



# BI.ZONE

## Кибербезопасность



# Как обеспечить кибербезопасность компании?



Границы IT-инфраструктур компаний размываются: появляются новые приложения, сайты и облачные сервисы, сотрудники переходят на удаленную работу. В то же время киберпреступники наращивают потенциал, совершенствуя инструменты атак и методы их доставки

Без обеспечения киберзащиты компании могут столкнуться с трудностями:

- Утечка конфиденциальной информации, которая может повлечь репутационные и финансовые риски
- Угроза остановки бизнес-процессов из-за возможных кибератак
- Необходимость соответствовать законодательству РФ, стандартам безопасности и своевременно отслеживать изменения требований

Избежать сложностей поможет надежный эксперт, который:

- Выстроит эффективную стратегию киберзащиты исходя из потребностей компании
- Обнаружит инциденты кибербезопасности и предотвратит действия злоумышленников
- Поможет повысить защищенность ИТ-инфраструктуры в соответствии с законодательством РФ и стандартам безопасности

## Надежная киберзащита вашего бизнеса



Кибербезопасность — комплекс решений, помогающий компаниям систематизировать подход к защищенности и обеспечить безопасную цифровизацию

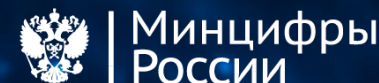
Задачи, которые решает сервис:

- Сократить расходы на обеспечение цифровой безопасности компании
- Оптимизировать технологические процессы
- Предупреждать мошенничество
- Соответствовать требованиям регуляторов

BI.ZONE – компания экосистемы Сбера в области стратегического управления цифровыми рисками

270+ защищенных клиентов  
850+ реализованных проектов  
600+ экспертов в области кибербезопасности

Наши решения включены в реестр отечественного ПО



# Сокращение расходов на обеспечение цифровой безопасности компании

## Подключение управляемых сервисов

- Не нужно самим вести постоянный мониторинг систем безопасности и тратить ценные ресурсы
- Высвобождаются время и средства для приоритетных задач

## Аутсорсинг любых процессов безопасности

- Не нужно искать новых сотрудников в штат
- Не нужно расширять компетенции специалистов



# Оптимизация технологических процессов



## Модернизация процессов безопасной разработки

- Сокращение стоимости уязвимости
- Отлаженные процессы между отделами разработки и кибербезопасности, где каждый занимается своим делом
- Управление жизненным циклом безопасной разработки

## Анализ защищенности приложений

- Выявление уязвимостей до их эксплуатации злоумышленником
- Понимание устойчивости приложений



# Предупреждение мошенничества

## Повышение киберграмотности персонала

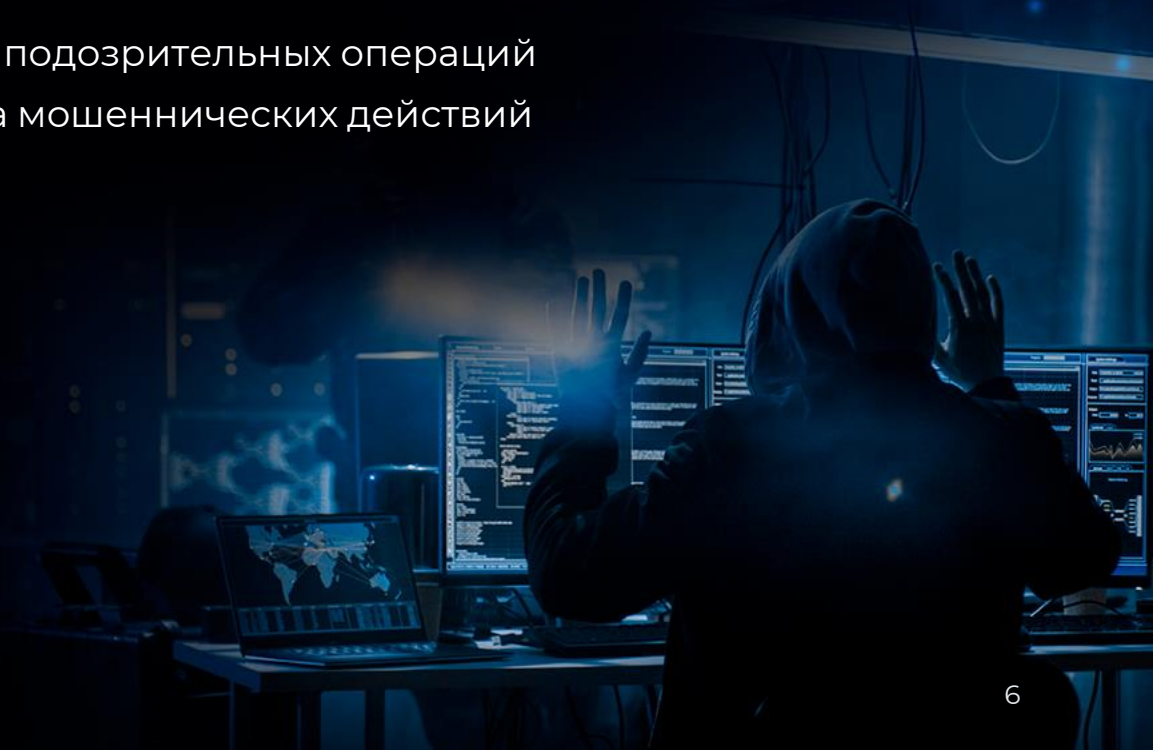
- Тренировка устойчивости сотрудников к фишинговым атакам
- Плановые учебные атаки

## Противодействие мошенничеству в банковских операциях

- Выявление подозрительных операций
- Блокировка мошеннических действий

## Защита бренда

- Выявление информационных атак
- Блокировка мошеннических ресурсов
- Мониторинг утечек данных



Решение задач

Безопасная цифровизация

# Соответствие требованиям регуляторов



Разработка комплекта документации в соответствии с требованиями 152-ФЗ, 187-ФЗ, GDPR, 382-П, 684-П, PCI DSS и др.

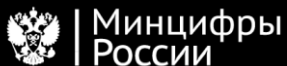
Минимизация расходов на систему защиты

Независимый аудит на соответствие требованиям

Помощь в изменениях, связанных с выполнением этих требований

Сопровождение при проверке контролирующих органов

Наши компетенции подтверждают



АССОЦИАЦИЯ  
БАНКОВ  
РОССИИ



КООРДИНАЦИОННЫЙ ЦЕНТР  
ДОМЕНОВ .RU/.RF

GENEVA  
DIALOGUE  
ON RESPONSIBLE  
BEHAVIOUR  
IN CYBERSPACE



### Банк

#### Исходные данные:

- Приложения банка обновляются в ходе релизов, которые определяются с помощью коммерческого сканера на основе статистического анализа исходного кода (SAST) и контроля зависимостей (SCA)

#### Проблемы:

- Релизы отклоняются из-за ложных уязвимостей, которые не выявляет ручная проверка
- Длинная очередь новых релизов ввиду большого числа сканируемых приложений
- Продуктовые команды не соблюдают требования безопасности банка, чтобы сократить срок обновления приложений

#### Решение:

- Выявлены и устранены проблемные места в логике работы сканера
- Подключение к BI.ZONE SSDLC помогло сократить затраты на поддержку SAST
- Определены запросы сканера, которые можно отключить, и сократить очередь релизов
- Составлены рекомендации для разработчиков, чтобы в короткие сроки исправлять ошибки при ложном срабатывании сканера

#### Результаты:

Для 5 крупных приложений банка увеличена эффективность работы сканера

В 10 раз планируется сокращение объема ложных срабатываний сканера на основе рекомендаций BI.ZONE



## Сеть ресторанов быстрого питания

### Исходные данные:

- Требовалось проверить безопасность информационных систем для обслуживания клиентов
  - ✓ мобильного приложения на базе Android и iOS (2,7 млн пользователей)
  - ✓ приложения и ПО для киосков самообслуживания (330 тыс. заказов в сутки)

### Решение:

- Проведен анализ защищенности по нескольким сценариям действий потенциального злоумышленника
- Выявлены уязвимости в обеспечении безопасности информационных систем клиента
- Разработаны рекомендации по устранению пробелов в системе безопасности клиента и повышению общего уровня защищенности

### Результаты:

За 1 месяц предоставлена поддержка сети ресторанов

24/7 обеспечен контроль безопасности компании

1 млн клиентов, данные которых защищены

# Преимущества



Эксперты BI.ZONE сертифицированы международными агентствами CISSP\*, CEN\*\* и другими



Лицензии ФСТЭК и ФСБ



Реализуем проекты в **25** странах мира



Гарантированный уровень **SLA 99,9%**



Организуем международные мероприятия по повышению уровня знаний в области кибербезопасности



Продукты компании включены в реестр отечественного ПО

\*Certified Information Systems Security Professional

\*\*Certified Ethical Hacker

# Кибербезопасность



## **Услуги оказывает:**

ООО «БИЗон»

105066, г. Москва, ул. Ольховская, д. 4, корп. 2, офис 515

ОГРН: 1167746317210, ИНН: 9701036178

Настоящий материал носит исключительно информационный характер, не является предложением по покупке продукта/услуги и не может рассматриваться как рекомендация к подобного рода действиям. Компания не утверждает, что все приведенные сведения являются единственно верными и не несет ответственности за использование информации, содержащейся в материале, а также за возможные убытки. Данные об использовании продукта/услуги в прошлом основаны на информации, которой компания располагала на дату выхода материала.