧЕН В РЕЕСТР
ОТЕЧЕСТВЕННОГО ПО
№15721 от 05.12.2022 г.



ВКЛЮЧЕН В РЕЕСТР
ОТЕЧЕСТВЕННОГО ПО
№16999 от 21.03.2023 г.



ВКЛЮЧЕН В РЕЕСТР
ОТЕЧЕСТВЕННОГО ПО
№10346 от 21.04.2021

**Модуль
«Учёт
персональных
данных»**

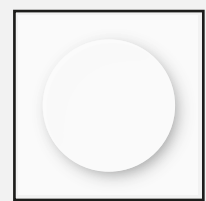
НОВАЯ РАЗРАБОТКА



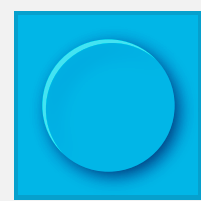
Требования регуляторов по разработке «Модели угроз и нарушителя безопасности информации»

Модель угроз необходима для исполнения требований регуляторов

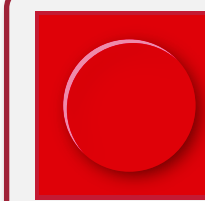
В ОТНОШЕНИИ:



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

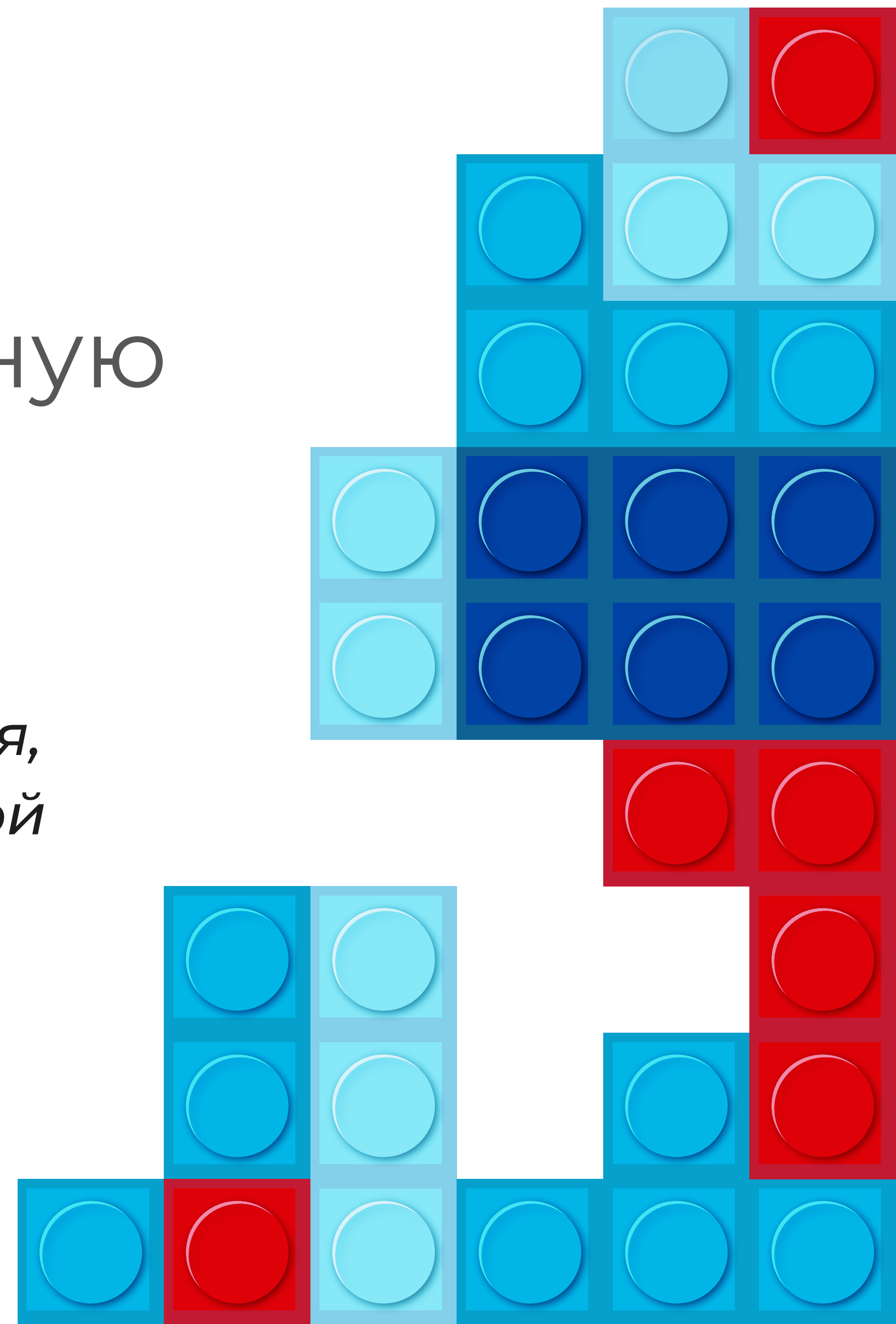


Штрафы за утечку вступают в силу с 30 мая 2025 г.

УК РФ Статья 274.1.

Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации

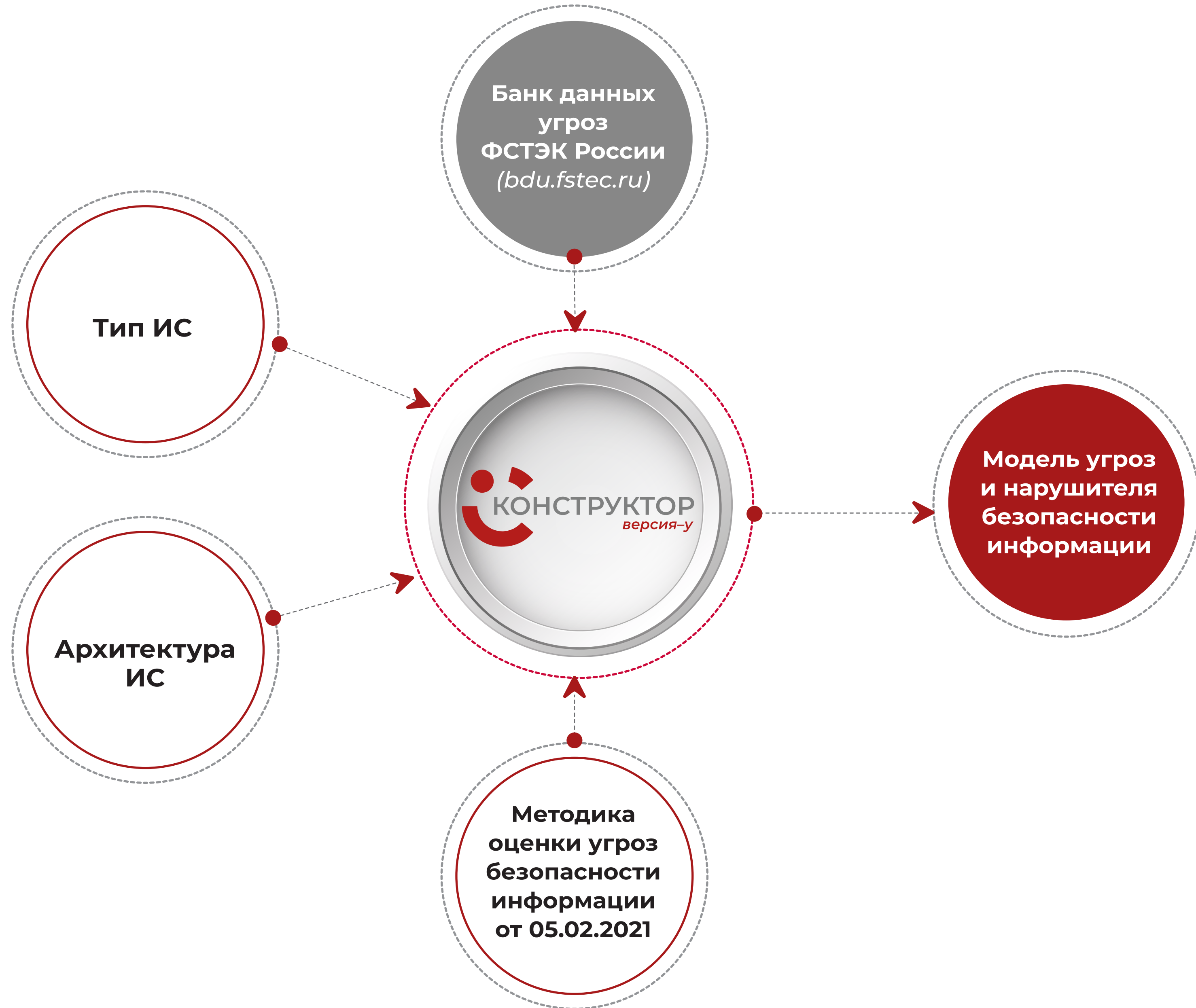
*Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации ... **наказываются лишением свободы на срок от 5 до 10 лет***



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)*





Разработка Модели угроз

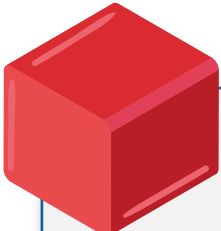
Моделирование угроз проводится для 222 угроз из БДУ ФСТЭК России

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

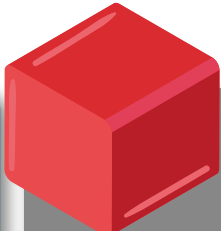
Алгоритм Конструктор-У



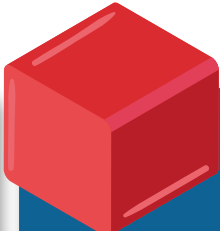
Конструктор-У:



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

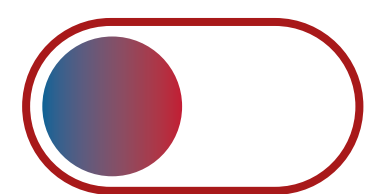


При изменении регуляторной базы позволяет получить бесплатные обновления в рамках техподдержки

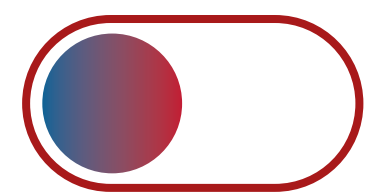


Отсутствие избыточности функционала

При формировании «Модели угроз» Конструктор-У:



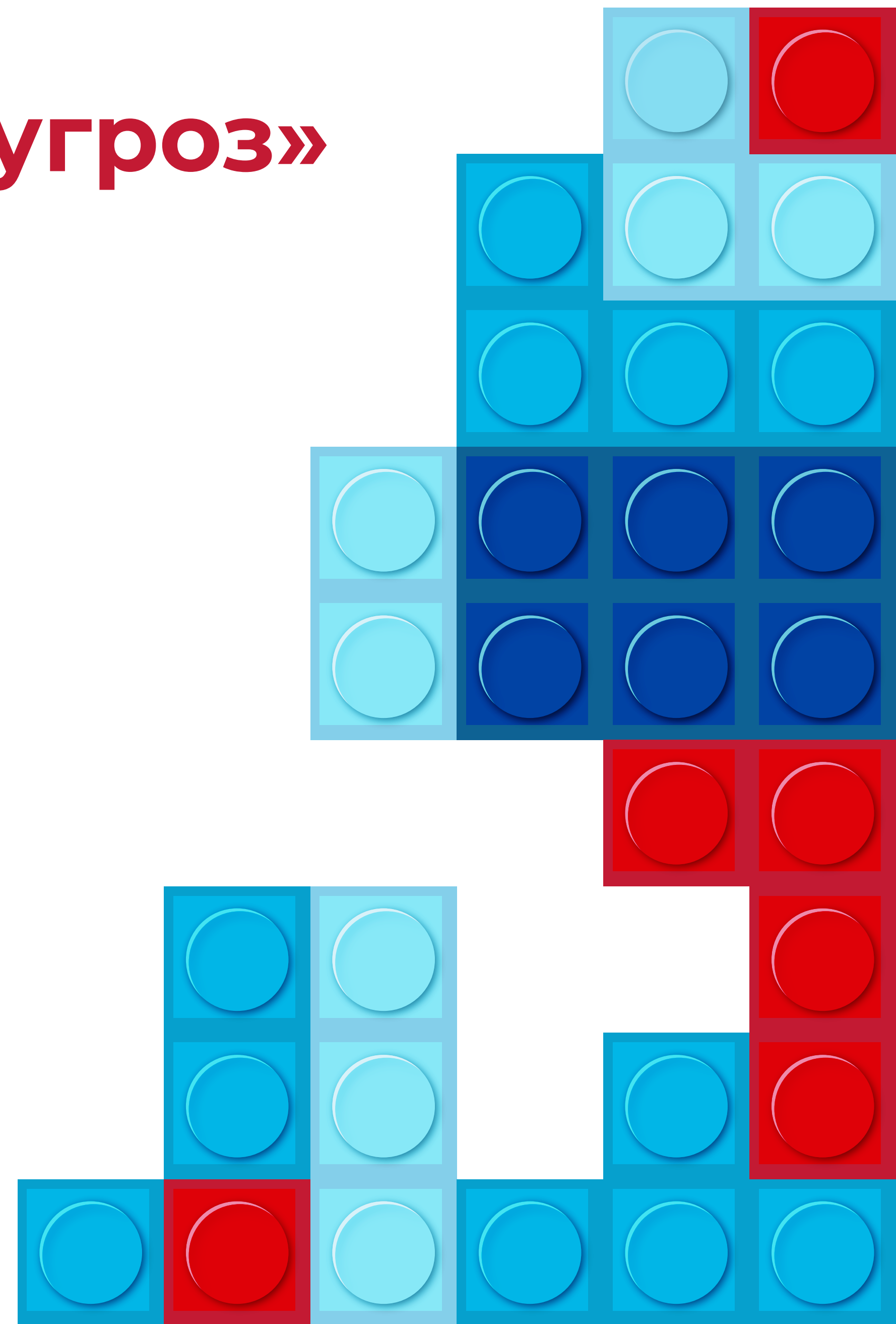
Использует нормативную базу ФСТЭК России и best practices в области ИБ



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*

