K2 кибер безопасность

WAF – необходимое звено в защите веб-приложений или навязанная коробка. Взгляд интегратора.

О спикере

Аскар Добряков

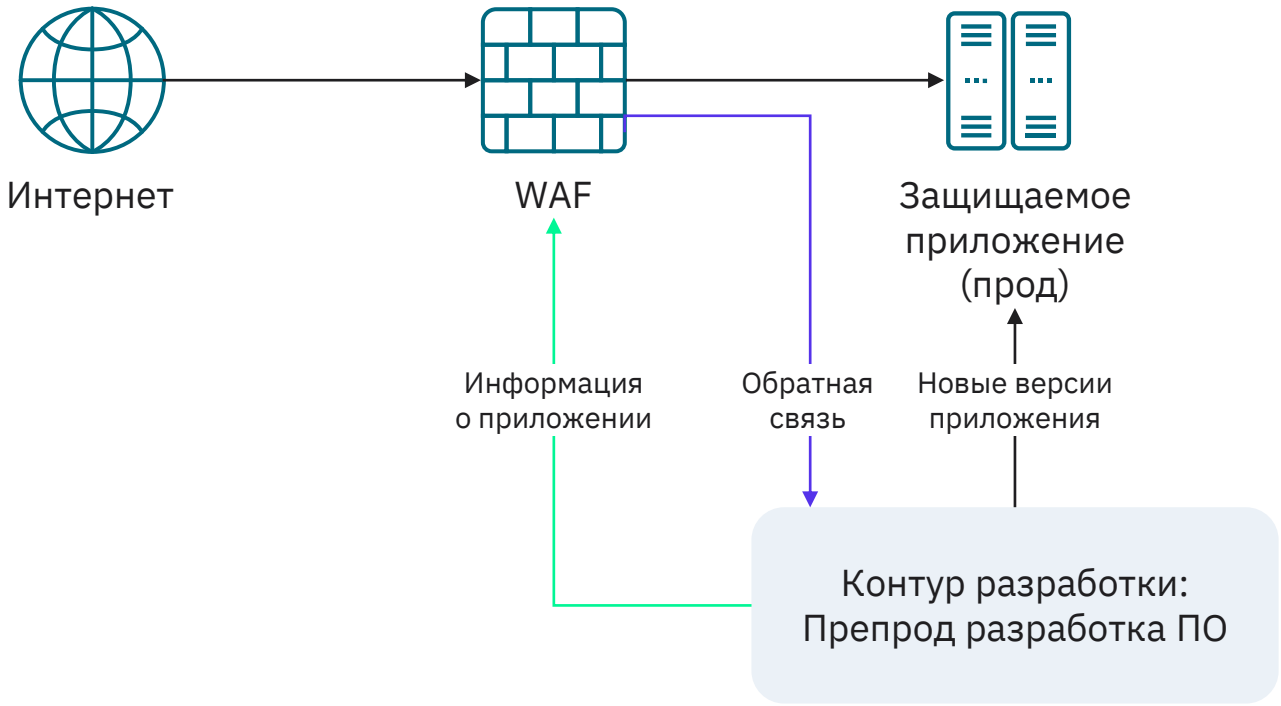
Ведущий эксперт направления
защиты бизнес-приложений
К2 Кибербезопасность

>15 в ИБ

>3 лет в AppSec

К2 кибер безопасность

Web Application Firewall



Железо или функции

Публикация | Верификация | Обнаружение атак | Визибилити | Доверие

K2 кибер безопасность

Публикация приложений

01

Реверс-прокси

02

Балансировка

Round-robin, least connection, response time, persistence

03

Отказоустойчивость

04

SSL

Чтобы SSLlabs выдал A+, а клиенты все еще могли подключаться

05

Управление заголовками

HSTS, CORS

K2 кибер безопасность

Верификация входных данных

01

Проверка данных, вводимых пользователем

02

URL, Endpoint

03

Контроль форм, JSON, XML, соответствие схемам и протоколам

04

Контроль соответствия HTTP

05

Безопасность API

Позитивная модель работы WAF

K2 кибер безопасность

Обнаружение атак

01

Сигнатуры атак

?id='or+1=1--a-
<script>prompt(1)</script>
/../../../etc/passwd

02

Корреляции, поведенческий анализ

100 запросов с одного IP
на форму логина за 1 минуту...
возможно, брутфорс?

03

Обнаружение ботов

CAPTCHA, reCAPTCHA,
Browser Challenge...
User-Agent:

04

Защита от L7 DoS

частота обращений
«тяжелые» страницы
Атаки из п. 1-3

05

Виртуальные патчи

K2 кибер безопасность

Визибилити и обзервабилити

01

Логирование подозрительных действий

02

Отправка сообщений в SIEM

03

Создание схемы веб-приложений и API

04

Сканирование и перепроверка атак

05

Анализ ответов приложения, поиск уязвимостей и потенциально успешных атак

K2 кибер безопасность

Доверие

01

Сертификат
ФСТЭК России

02

Репутация
вендора

В информационных системах применяются средства защиты информации, сертифицированные на соответствие обязательным требованиям по безопасности информации, установленным ФСТЭК России, или на соответствие требованиям, указанным в технических условиях (заданиях по безопасности). При этом функции безопасности таких средств должны обеспечивать выполнение настоящих Требований.

Приказ ФСТЭК №17

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 57580.1— 2017

Безопасность финансовых (банковских) операций

ЗАЩИТА ИНФОРМАЦИИ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

Базовый состав организационных и технических мер

РЗИ.11	Применение сертифицированных по требованиям безопасности информации средств защиты информации не ниже 4 класса**
РЗИ.12	Применение сертифицированных по требованиям безопасности информации средств защиты информации не ниже 5 класса**
РЗИ.13	Применение сертифицированных по требованиям безопасности информации средств защиты информации не ниже 6 класса**
РЗИ.14	Применение СКЗИ, имеющих класс не ниже КС2**
РЗИ.15	Обучение, практическая подготовка (переподготовка) работников финан-

Вариант 1

Зона ответственности ИБ

WAF

- Публикация приложений
- Верификация входных данных
- Обнаружение атак
- Визибилити
- Доверие

Максимальный набор функций

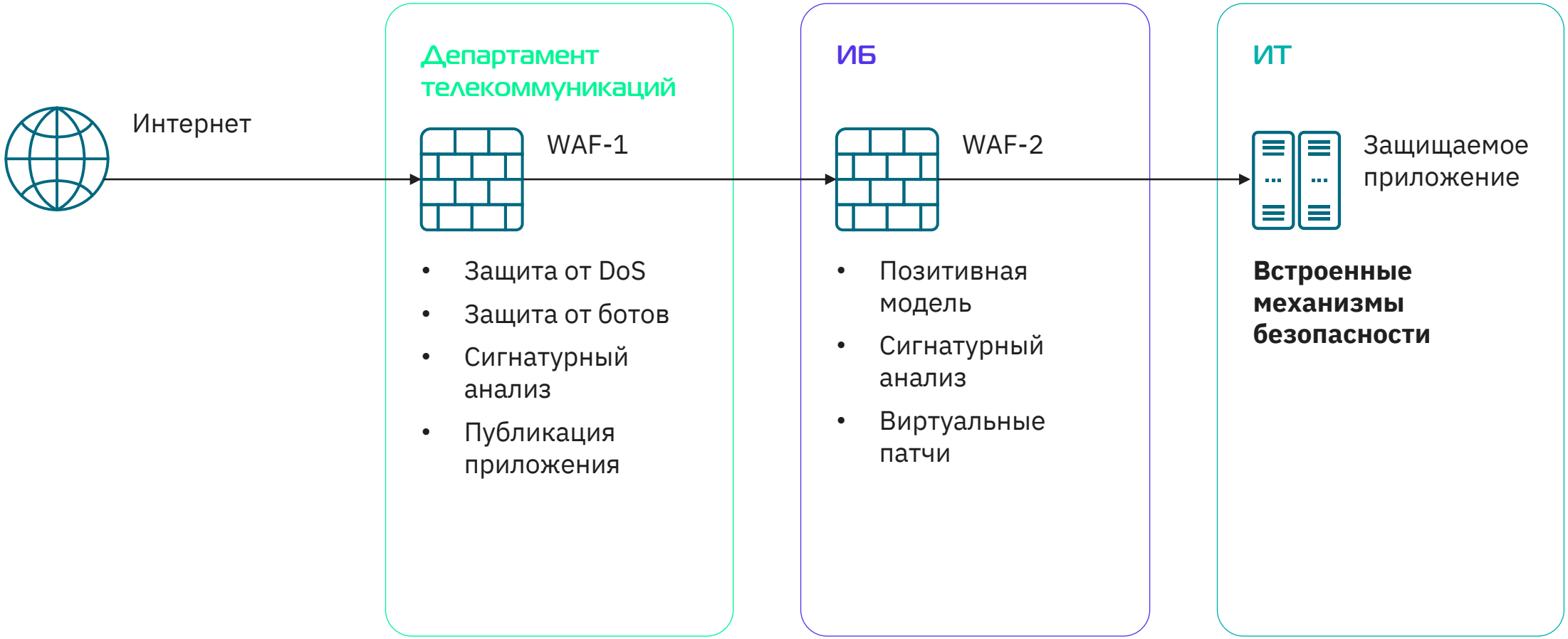
Зона ответственности ИТ

Защищаемое приложение (прод)

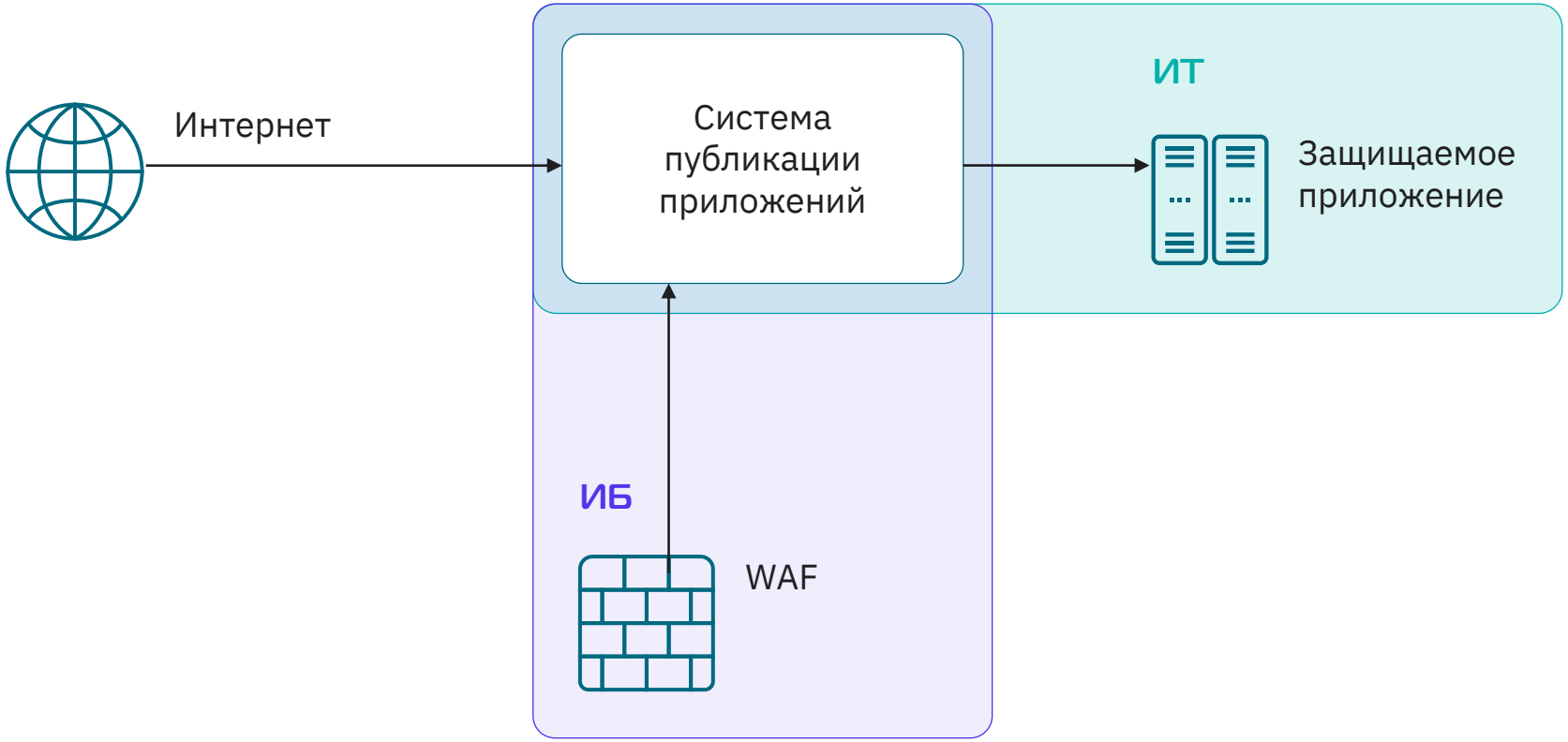
Встроенные механизмы безопасности

- Патчи
- Идентификация пользователей
- Управление доступом
- Регистрация действий пользователей в системе
- Отказоустойчивость

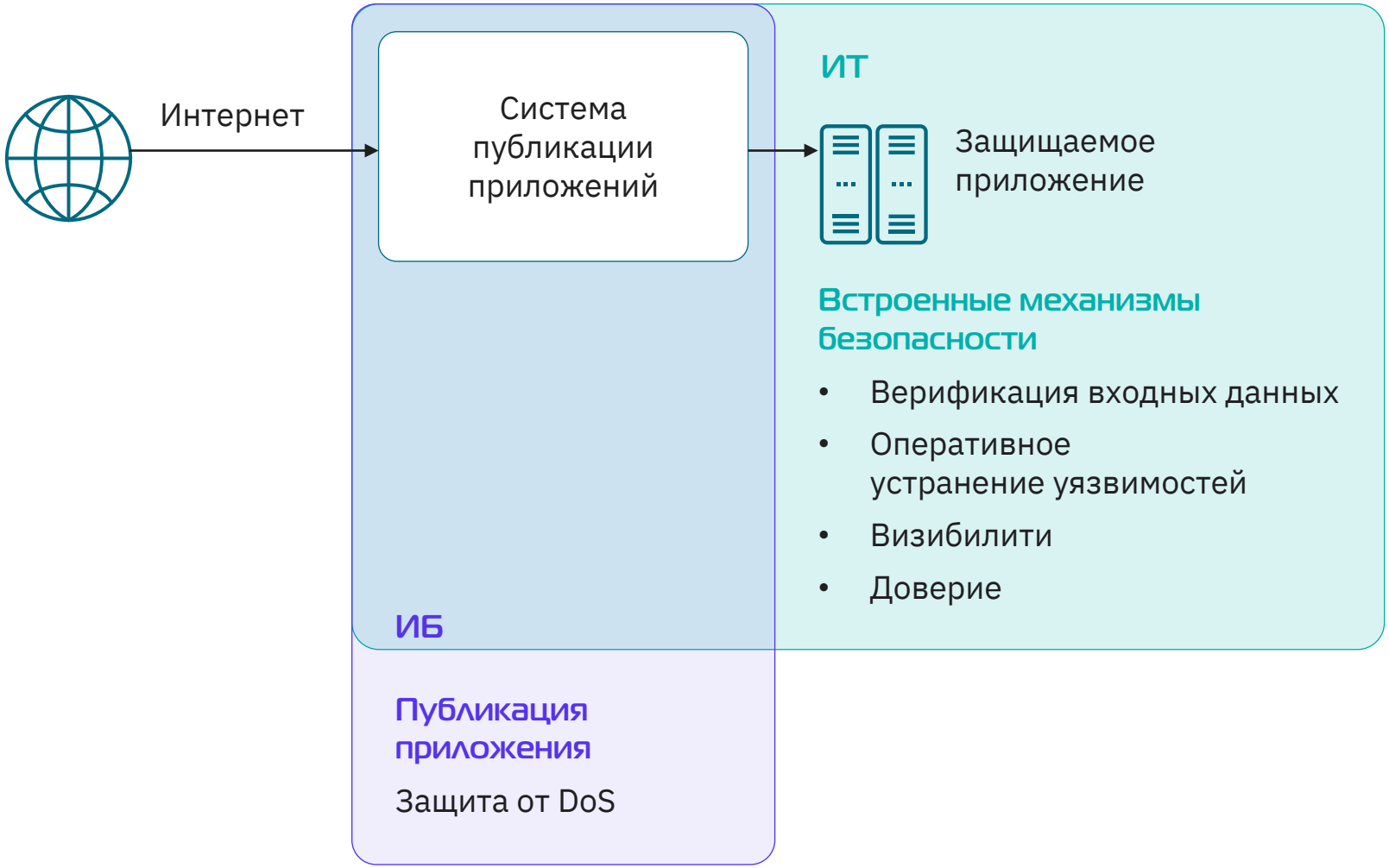
Вариант 2 – лучше WAF может быть только два WAF



Вариант 3


Интернет
Система публикации приложений
ИТ
Защищаемое приложение
ИБ
WAF

Вариант 4


Интернет
Система публикации приложений
ИТ
Защищаемое приложение
Встроенные механизмы безопасности
• Верификация входных данных
• Оперативное устранение уязвимостей
• Визибилити
• Доверие
ИБ
Публикация приложения
Защита от DoS

Выводы

Есть функции ИБ, которые надо выполнить или не надо, если риски принимаются

Есть различные варианты, куда технически можно приземлить эти функции

Выбор осуществляется исходя из технической возможности, распределения зон ответственности и экономической целесообразности

WAF – это только инструмент, который может реализовать часть данных функций

Спасибо за внимание

Карьера
в К2 Кибербезопасность

Наш канал в телеграме

К2 кибер безопасность