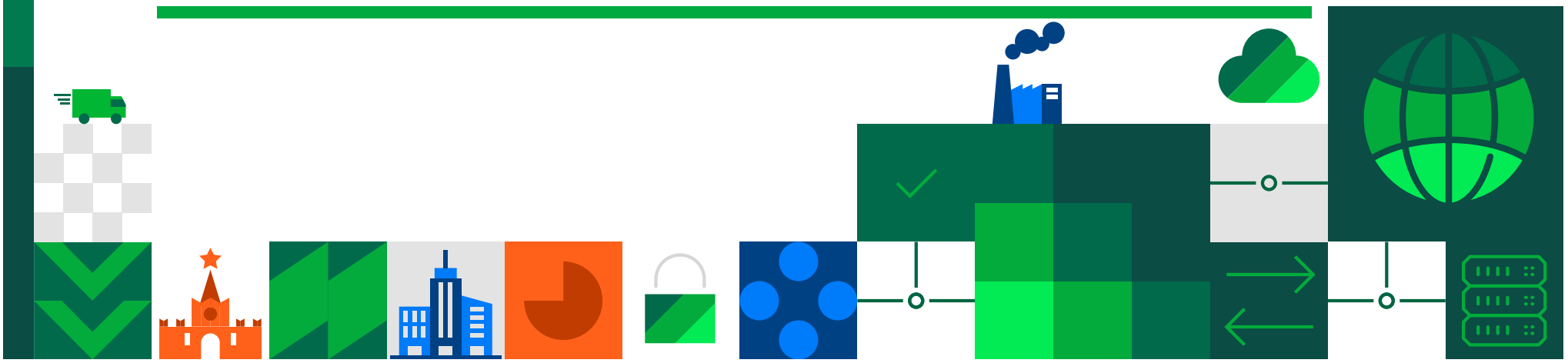
КОД безопасности

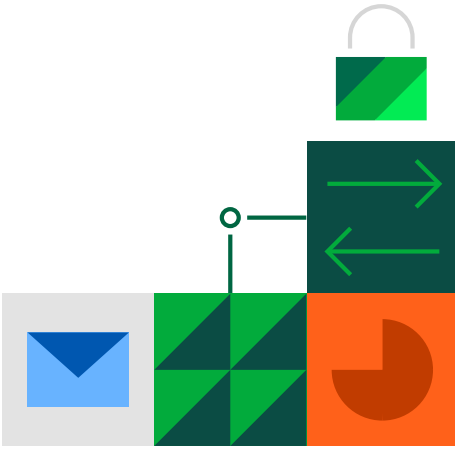
Текущие проблемы в разработке NGFW и варианты их решения



КОД безопасности

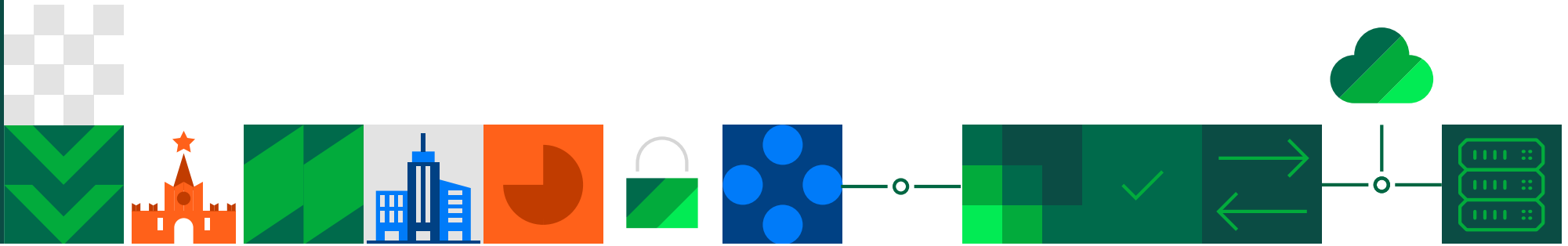
Основные поинты

- Что такое NGFW
- Требования и реалии рыка
- Кадровый дефицит
- Hardware
- Software
- Обеспечение качества
- Резюме



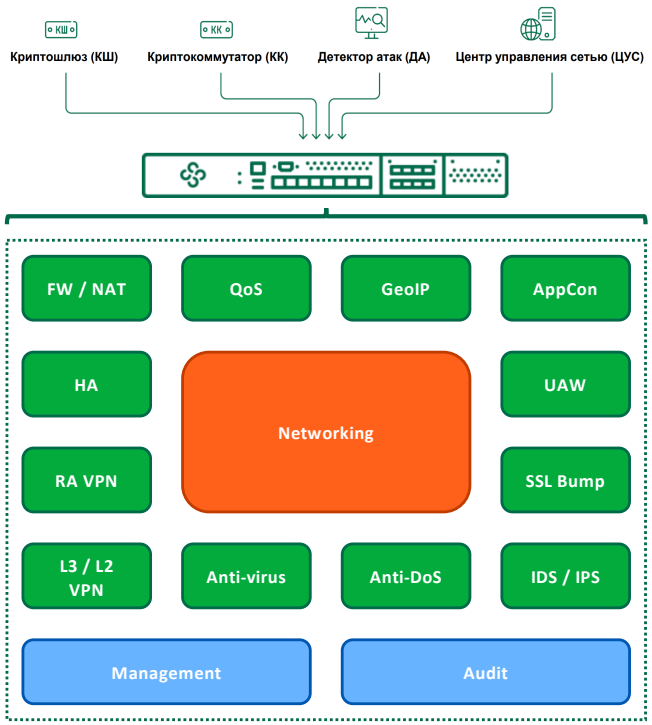
КОД безопасности

Что такое NGFW



КОД безопасности

Что такое NGFW



Сетевое взаимодействие

- Использование различных типов интерфейсов, статическая и динамическая маршрутизация, DHCP сервис с различными опциями (**Networking**)

Контроль доступа

- Пакетная фильтрация и трансляция адресов (**FW / NAT**), приоритизация трафика (**QoS**) фильтрация по географическим объектам (**GeoIP**), контроль протоколов и приложений (**AppCon**), аутентификация пользователей (**UAW**), HTTPS инспекция и URL фильтрация (**SSL Bump**)

Обнаружение угроз

- Сигнатурный анализ на предмет различных атак (**IDS / IPS**), эвристический анализ на предмет Syn, Scan, и Spoofing атак (**Anti-DoS**), потоковый антивирус (**Anti-Virus**)

Криптографическая защита

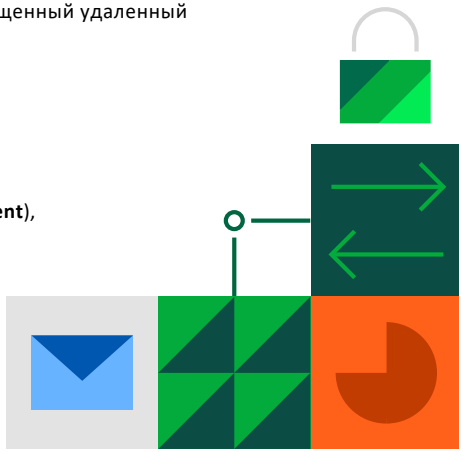
- Защита коммуникаций между офисами (**L3 / L2 VPN**), защищенный удаленный доступ (**RA VPN**)

Обеспечение работы

- Объединение узлов в отказоустойчивый кластер (**HA**)

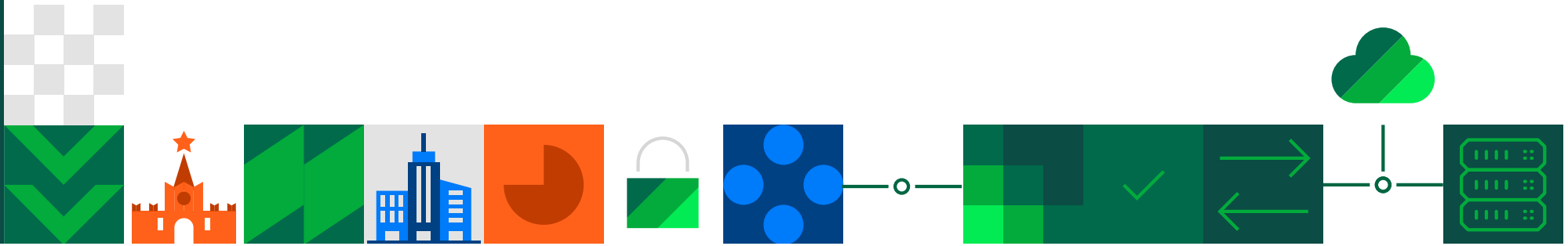
Управление

- Централизованное управление конфигурацией (**Management**), централизованный аудит и мониторинг работы (**Audit**)



КОД безопасности

Требования и реалии рынка



КОД безопасности

Требования и реалии рынка

Уход с рынка крупных зарубежных вендоров

- Часть зарубежных вендоров прекратила работу на отечественном рынке (Fortinet, Cisco, Palo Alto Networks и др.)
- Часть осталась, но испытывает перебои в цепочках поставок и санкционное давление

Дефицит квалифицированных специалистов

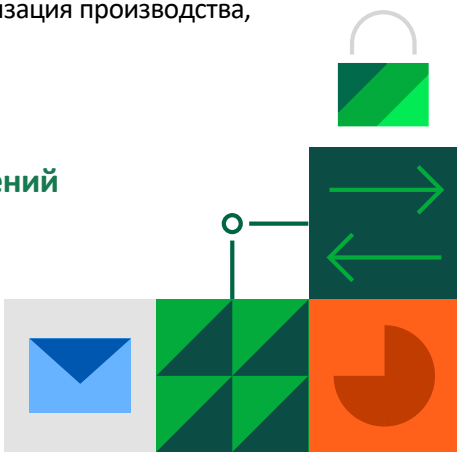
- Рост объема решаемых задач и потребность в дополнительном ресурсном обеспечении
- Отток специалистов с рынка на фоне последних событий

Усиление требований регулятора

- Усиление требований для отечественных вендоров (локализация производства, функциональные требования, SDL)
- Усиление требований по защите ГИС и объектов КИИ
- Требования по импортозамещению зарубежных решений

Изменение векторов развития и специализации решений

- Enterprise → Telecomm
- Informational Technologies → Operational Technologies

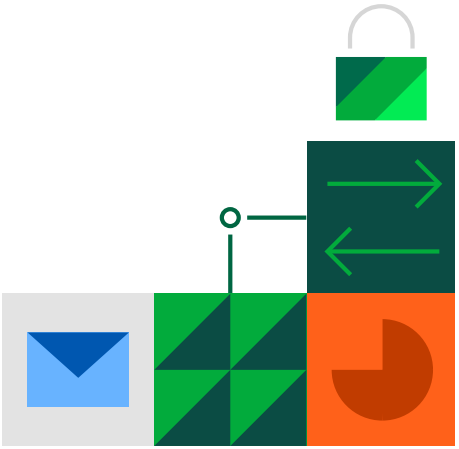


КОД безопасности

Требования и реалии рынка

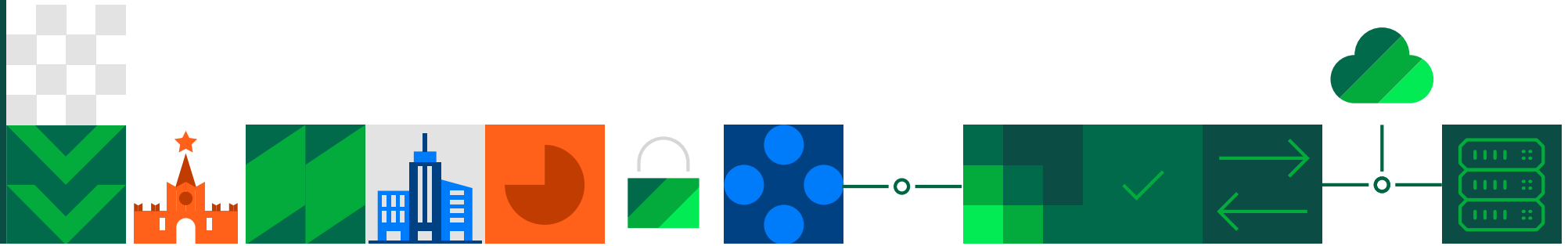
Решения

- ✓ Баланс между потребностями заказчиков, глобальными тенденциями и реальными возможностями вендоров
- ✓ Внутреннее стимулирование разработки для ускорения технологического развития
- ✓ Приоритизация и специализация направлений разработки для конкретных потребностей рынка, направление безопасности АСУ ТП
- ✓ Совместная и продуманная образовательная работа для подготовки специалистов «под ключ» с привлечением образовательных учреждений



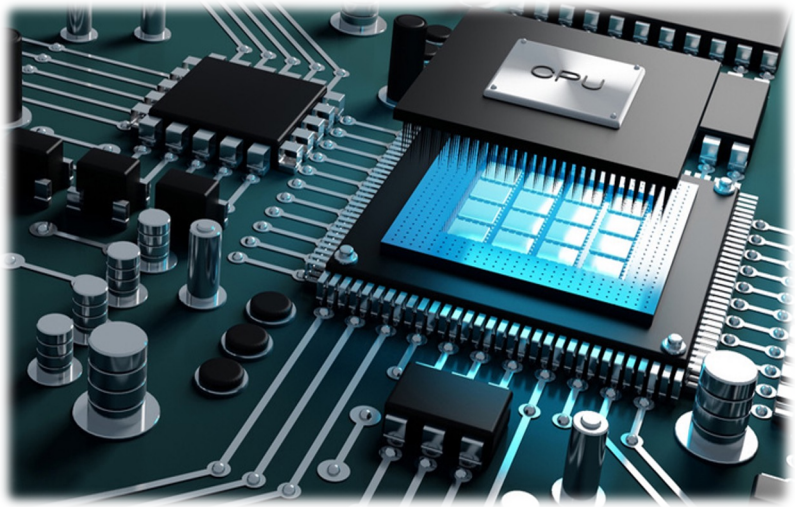
КОД безопасности

Hardware

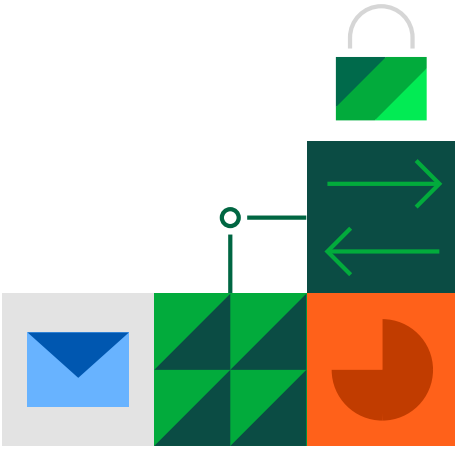


КОД безопасности

Hardware



- Перебои в цепочках поставок специализированных платформ
- Высокие риски при ставке на параллельный импорт
- Отсутствие подходящей отечественной элементной базы

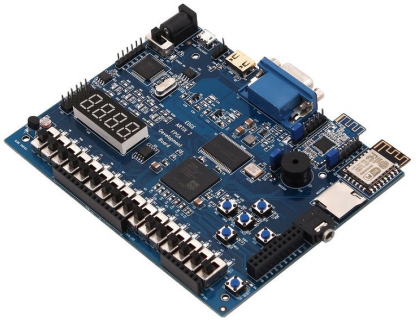


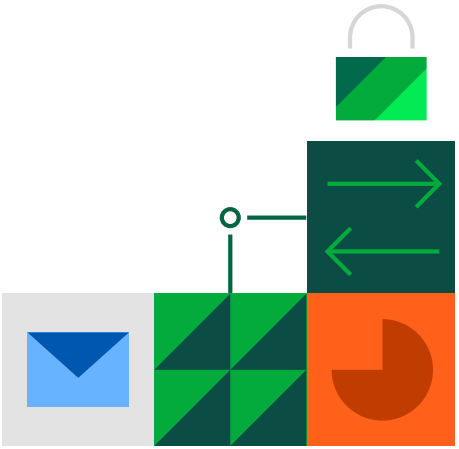
КОД безопасности

Hardware

Решения

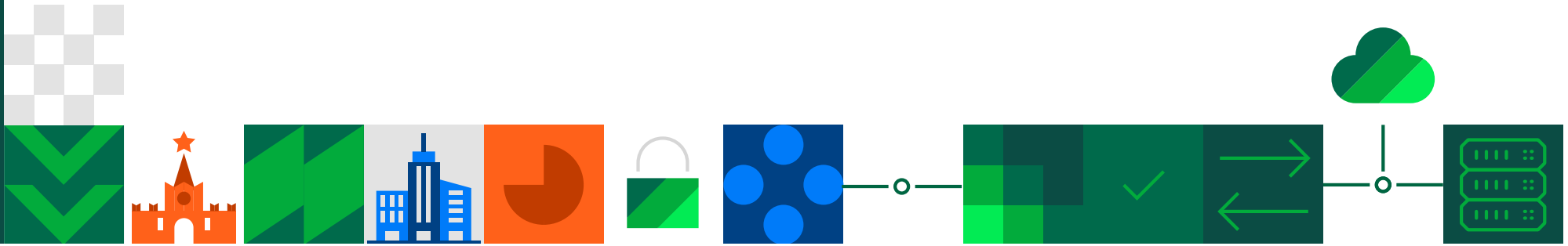
- ✓ Переводим эксплуатируемые решения на доступную элементную базу (Соболь на Artix FPGA)
- ✓ Для отдельных задач прорабатываем варианты решений без АМДЗ по направлению сертификации ФСБ
- ✓ Продолжаем развивать собственные аппаратные платформ (серия «R» доступна во всех сегментах – SOHO, SMB, ENTERPRISE)
- ✓ Развиваем направление аппаратных криптоускорителей (FPGA)





КОД безопасности

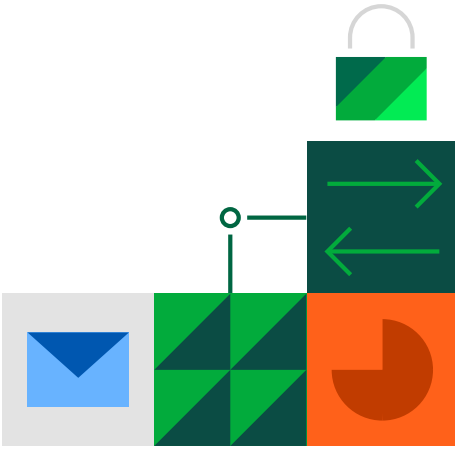
Software



КОД безопасности

Software

- Ограниченные возможности по интеграции open source компонентов
- Наличие уязвимостей и особенности лицензирования open source компонентов
- Требования регулятора в контексте SDL
- Развитие облачных инфраструктур

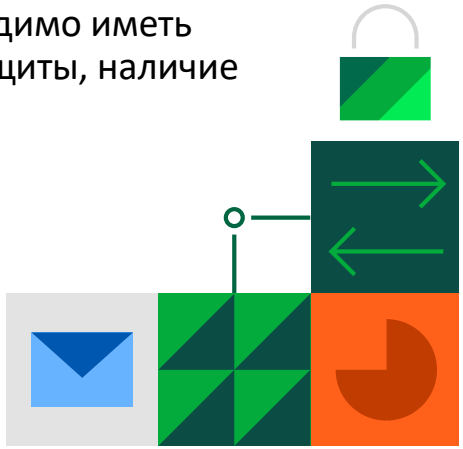


КОД безопасности

Software

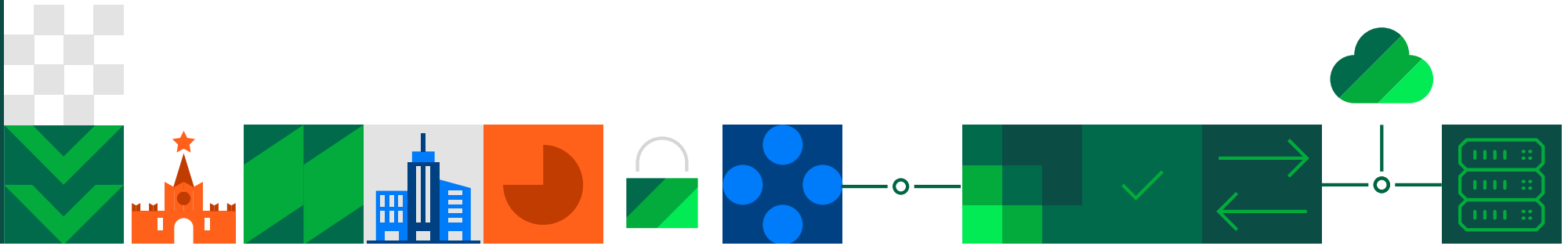
Решения

- ✓ Принимаем активное участие в работе над доверенным ядром Linux совместно с ИСП РАН вместе с коллегами по рынку (ИнфоТеКС, РусБИТех-Астра, Яндекс.Облако и др.)
- ✓ Усиливаем команду SDL, дополнительно выделяя ресурсы специально под каждый из продуктов и ставя на промышленные «рельсы»
- ✓ Прорабатываем вопрос с виртуальным исполнением в контексте:
  - снижения рисков при поставках специализированных платформ
  - адаптации архитектуры решения для интеграции в облачные инфраструктуры и высоконагруженные системы
- ✓ В контексте специализации направлений разработки жизненно необходимо иметь устойчивый сегмент рынка доверенных баз правил для механизмов защиты, наличие которых в решении требует регулятор



КОД безопасности

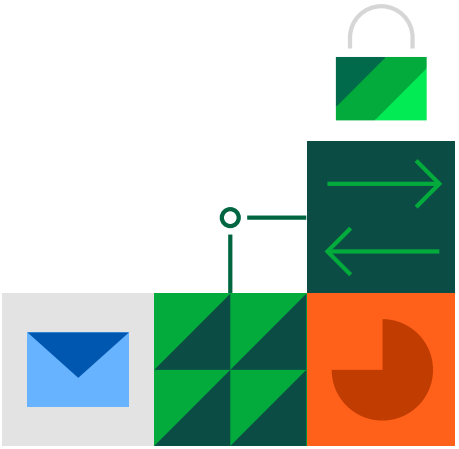
Обеспечение качества



КОД безопасности

Обеспечение качества

- Отсутствие методик тестирования производительности
- Отсутствие инструментов для тестирования производительности

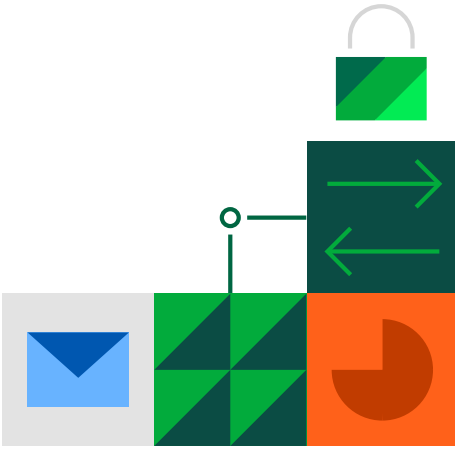


КОД безопасности

Обеспечение качества

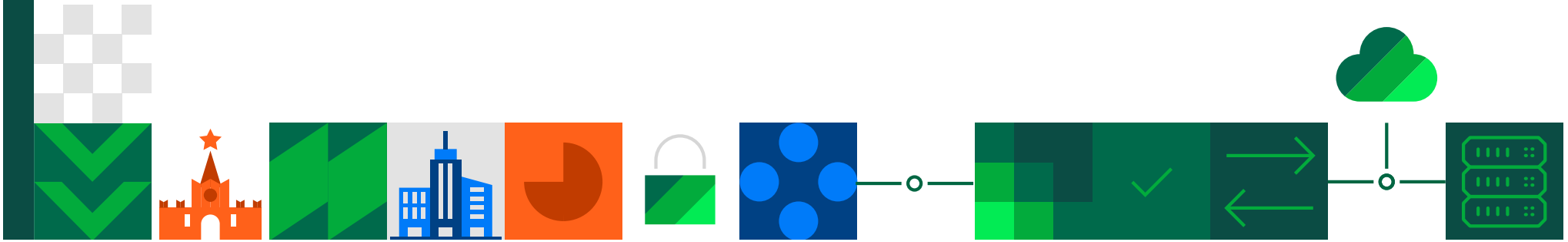
Решения

- ✓ Принимаем активное участие в работе по создание инфраструктуры для тестовой лаборатории для тестирования производительности СКЗИ (VPN) сетевого уровня совместно с АНО НТЦ ЦК
- ✓ В связи с уходом лидера области – IXIA – активно внедряем использование инструмента TRex для тестирования производительности собственными силами
- ✓ Полученные в результате наработки можно будет использовать для тестирования производительности NGFW



КОД безопасности

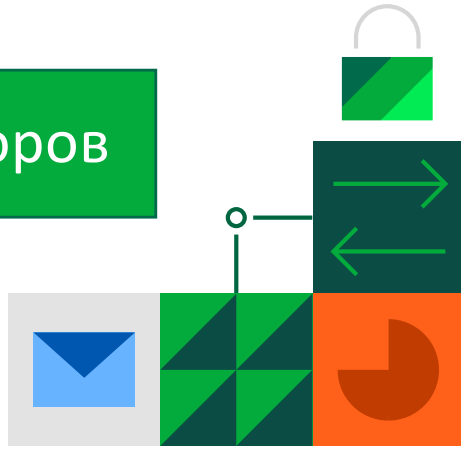
Резюме



КОД безопасности

Резюме

- Время вызовов – время роста
- Мудрое руководство регулятора
- Сотрудничество со стороны других вендоров



КОД безопасности

Спасибо за внимание!

info@securitycode.ru
www.securitycode.ru