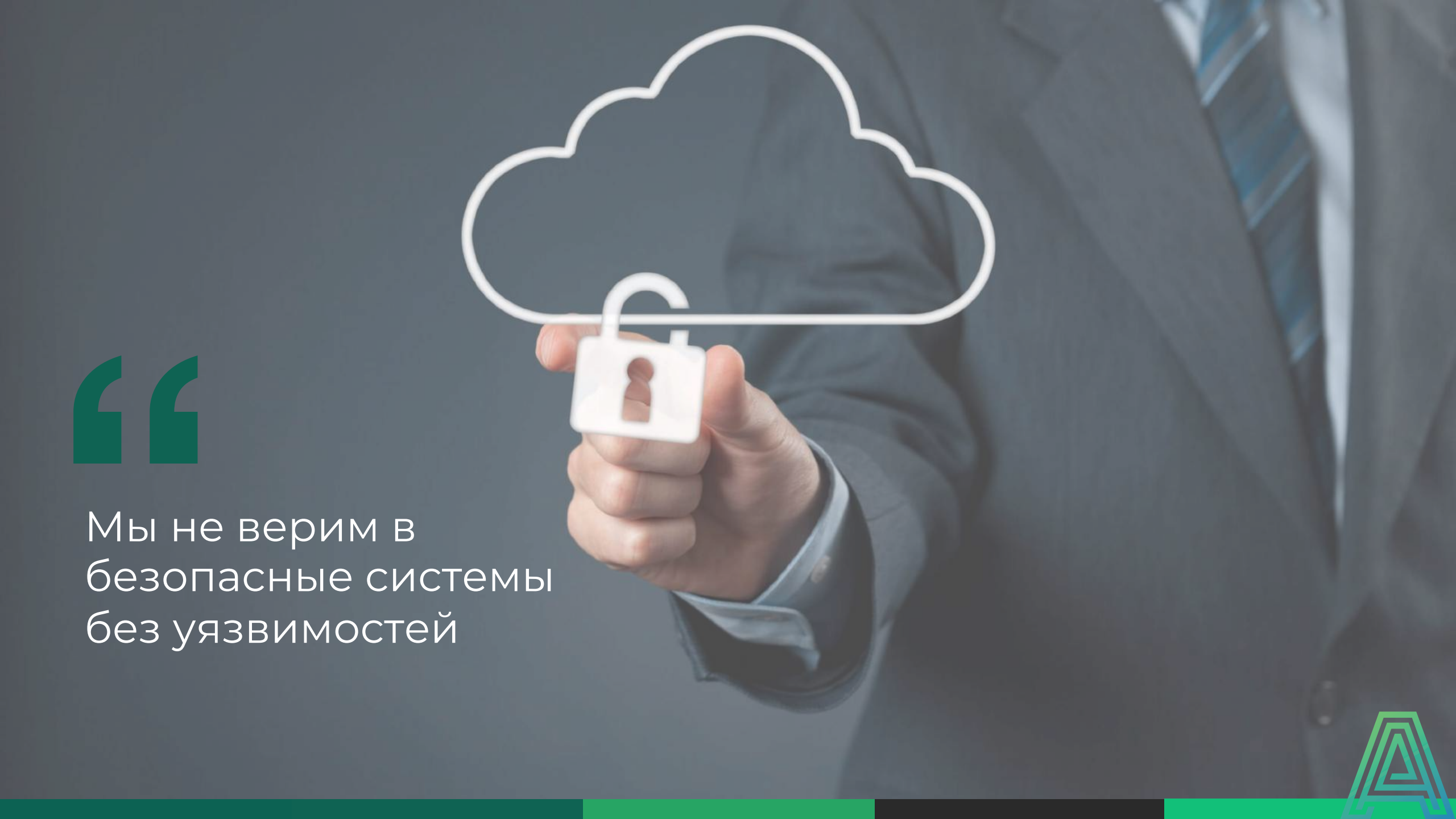

Antihacking
Независимая оценка информационной безопасности

Антихакинг выполняет работы по оценке защищенности, позволяет разработать адекватную и всеобъемлющую программу мероприятий по повышению уровня защищенности системы, с целью снижения операционных, финансовых и репутационных рисков до минимума.

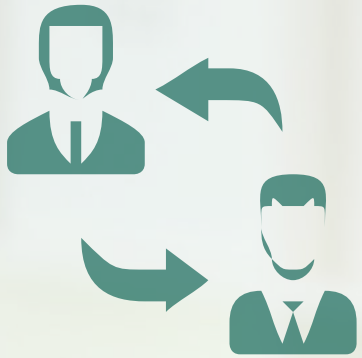
globalit
информационная безопасность



Мы не верим в
безопасные системы
без уязвимостей

— Наша МИССИЯ

Помочь компаниям понять свои риски, иметь возможность получить независимую оценку безопасности и принять меры для защиты своих интересов в информационном пространстве.



Для кого мы работаем?

Информационная безопасность неотложная часть любого бизнеса. Каждая компания, имеющая доступ к сети подвержена угрозам извне. В то же время разные компании по разному относятся к решению вопросов ИБ. Мы выделили 5 сегментов бизнеса чаще других подверженных атакам. Какой опасности подвержен Ваш бизнес?

Финансовый сегмент

Банки и Платежные Системы

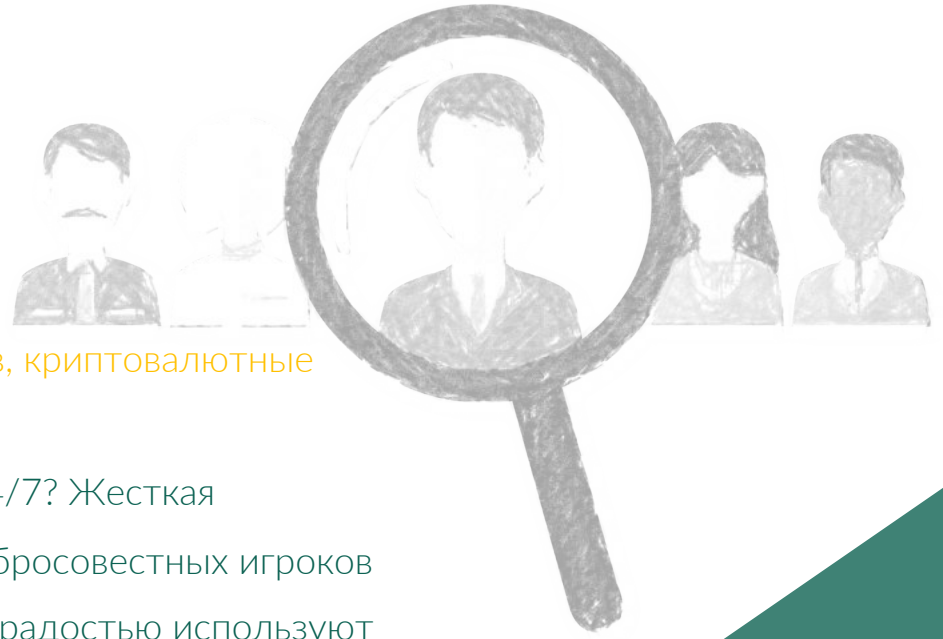
Финансовые потоки – главная цель злоумышленников. Очень часто стандартные методы защиты не являются достаточными чтобы уберечь свои системы от внешнего проникновения. Высокая финансовая отдача все сильней завлекают нарушителей. Хакеры готовы тратить многие часы своего труда чтобы найти хоть самую малую уязвимость.

Реальный сегмент

Производственные компании

Компании с большими оборотами и множеством сотрудников чаще всех подвержены внешним и внутренним атакам. Хакеры нацелены на получение доступа во внутренний периметр сети, на атаки на корпоративные сети, на атаки с использованием социальной инженерии и многое другое. Независимые и постоянные оценки всех уровней системы приобретает неотложный характер.

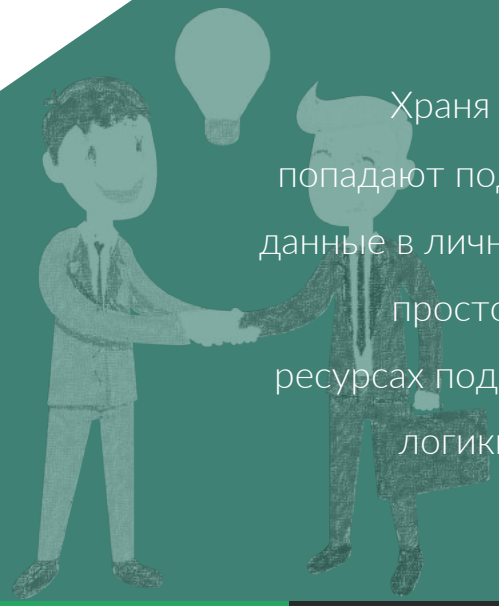
B2C сегмент



Ритейл, онлайн магазины, продажа билетов, криптовалютные проекты, букмекерские конторы, лотереи

У вас есть продающий сайт работающий 24/7? Жесткая конкурентная среда часто вынуждает недобросовестных игроков выйти за рамки закона. Ваши конкуренты с радостью используют любую уязвимость вашего сервиса с целью парализовать ваш бизнес. Такие атаки легко предотвратить, если задуматься об этом заранее.

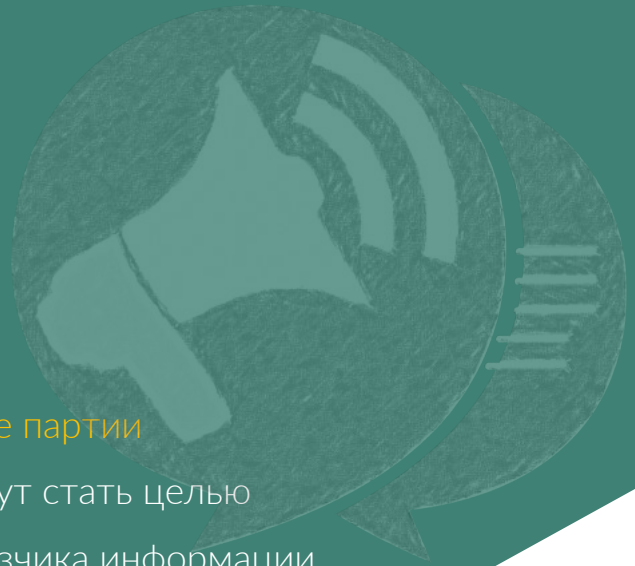
B2B сегмент



Хостинги, разработчики, веб-студии и агентства, сервисы лояльности

Храня большие массивы данных этот сектор часто попадают под прицел хакеров, чтобы использовать ваши данные в личных целях, очернить вашу репутацию или же просто продать информацию на черном рынке. На ресурсах подобных организаций часто находятся ошибки логики веб-приложений, представляющие легкую мишень для преступников.

Медиа сегмент

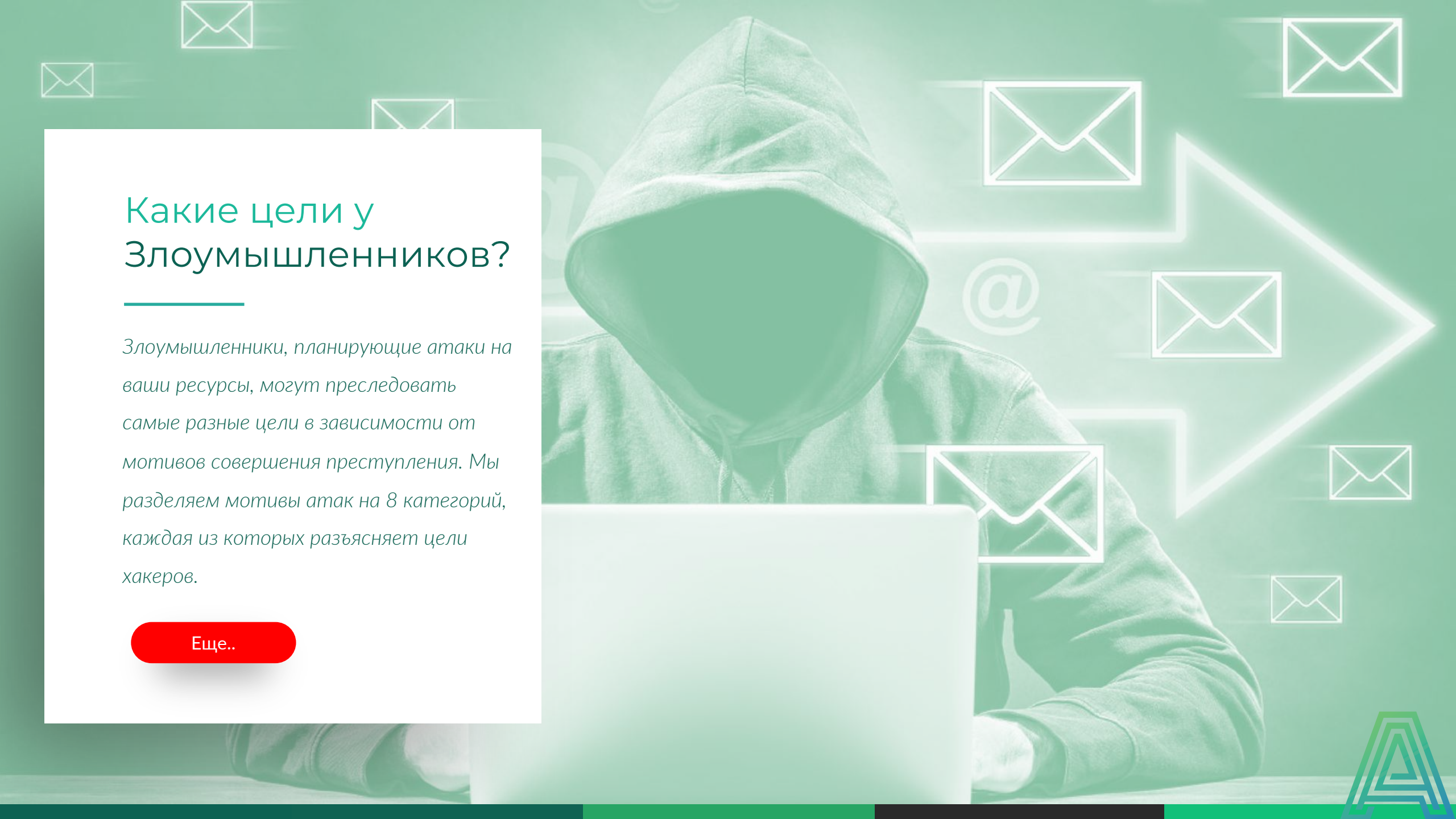


Информационные порталы, СМИ, Политические партии

Ресурсы с большими объемами посещений могут стать целью хакеров для размещения необходимой для заказчика информации, с целью использования пост-эффекта или порчи репутации.

Другие

Антихакинг занимается консультированием компаний и не вошедших в 5 сегментов бизнеса. Мы проводили аудиты для самых разных отраслей, поэтому отлично понимаем что нужно для каждого бизнеса, каким потенциальным угрозам он подвержен и как максимально эффективно их выявить и устранить.



Какие цели у Злоумышленников?

Злоумышленники, планирующие атаки на ваши ресурсы, могут преследовать самые разные цели в зависимости от мотивов совершения преступления. Мы разделяем мотивы атак на 8 категорий, каждая из которых разъясняет цели хакеров.

Еще..

Кража коммерческой тайны, персональных данных и компрометирующей информации

У любого крупного предприятия есть коммерческая тайна, представляющая собой ценную информацию. Злоумышленники могут запросто продать полученную информацию на черном рынке вашим конкурентам и недоброжелателям.

1

Остановка деятельности ресурса посредством DDoS атак

Имея доступ к многочисленным зомби-компьютерам хакер может закидать ваш ресурс огромным числом запросов, превышающим допустимый лимит по вашему каналу. Если это произойдет, то ваш ресурс перестанет отвечать на поступающие запросы. Это полностью прекратит деятельность ресурса и бизнес процесс встанет.

2

3

Вывод денежных средств с прямыми финансовыми мотивами

Классическая схема получения доступа и слива огромных финансовых активов на несуществующие счета, за границу, в офшоры и тд.

4

Использование уязвимостей протоколов для подмена финансовых данных

Преступник может подменять любого рода данные, например значения валют и вместо 100 тыс. рублей, компания переведет на сомнительные счета 100 тыс. долларов сама об этом не заподозрив.

Использование заполученных привилегированных аккаунтов

Этим способом злоумышленник может без вашего ведома проводить операции на протяжении времени. Возможно когда вы узнаете об этом будет уже поздно.

Подмена информации с использованием необходимых информационных сливов, вбросов для получения необходимого эффекта

Получив доступ к ресурсам хакер может, например, сделать публикацию от вашего имени, имеющую критический характер, что приведет к дезинформации и дестабилизации бизнеса. В это же время кто-то по другую сторону экрана будет шортить ваши акции.

5 6 7 8

Заражение ресурсов для использования вычислительных мощностей для майнинга

Вы можете даже не подозревать что ваш офис превратился в крипто-ферму (если только температура не слишком высокая).

Заражение вирусом с целью получения компрометирующей информации

Многие современные зловреды (troyan) могут проникать в корень системы и получать доступ к файлам с конфиденциальной информацией, которую впоследствии злоумышленники используют для шантажа и вымогательства денежных средств.

Наши Задачи

Обнаружить

Выявить недостатки в применяемых Заказчиком мерах информационной безопасности и оценка возможности их использования нарушителем

Продемонстрировать

Практически продемонстрировать возможности использования уязвимостей (на примере наиболее критических

Оценить

Получить на основе объективных свидетельств комплексную оценку текущего уровня защищенности Системы

Порекомендовать

Выработать рекомендации по устранению выявленных уязвимостей и недостатков с целью повышения уровня защищенности Системы

Что мы проверяем?

Только комплексный подход к решению вопросов безопасности может обеспечить действительно полезную отдачу от проведенного аудита.

Веб-приложение

Это ваш сайт, лицо вашей компании. Его безопасность носит критический характер для компаний.

Серверное ПО

Функционирование вашей компании опирается на серверное ПО

Внешний периметр сети

Сегмент сети между внутренними системами и внешними сетями

HTTP протокол

Протокол, обеспечивающий передачу ваших данных содержащих гипертекстовые документы

Комплексный Аудит Безопасности веб-приложения

Мощный инструмент тестирования безопасности веб-приложений. Подразумевает ручной и инструментальный анализ всех скриптов веб-приложения и поиск в них уязвимостей. Мы выявляем уязвимости в 100% случаев, из них 86% являются уязвимости критического характера, способных привести к серьезным последствиям.

от 70.000 руб.

Пентест

Исследования

Аудит

Исследования

Тестирование
На проникновение (Pentest)

Пентест – это тест цель которого является выявление уязвимых мест системы заказчика и составления рекомендаций по устранению выявленных уязвимостей посредством имитации действий злоумышленника.

Пентест проводится как для внешнего анализа периметра корпоративной сети так и для внутренних ресурсов.

от 100.000 руб.

Аудит

Пентест

Исследования

- Исходного кода (Code Review)
- Тесты логики веб-приложений:
  - ✓ Подмены параметров
  - ✓ Ошибок фильтров или проверки на стороне клиента
  - ✓ Незащищенных страниц
  - ✓ Неавторизованного доступа
  - ✓ Ошибки многопоточности или низкий уровень абстракции

Индивидуальная оценка

Bug Bounty программа

Программа аудита безопасности, предполгающая поиск уязвимостей, по правилам которой Исполнитель получает вознаграждение только за их выявление. В свою очередь Заказчик выполняет оплату в соответсвии с оговоренной расценкой за каждую уязвимость соответсвенно.

По результату

Экспресс аудит безопасности сайта

Программа тестирования веб-сайта, предполагающая проверку на самые расспространенные ключевые уязвимости, угрожающие сайтам. Аудит не предполагает углубленного анализа и оптимален для ресурсов с небольшими объемами данных.

от 40.000 руб.

Почему МЫ?

Мы не верим в безопасные системы без уязвимостей. Наш многолетний опыт и компетенции позволяют решать задачи любого уровня сложности, начиная от аудита информационных систем до реверс инжиниринга мобильных приложений.

322

Веб-приложения

8.955

Уязвимостей

250

Организаций

8

Лет опыта

Индивидуальный подход к каждому клиенту и тесное взаимодействие в процессе работы - залог успешного выполнения проекта.

Кто наши Специалисты?

Наши специалисты демонстрируют высший уровень квалификации во всех проведенных работах. На 96% протестированных ресурсов были выявлены уязвимости критического характера. Отчеты и рекомендации по устранению выдаются в самом доступном виде.

Достижения

Крупнейшая награда за нахождение уязвимости от Яндекса, позиции среди первых 50 лучших хакеров по рейтингу hackerone

Разработка

Написали собственную утилиту для поиска скрытых портов в unix системах

Bug Bounty

Десятки наград по программам Баг Баунти ведущих компаний вроде mozilla, yahoo и др.

10 Аудиторов высшего звена

Нашли уязвимости таких систем как:

- Visa
- MasterCard
- Microsoft.com
- Intel.com
- Twitter.com
- Yahoo.com
- Adobe.com
- Vimeo.com
- Dropbox.com
- Yandex.ru
- Qiwi.ru
- Ok.ru

Международные стандарты

Мы проводим работы по анализу по таким общепризнанным стандартам и руководствам по обеспечению информационной безопасности как:

- Open Source Security Testing Methodology Manual OSSTMM
- Information Systems Security Assessment Framework ISSAF
- British Standards Institution BSI Penetration Testing Model
- Web Application Security Consortium WASC Threat Classification v2.0
- Open Web Application Security Project OWASP Testing Guide

Отчет о проведенной работе соответствует вышеперечисленным стандартам.

Продукция Global IT

Мы предлагаем только совершенные технологии защиты данных

РОССИЙСКИЕ СЕРТИФИЦИРОВАННЫЕ МЕЖСЕТЕВЫЕ ЭКРАНЫ

Межсетевые экраны унифицированной защиты сети с сертификатами ФСТЭК НДВ-2/МЭ-2, ФСБ МЭ-4, СОВ-2

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ДАННЫХ

USB флэш-накопители с 256-битным аппаратным шифрованием военного класса AES.

СИСТЕМЫ ЗАЩИТЫ ВЕБ-ПРИЛОЖЕНИЙ

Автоматическое обнаружение, классификации, распознавания и блокировки угроз и атак.

ЗАЩИЩЕННЫЕ ПРОГРАММНО-ТЕХНИЧЕСКИЕ КОМПЛЕКСЫ

Решения для надежной защиты ИТ-инфраструктуру от кибер угроз нового типа.

Еще..

Деятельность Global IT

Наиболее актуальный комплекс услуг в области обеспечения информационной безопасности и защиты информации

АУДИТ БЕЗОПАСНОСТИ WEB-ПРИЛОЖЕНИЙ

глубокий анализ защищенности всех компонентов Web-приложений: механизмы авторизации, сетевое взаимодействие, хранилища информации, серверные и клиентские компоненты, настройки ОС.

АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

комплекс работ, включающий исследование всех аспектов обеспечения информационной безопасности в организации, проводимое по согласованному с заказчиком плану, в соответствии с выбранной методикой и критериями.

ЦЕНТР ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ И ИНТЕГРАЦИИ

сервисное обслуживание пользователей продукции различных производителей для оказания технической поддержки первого уровня.

ОЦЕНКА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

поможет правильно оценить риски информационной безопасности, разработать и внедрить процедуру оценки рисков.

АТТЕСТАЦИЯ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ И АВТОМАТИЗИРОВАННЫХ СИСТЕМ

определяется соответствие объекта требованиям стандарта и нормативным документам по обеспечению безопасности информации.

РАЗРАБОТКА ДОКУМЕНТАЦИИ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

разработка организационно-распорядительных документов в области информационной безопасности для различных по размеру и профилю компаний.

Еще..

КПРФ

ВОКРУГ СВЕТА
VOKRUGSVETA.RU

MECHEL

MirCli

X5 RETAIL GROUP

REG.RU

интернет хостинг центр

ALFA CASHIER

ХЛЕБПРОМ

Быстроденьги
займы до зарплаты

beget
IO-HOSTS

nethouse

Эти компании доверили нам свою безопасность и остались довольны. Что насчет Вас?

Всегда рады
Помочь Вам

Безопасность ночью не ждет, поэтому мы работаем 24/7

Москва, Варшавское ш. 28А, оф. 239

+7 (495) 108 24 12

info@antihacking.ru

antihacking.ru

globalitrus

/globalitrussia

Вся представленная в информация, касающаяся технических характеристик и стоимости услуг, носит информационный характер и ни при каких условиях не является публичной офертой, определяемой положениями Статьи 437(2) Гражданского кодекса РФ. ООО «Глобал АйТи» ИНН 7743861490 КПП 772601001 117105, г. Москва, Варшавское шоссе д. 28а, оф. 239. GLOBAL IT LLC