Содержание

4.....НАМИБ

8.....КОМИБ

10.....Angara Security

16.....Код Безопасности

20.....Музей криптографии

22.....Сайберус — Безопасности

26.....Сайберус — CyberED

34.....Сайберус — Кибердом

34.....Сайберус — Кибериспытание

38.....Security Vision

НАМИБ

Национальная Ассоциация международной информационной безопасности (НАМИБ) – некоммерческая организация, созданная в 2018 году по инициативе Совета Безопасности РФ для координации деятельности членов Ассоциации по содействию реализации государственной политики Российской Федерации в области международной информационной безопасности (МИБ).

К основным целям деятельности НАМИБ отнесены:

- содействие продвижению российских инициатив в области обеспечения МИБ;
- содействие федеральным органам законодательной и исполнительной власти Российской Федерации в их деятельности по реализации государственной политики в области МИБ, по обеспечению национальных интересов Российской Федерации в информационной сфере, а также российским коммерческим и некоммерческим организациям, и гражданам, участвующим в соответствии с законодательством Российской Федерации в реализации государственной политики в указанной области;
- содействие формированию системы обеспечения устойчивого функционирования глобальной и национальной информационных инфраструктур безопасного использования информационных и коммуникационных технологий во всех сферах жизни общества и управления государством.

Учредителями Ассоциации являются:

МГУ имени М.В. Ломоносова,
МГИМО,
РАНХиГС,
Дипломатическая академия МИД России,
Редакция журнала «Международная жизнь».

Председатель Наблюдательного совета Ассоциации:

Олег Владимирович Храмов,
заместитель Секретаря Совета Безопасности Российской Федерации.

«...в эффективной реализации государственной политики, обозначенной в новой редакции Основ государственной политики в области международной информационной безопасности, надо активнее использовать возможности научных и экспертных кругов, делового сообщества, в том числе, конечно, Национальной Ассоциации международной информационной безопасности.»

- Президент России В.В. Путин

Форум партнерства Россия-Африка, 2024 г.

Основные направления деятельности

- проработка в упреждающем режиме проблемных вопросов обеспечения МИБ в интересах формирования переговорных позиций государственных органов; организация взаимодействие с МИД России и заинтересованными федеральными органами законодательной и исполнительной власти с коммерческими и некоммерческими организациями и гражданами, содействующими реализации государственной политики в области МИБ;

- участие в составе российских делегаций в подготовке и проведении экспертных консультаций по вопросам формирования системы МИБ в формате международных организаций (ООН, ОБСЕ, ШОС, СНГ, ОДКБ, БРИКС, АТЭС, «Группы двадцати» и др.), а также двусторонних, многосторонних и региональных консультаций Российской Федерации с другими государствами;

- подготовка совместно с заинтересованными организациями и федеральными органами исполнительной власти предложений по укреплению международного сотрудничества, направленного на содействие успешному осуществлению нацпроекта «Экономика данных» в части, касающейся вопросов информационной безопасности.

Основные мероприятия и проекты

- Ежегодный Международный форум «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности». XIX Форум пройдет в Москве 16-18 сентября 2025 г. в гибридном (очно и on-line) формате.

- Международная конференция по проблемам обеспечения системы международной информационной безопасности (по плану Международного исследовательского консорциума информационной безопасности).

▷ НАМИБ аккредитована при Рабочей группе открытого состава ООН по международной информационной безопасности

▷ На Ассоциацию возложены функции Контактного Пункта для прямого взаимодействия по линии научно-академических организаций стран-членов БРИКС по вопросам МИБ.

Издательская деятельность

- Сборники докладов участников XVII и XVIII международных форумов «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности»

- Особенности политики государств – участников БРИКС в сфере развития ИКТ, обеспечения национальной и международной информационной безопасности

- Сборник материалов по проблематике информационной безопасности государств – членов Лиги арабских государств

Подробнее
о нас:

КОМИБ

— проверенный инструмент создания справедливой, надежной и устойчивой системы международной информационной безопасности.

Автономная некоммерческая организация «Центр координации государственно-частного партнерства в области международной информационной безопасности» (АНО КОМИБ) создана Национальной Ассоциацией международной информационной безопасности при поддержке Совета Безопасности Российской Федерации для повышения эффективности государственно-частного партнерства во внешнеэкономической деятельности в области информационной безопасности.

КОМИБ:

- консультирует иностранных партнеров при разработке государственных программ создания комплексных систем ИБ на базе решений, предлагаемых российскими компаниями;
- рекомендует иностранным партнерам релевантные российские компании для выполнения проектов ИБ;
- обеспечивает необходимые согласования для исполнения международных проектов ИБ;
- помогает иностранным партнерам осуществлять независимый аудит по текущим комплексным проектам в области ИБ с российскими компаниями.

Деятельность КОМИБ в формате G2B ориентирована на потребности и интересы российских операторов связи, провайдеров, поставщиков ИТ-услуг, а также производителей товаров и услуг в сфере информационной безопасности.

Подробнее о нас:

КОМИБ выполняет как представительские, так и обслуживающие функции для компаний, работающих на рынке информационной безопасности:

- обеспечивает помощь, предоставляет консультации по ведению бизнеса;
- представляет интересы предпринимателей при взаимодействии с органами власти;
- оказывает помощь в формировании правовой среды и инфраструктуры предпринимательства;
- оказывает помощь российским предпринимателям в установлении деловых связей с иностранными партнёрами.

КОМИБ

- обладает необходимыми техническими компетенциями;
- владеет необходимой экспертизой в области международных отношений для участия в формировании перего-ворных позиций в ходе консультаций в формате G2G;
- профессионально оценивает текущую ситуацию на международных рынках, способна давать надежные прогнозные оценки развития ситуации на внешних рынках ИБ;
- имеет сложившиеся рабочие контакты с коммерческими компаниями для привлечения заинтересованных организаций к работе в контексте достигнутых в формате G2G договоренностей.

ANGARA SECURITY

**Angara Security — группа компаний,
создающая передовые решения и сервисы в сфере кибербезопасности
и предоставляющая полный спектр услуг по защите информации:**

- проектирование, внедрение и сопровождение как комплексных систем обеспечения ИБ (СОИБ), так и отдельных решений;
- сервисы для управления киберустойчивостью на всех этапах Cyber Kill Chain®, а также выявления, реагирования и предупреждения киберинцидентов, анализа защищенности информационных инфраструктур;
- услуги по безопасной разработке, консалтингу и аудиту и многое другое.

Услуги кибербезопасности

ANGARA SECURITY

Мониторинг и управление киберинцидентами (SOC and MDR)

Круглосуточный мониторинг киберинцидентов на всех стадиях — от предотвращения и выявления киберинцидентов до реагирования и устранения последствий.

Для оказания услуги используется стек программных продуктов, базирующийся на системах классов SOAR, SIEM и EDR, а также ML-сценарии собственной разработки.

Компьютерная криминалистика и реагирование на киберинциденты

Реагирование на киберинциденты, устранение их последствий, а также исследование образцов вредоносного программного обеспечения. Предоставляем детальный отчет по реагированию, реконструкцию событий инцидента, а также даем рекомендации по повышению уровня защищенности информационной инфраструктуры для предотвращения подобных инцидентов в будущем.

Управление цифровым следом (Digital footprint analysis and DRP)

Сбор и анализ информации из открытых источников как в индексируемых, так и неиндексируемых сегментах сети Интернет (в т.ч. в мессенджерах, социальных сетях и т.д.), которая может свидетельствовать:

- о свершившейся или планируемой компьютерной атаке на организацию;
- о краже и/или продаже конфиденциальной информации;
- об использовании брендинга компании в фишинговых целях.

Управление поверхностью атаки и ак (Attack Surface and Internal Assets Ma

Услуга позволяет получать данные об актуальном сост и внутреннего периметра, а также всю необходимую и для устранения наиболее критичных уязвимостей. Заключается в постоянном автоматизированном сканировании внешнего периметра и активов внутри инфраструктуры с целью выявления новых хостов, сетевых портов и уязвимостей.

Полученные результаты верифицируются, после чего ранжируются по степени критичности и формируются в перечень выявленных уязвимостей и недостатков.

Решения для кибербезопасности

Внедрение, поддержка, аудит

Внутреннее и внешнее тестирование на проникновение

Проверка уровня защищенности инфраструктуры и приложений путем моделирования действий злоумышленника. Также производится демонстрация векторов атак, которые возможно реализовать с использованием выявленных уязвимостей. Работы могут проводиться из сети Интернет или путем подключения к корпоративной сети. Тестирование на проникновение поможет:

- оценить текущий уровень кибербезопасности вашей инфраструктуры;
- проверить эффективность системы киберзащиты;
- получить подробные рекомендации по устранению найденных уязвимостей.

Анализ мобильных и веб-приложений

Оценка состояния защищенности приложений как отдельной информационной системы. Работы проводятся с учетом общепринятых практик и рекомендаций OWASP и SANS/CWE. Проверяются не только технические аспекты, но и бизнес-логика приложений и возможность проведения атак на клиентов приложений.

Выявление нестойких паролей

Проверка стойкости паролей, используемых в корпоративной сети, к взлому или подбору. При выполнении данных работ мы делаем копию базы NTDS (Active Directory), обезличиваем ее и выполняем перебор по часто встречающимся, утекшим или легко угадываемым паролям. В результате работ заказчик получает перечень тех учетных записей, которые могут быть скомпрометированы в короткие сроки с использованием онлайн брутфорс-техник и информации о публичных утечках данных аутентификации.

Тестирование с применением методов социальной инженерии

Проверка осведомленности сотрудников об атаках с применением методов социальной инженерии. Разрабатываются различные сценарии и легенды, эксплуатирующие человеческие слабости (любопытство, страх, жажду наживы и т.п.).

Варианты сценариев:

- различные виды почтового фишинга (phishing, spearphishing);
- телефонный обзвон работников (voice phishing);
- имитация зараженных носителей.

Red Team Operations

Проверка адекватности и корректности процессов мониторинга событий безопасности (SOC, SIEM, IRP...) путем имитации реальных атак на инфраструктуру с использованием продвинутых техник и инструментов. В процессе работ происходит плотное взаимодействие с командой защиты, чтобы выявить возможные пробелы в правилах корреляции, недостатки конфигураций средств защиты информации или процессов реагирования на инциденты.

Услуги по оценке рисков ИБ

Определение основных рисков ИБ и приоритетных направлений развития системы обеспечения информационной безопасности. В рамках услуги предлагается сбор и анализ исходных данных по компании в части бизнес-процессов и ИТ-инфраструктуры, разработка методики оценки рисков ИБ и проведение самой оценки рисков ИБ.

Комплексная защита систем информатизации

Создание комплексной системы информационной безопасности, предусматривающей реализацию организационных и технических мер для выполнения требований законодательства и международных стандартов по созданию систем защиты и обеспечению безопасности информационных систем.

Анализ исходного кода приложений

В рамках услуги применяются как автоматизированные инструменты (сканеры), так и ручной анализ. Предмет анализа — уникальный исходный код и используемые в нем сторонние компоненты (зависимости), которые могут содержать известные уязвимости.

Помимо этого, может проводиться глубокий поиск секретов внутри git-репозиториев с целью выявления их потенциальной компрометации.

Создание защищенного процесса разработки

В рамках услуги проводится детальный анализ процессов разработки и инфраструктуры DevSecOps, включающий в себя:

- аудит уровня зрелости ИБ-процесса разработки;
- аудит безопасной настройки инфраструктуры DevSecOps;
- создание дорожной карты повышения защищенности и обеспечения кибербезопасности как кода приложения, так и его окружения.

Аудит ИБ

Детальный анализ ИТ-инфраструктуры и процессов ИБ на соответствие законодательству и международным стандартам (в том числе ISO/IEC 27001).

Услуга включает в себя аудит процессов ИБ, технический аудит, тестирование на проникновение и подготовку отчетной документации.

Продукты для кибербезопасности

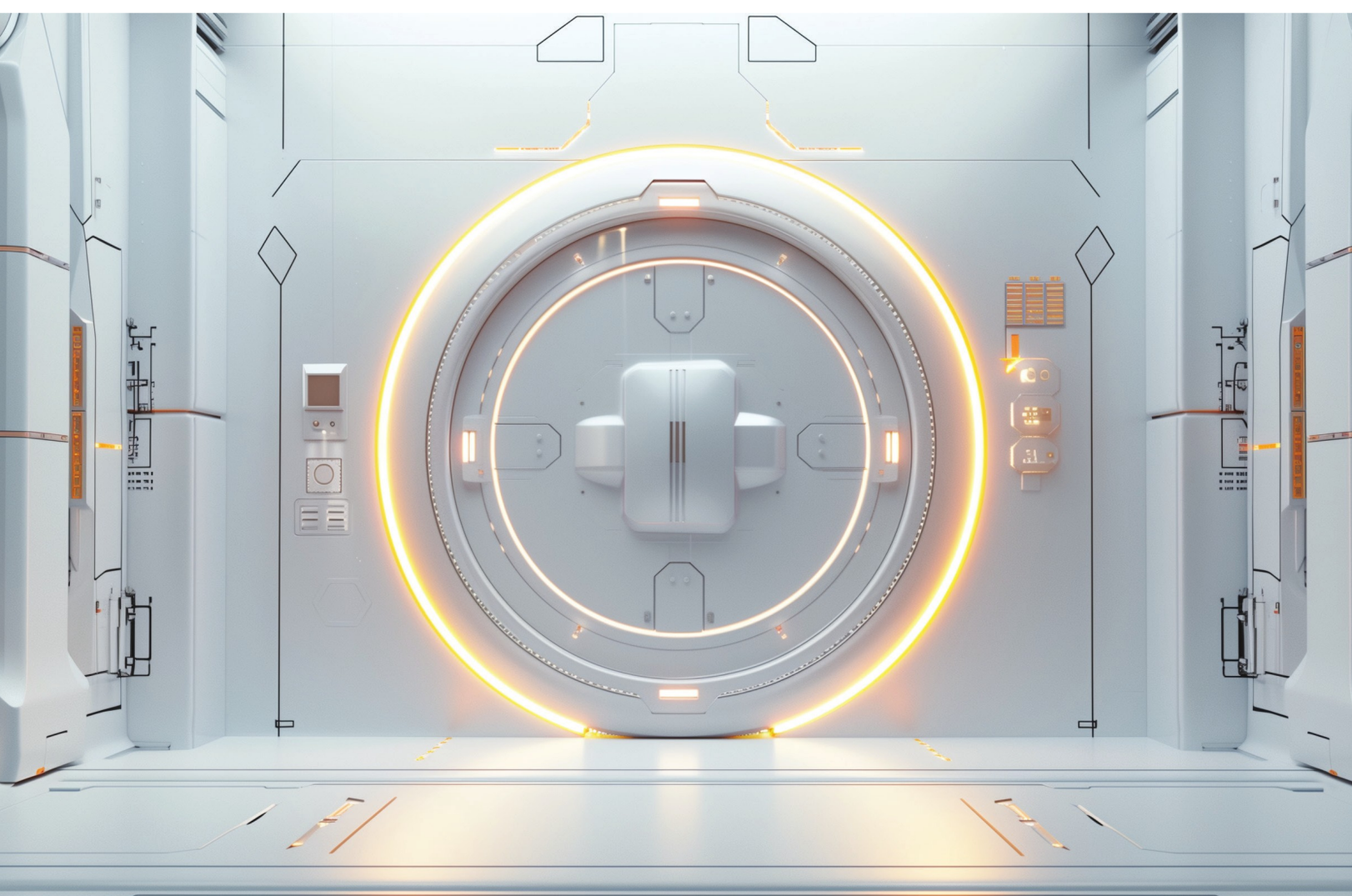
Angara ECHO

Платформа для управления цифровым следом. Angara ECHO проводит автоматизированный мониторинг и анализ в индексируемых и неиндексируемых источниках, чтобы оперативно обнаружить чувствительную информацию.

Принять превентивные меры гораздо дешевле, чем реагировать на инцидент ИБ и устранять его последствия. Angara ECHO позволит лучше подготовиться к планируемым атакам или вовсе их предотвратить.

Blazar NAC

Российское решение класса Network Access Control. Обеспечивает защиту информационных ресурсов от несанкционированного доступа путем настройки и строгого соблюдения политик доступа к корпоративной сети.



ANGARA SECURITY

КОД безопасности

Российский разработчик широкого спектра программных и аппаратных средств защиты информационных систем, соответствующих требованиям российских и международных стандартов

Продукты «Кода Безопасности» применяются для защиты конфиденциальной информации, персональных данных, а также сведений, составляющих государственную и коммерческую тайну.
Средства защиты «Кода Безопасности» составляют единую экосистему безопасности и предназначены для защиты ключевых элементов ИТ-инфраструктуры:
Компания разрабатывает несколько линеек продуктов, объединенных общим архитектурным замыслом и ориентированных на обеспечение комплексной безопасности ключевых компонентов ИТ-инфраструктуры. Такой подход позволяет нашим заказчикам поэтапно развивать свою систему обеспечения информационной безопасности.

Под Защитой Кода Безопасности

более 3 млн рабочих мест.

Сегодня продукты

«Код Безопасности»,

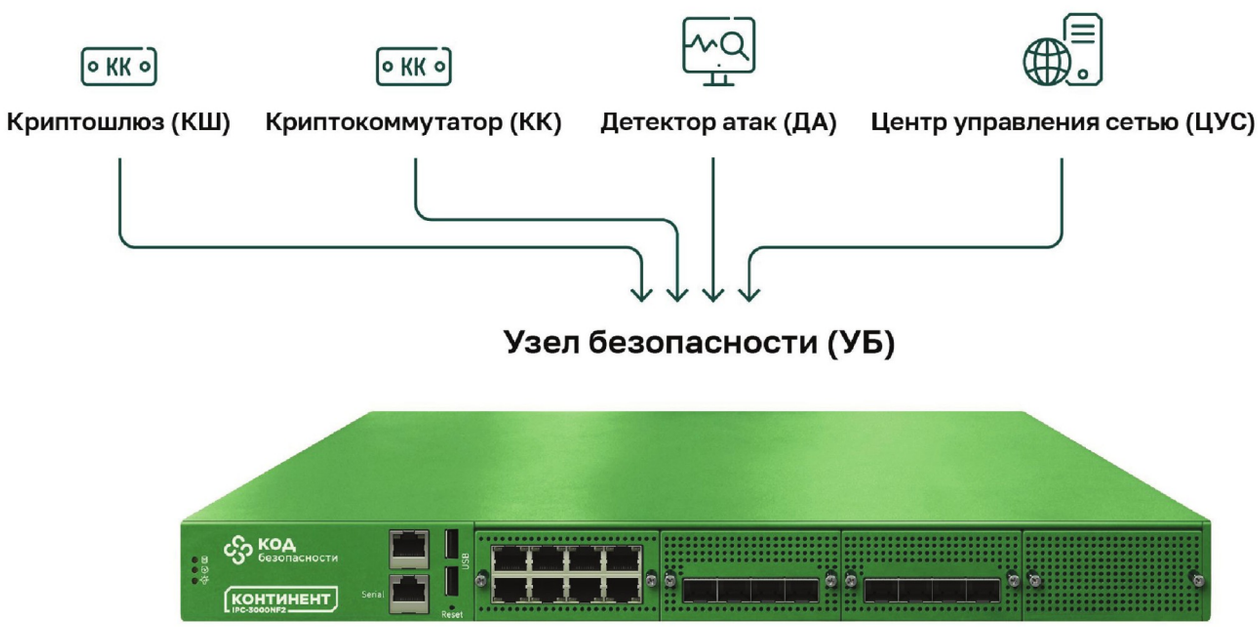
используют
более 50000 организаций
среди которых -
государственные структуры и крупные коммерческие компании.

NGFW Континент 4

Задачи:

- Защита внешнего периметра сети
- Защита сетей центров обработки данных
- Защита геораспределенных сетей
- Защита технологических сетей

Возможности:



FW | IPS | App Control | L2 VPN | L3 VPN | MGMT | Threat Intelligence | Log | URL Filtering | Antivirus | GeoIP

Решение покрывает все потребности заказчиков как в небольших устройствах, так и в высокопроизводительных устройствах

Высокопроизводительные устройства

Средние устройства

КОД БЕЗОПАСНОСТИ

Security Code Orchestrator

Задачи:

- Централизованное управление продуктами Кода Безопасности
- Единая система мониторинга
- Шина интеграции разнородных продуктов между собой

Возможности:

КОД безопасности

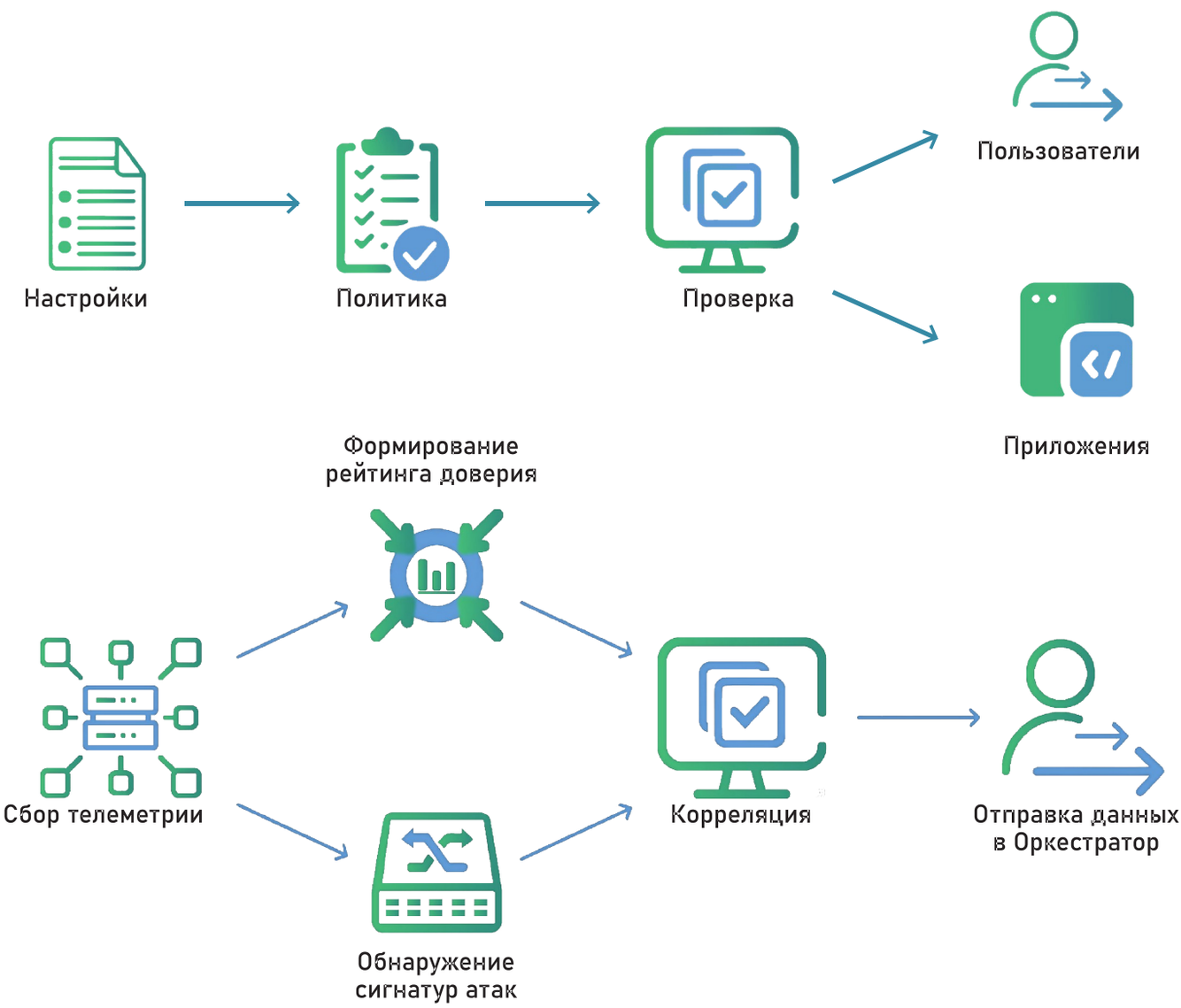
S ecret Net EDR

Задачи:

- Сбор и обработка телеметрии с конечных устройств
- Выявление признаков вредоносной активности
- Формирование рейтинга доверия конечному устройству для дальнейшего использования другими средствами защиты
- Проверка конечной точки на соответствие требованиям безопасности

Возможности:

Проверка на соответсвие параметрам



Музей Криптографии

Музей криптографии –
первый и единственный в России научно-технологический музей, посвященный криптографии, смежным дисциплинам и технологиям коммуникации, был открыт для широкой публики в декабре 2021

Музей располагается в Москве, в историческом здании на Ботанической улице, 25, построенном в 1885 году как Александро-Мариинский приют для детей бедных священников. Более 60 лет здание занимали школы, детские дома и спецтюрьма, знаменитая Марфинская шарашка, где с 1947 по 1954 годы заключенные и вольнонаемные ученые вместе работали над созданием техники секретной связи.

В 1950-е годы шарашка была преобразована в Научно-исследовательский институт автоматики. Здание оставалось засекреченным вплоть до 2019 года, когда было передано Музею криптографии.

Постоянная экспозиция музея рассказывает о прошлом, настоящем и будущем криптографии и технологий коммуникации, о людях и изобретениях, изменивших мир. Она включает четыре раздела и построена в обратной хронологии: от цифровой эпохи и компьютеров маршрут ведет к эпохе индустриальной, когда были созданы радио, телефон, телевидение и телеграф. Затем — к эпохе домашинной криптографии, когда основным средством передачи информации были письма. И, наконец, к протокриптографии — к зарождению самой идеи письменной коммуникации посредством алфавитных систем и знаков. Отдельный, пятый раздел музея, посвящен истории здания и людям, чьи судьбы были с ним связаны.

В экспозиции представлена уникальная коллекция шифровальной техники и архивных документов, большинство из которых впервые демонстрируется широкой публике, а также специально созданные интерактивные, мультимедийные и игровые экспонаты, объясняющие простым языком детям и взрослым суть сложных криптографических механизмов и математических понятий. С их помощью можно разгадать криптографические загадки, разобраться в устройстве сложных систем шифрования, узнать о секретах безопасной коммуникации в разные эпохи, установить взаимосвязь криптографии и важных исторических событий, заглянуть в будущее.

В экспозиционных залах и общественных пространствах музея также можно увидеть произведения медиаискусства, которые дополняют основную экспозицию и создают особое повествование о влиянии науки на жизнь человека и общества. Экспозиция и общественные пространства музея созданы с учетом потребностей самых разных посетителей. В музее есть издательская программа, проходят лекции и мастерклассы, кинопоказы и конференции, временные выставки и другие события, отвечающие основной миссии музея — просветительству и популяризации науки и технологий.

Помо
стран

Киберсуверенитет как основа процветания нации

Киберсуверенитет — неотъемлемая составляющая независимости государства, его способность самостоятельно защищать национальное киберпространство, объективно оценивая уровень кибербезопасности и исключая зависимость от других государств или зарубежных корпораций. Это вопрос стратегического планирования и государственного управления, который затрагивает интересы всех слоёв общества.

Национальная безопасность

Без контроля над собственными цифровыми ресурсами страна рискует стать уязвимой к вмешательству со стороны других государств или киберпреступников.

Экономическая независимость

Разработка собственных технологий и систем безопасности позволяет снизить риски от других стран, обеспечить экономическую самостоятельность и стимулировать внутренние инновации.

Социальное благополучие

Защита данных граждан от утечек и злоупотреблений — это не только вопрос конфиденциальности, но и ключевой элемент доверия к государственным институтам.

ПМЭФ, 2024. Подписание соглашения с Оманом в присутствии министра торговли, промышленности и продвижения инвестиций Кайса бин Мохаммеда Аль Юсефа.

Роль государства в цифровом развитии

Киберсуверенитет содействует созданию устойчивой цифровой среды. Развитие национальной стратегии кибербезопасности позволяет наладить эффективное сотрудничество между различными уровнями власти и частным сектором, формируя единую политику в сфере кибербезопасности.

Инновации и развитие талантов

Киберсуверенитет открывает возможности для развития внутреннего рынка ИТ, привлекая таланты и инновации. Защита интеллектуальной собственности и поддержка стартапов в области кибербезопасности может значительно усилить позиции страны на международной арене.

Глобальное сотрудничество

Киберсуверенитет стимулирует международное сотрудничество. Обмен опытом с другими государствами в области кибербезопасности позволяет создать глобальную сеть защиты от киберугроз. Достижение киберсуверенитета государства опирается на три взаимосвязанных процесса: измерение эффективности киберзащиты государства, развитие человеческого капитала и национальных технологических компетенций.

Как Сайберус помогает странам-партнёрам строить киберсуверенитет

Сайберус — фонд развития результативной кибербезопасности, объединяющий силы разработчиков технологий киберзащиты, бизнеса и государства для построения безопасного цифрового будущего России и мира.

На базе экспертизы и опыта российских компаний в сфере кибербезопасности и при поддержке государства Сайберус формирует единое страновое предложение по развитию индустрии кибербезопасности для достижения киберсуверенитета страны-партнёра.

Фонд предлагает решения, которые трансформируют национальные отрасли и создают устойчивый фундамент для их независимого и самодостаточного развития.

Три взаимосвязанных мета-продукта Сайберус

1 Развитие человеческого капитала

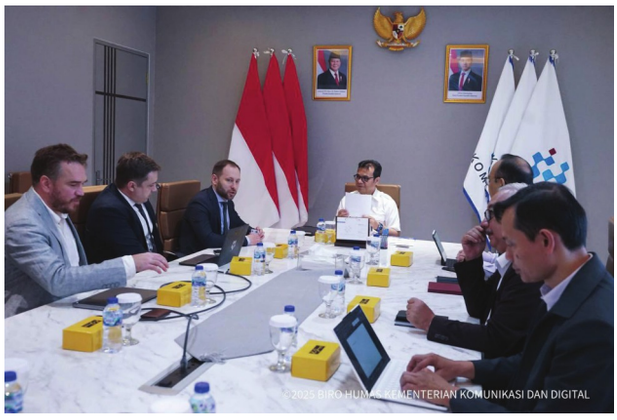
Для укрепления киберсуверенитета необходимо создать и постоянно развивать национальное сообщество специалистов по кибербезопасности. Мета-продукты Сайберус включают механизмы, направленные на обучение, поддержание интереса и создание возможностей для финансовой и карьерной реализации в этой сфере, что приводит к формированию самовоспроизводящегося профессионального сообщества.

2 Измерение эффективности киберзащиты государства

Чтобы объективно оценить уровень киберзащищённости, необходимо определить неприемлемые для государства события, а также стоимость кибератак, которые могут к ним привести. Сайберус обладает методикой непрерывного измерения эффективности киберзащиты посредством контролируемых кибератак.

3 Усиление национальных технологических компетенций

Сайберус предоставляет критически важные для кибербезопасности информационные системы, решения и методики в форматах, не только позволяющих укрепить киберсуверенитет стран-партнёров, но и открывающих возможности для реэкспорта. Мета-продукты Сайберус свободны от ограничений на модификацию.



Индонезия, апрель 2025. Переговоры с Министерством коммуникаций и цифровых технологий Индонезии в рамках российско-индонезийского бизнес-форума.

Москва, март 2025. Подписание соглашения с ОДКБ. Подписанты: генсек ОДКБ Имангали Тасмагамбетов и сооснователь Сайберус Юрий Максимов.

Санкт-Петербург, апрель 2024. Сайберус представил экспортное предложение на Встрече Высоких представителей, курирующих вопросы безопасности.

САЙБЕРУС

Более 30 стран ведут переговоры с Сайберус по вопросам развития суверенной индустрии кибербезопасности.

Среди партнёров проекта: Positive Technologies, Innostage, Кибериспытание, CyberED, Кибердом, EveryTag и другие игроки российской индустрии кибербезопасности.

CyberED

Создайте образовательную среду для роста профессионалов в кибербезе

Сверхбыстрое развитие мировой отрасли кибербеза предъявляет всё более высокие требования к уровню квалификации специалистов по информационной безопасности, а также к количеству высококлассных экспертов для обеспечения защиты национальных интересов.

CyberED — образовательная платформа, входящая в фонд развития результативной кибербезопасности Сайберус. Проект нацелен на создание и развитие образовательных проектов в сфере кибербезопасности, через реализацию которых происходит усиление локального экспертного сообщества, повышение защищённости бизнеса и критической инфраструктуры, а также ускорение внедрения инноваций.

От онлайн-обучения до оценки и сертификации

CyberED предлагает более 70 программ в разных сферах кибербеза, а также комплекс инструментов для успешного освоения знаний и навыков, который включает LMS платформу для дистанционного обучения, учебный контент и платформы для практических упражнений и лабораторных работ.

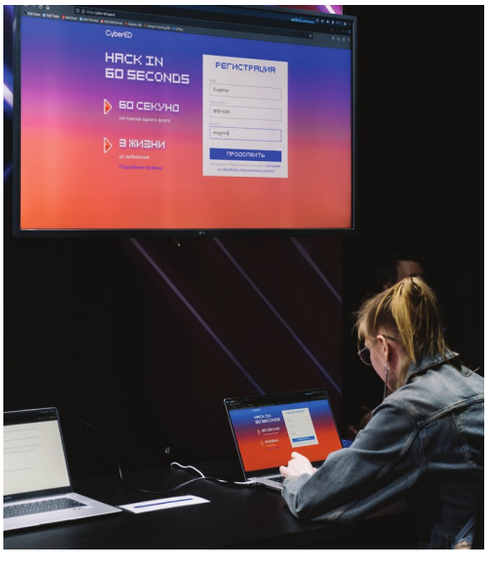
Обучение с нуля до уровня мировых экспертов

В CyberED работают преподаватели-практики, которые эффективно помогают студентам развить необходимые навыки, продвинуться по карьерной лестнице и глубоко понять процессы отрасли.

Комплексный подход

Образовательные программы CyberED охватывают практически все направления кибербеза, включая наступательную безопасность (red team), построение защиты (blue team), безопасную разработку.

Цель CyberED — создать образовательную среду, где объединены высококлассное обучение и профессиональное комьюнити для обмена опытом.



Проводим обучение на базе 30+ собственных лабораторных стендов, имитирующих реальный опыт решения задач.

Выпускники CyberED уже сейчас формируют будущее кибербезопасности по всему миру

6600+ специалистов
по кибербезопасности прошли обучение на платформе CyberED за 6 лет

300+ российских компаний
доверили CyberED обучение сотрудников

70+ образовательных программ
с возможностью доработки под требования заказчика предлагает CyberED.

При проработке программ учитывается и адаптируется международный опыт обучения образовательных компаний в сфере ИБ.

В 2024 году CyberED в партнёрстве с Positive Technologies организовал международный хакатон Hack Camps.

Практика в условиях атак

Сотрудничаем со Standoff 365, одной из крупнейших в мире кибертренировочных площадок, предоставляя стажировки нашим студентам.

Международный опыт

В 2024 году CyberED в партнёрстве с Positive Technologies организовал международный хакатон Hack Camps. В рамках проекта более 50 иностранцев из стран Ближнего Востока, Африки и Юго-Восточной Азии приехали в Россию на 2 недели и получили актуальные навыки от лучших специалистов по кибербезопасности в РФ.

Оценка навыков и сертификация

Проводим эффективную оценку навыков команд на основе ролей специалистов. Предоставляем подробные данные о профессиональном развитии и росте.

Профессиональные соревнования

Организуем CTF (Capture The Flag) соревнования с моделированием реальных угроз и инцидентов, чтобы развивать навыки командной работы и решения проблем в условиях стресса.

Индивидуальный подход

Скорректируем существующие или соберём с нуля образовательные программы с учётом потребностей страны-партнёра.

Программы CyberED

1 / Red Team

Ethical Hacker / Профессия «Белый Хакер»

Курс по основам этичного хакинга для начинающих специалистов. Включает базовые знания по взлому систем и защите информации.

Penetration Testing Specialist / Специалист по тестированию на проникновение

Основной курс, посвящённый освоению профессиональных навыков в тестировании на проникновение. Включает практические задания и работу с реальными сценариями атак.

Web Application Attacks / Получение первичного доступа через атаки на веб-приложения

Дополнительный продвинутый курс со специализацией на атаках на веб-приложения и изучении их уязвимостей.

Active Directory Attacks / Атаки на Active Directory

Дополнительный курс, посвящённый анализу уязвимостей и методам атак на Active Directory.

Social Engineering Attacks / Получение первичного доступа через атаки социальной инженерии

Курс, направленный на изучение методов социальной инженерии. Включает практические примеры и рекомендации по защите от таких атак.

2 / Blue Team

Information Security Specialist / Специалист по противодействию кибератакам

Курс по изучению основ информационной безопасности для начинающих специалистов. Включает базовые методы защиты систем и обнаружения атак.

Security Operations Center Analyst / Аналитик Центра противодействия кибератакам

Основной курс по подготовке специалистов для работы в центрах противодействия кибератакам. Включает теоретические и практические модули.

Threat Intelligence

Дополнительный курс, посвящённый сбору, анализу и использованию данных об угрозах. Включает практическую работу с Threat Intelligence платформами.

Defending against Web Application Attacks / Веб-приложения: отражение атак

Дополнительный курс по защите веб-приложений от атак. Рассматриваются реальные кейсы атак и их предотвращение.

Practical Blue Team Course / Практический курс Blue Team

Дополнительный практико-ориентированный курс в области Defensive Security, направленный на повышение навыков и отработку сценариев выявления сложных APT атак. Предназначен для расширения знаний и повышения квалификации специалистов SOC.

3 / Secure Software Development

Fundamentals of Secure Software Development / Основы безопасной разработки

Видеокурс по основам безопасной разработки программного обеспечения для начинающих специалистов. Рассматриваются основные уязвимости и методы их предотвращения.

Secure Software Development Specialist / Специалист по безопасной разработке приложений)

Основной курс, нацеленный на профессиональное освоение навыков безопасной разработки приложений. Рассматриваются реальные примеры и лучшие практики обеспечения безопасности ПО.

4 / Custom Courses

Индивидуальные программы обучения, разрабатываемые на основе запросов клиента. Учитывают специфические потребности заказчика и уровень подготовки сотрудников.

кибердом

Место силы индустрии кибербезопасности

Для обеспечения киберсуверенитета страны необходимо создание внутренних сил кибербезопасности — специалистов по реагированию и защите, этичных хакеров, а также внутренних решений по IT и кибербезопасности для эффективного импортозамещения. Но просто обучить специалистов мало. Важно, чтобы они не релоцировались в другие страны, которые могут предложить лучшие условия и интересные проекты. Решить эту задачу помогает формирование сильного кибербез-сообщества и создание интересных отраслевых проектов.

Кибердом — эпицентр развития технологической индустрии страны, а также её глобальный амбассадор на мировой арене.

150 тыс

человек посетили Кибердом в 2024 году

1,5 тыс

экспертов индустрии кибербезопасности

300

проектов реализовано

Объединение в интересах страны

Кибердом объединяет и сонаправляет главных акторов индустрии для достижения общих целей в сфере кибербезопасности и киберсуверенитета. Каждая аудитория находит здесь то, что для неё важно.

Профессиональное сообщество. Комфортная среда для сотворчества и развития специалистов индустрии.

Бизнес. Продвижение передовых продуктов и решений, поддержка импортозамещения.

Государство. Демонстрация решающей роли государства в развитии технологий для безопасной цифровизации страны.

Кадры и стартапы. Образование и развитие следующего поколения профессионалов, которые будут развивать отрасль и защищать государство.

Общество. Повышение уровня цифровой грамотности и популяризация профессий в области информационной безопасности.

Киберполигон, где проводятся соревнования на макетах, воссоздающих инфраструктуру различных индустрий: нефтедобывающей, транспортной, финансовой и других.

Киберполигон — сердце Кибердома

Для демонстрации возможностей технологий информационной безопасности в Кибердоме находится киберполигон — постоянно действующая мультиформатная площадка для развития практических навыков белых хакеров и динамичного погружения зрителей в результативную кибербезопасность в режиме шоу, экспозиции или кибербитвы.

На киберполигоне воспроизводятся кибератаки разной степени сложности, которые могут в реальности происходить на объектах разных отраслей, например, транспортной, финансовой, нефтедобывающей и др. Участники могут исследовать уязвимости, отрабатывать защитные тактики и формировать стратегии противодействия реальным угрозам.

На киберполигоне проводятся:

- тренировки Blue Team и Red Team компаний;
- киберучения для студентов специальности «информационная безопасность»;
- кибербитвы и CTF-соревнования как для профессионалов мирового уровня, так и для молодых специалистов.

Представительские пространства Кибердома — место важных встреч и переговоров.

От киберграмотности до международного сотрудничества

Универсальное пространство Кибердома можно использовать для самых разных задач, в том числе для демонстрации национальных технологий и уровня развития индустрии. Еженедельно московский Кибердом принимает делегации из стран Ближнего Востока, Юго-Восточной Азии, Африки и других регионов. Среди гостей — предприниматели, представители иностранных правительств, дипломаты и сотрудники международных государственных организаций, таких как ООН.

Международная сеть Кибердомов позволяет выстроить конфиденциальный обмен опытом и информацией между регионами и странами за счёт кросс-обучения специалистов, демонстрации внутренних технологий и продуктов для зарубежных рынков, проведения международных и региональных конференций в офлайн- и онлайн-форматах, организации международных кибербитв для тренировок этичных хакеров. Всё это направлено на системное и эффективное продвижение результативной кибербезопасности и развитие киберсуверинитета страны.

Примеры проектов для локализации в Кибердоме вашей страны

Развитие технологий и продуктов

Независимые тестирования для развития и совершенствования ИБ-решений рынка: WAF-день, NGFW-день, SIEM-день и другие мероприятия

Развитие и менторство стартапов, M&A

Бизнес-клуб: включает мероприятия по развитию технологий, CISO-клубы, профессиональные митапы

Конференции для HR и маркетологов в ИБ: внедрение лучших практик по управлению экспертами в ИБ и совершенствованию продуктов

CEO-трансформация

CEO-клуб: управление цифровой трансформацией, диджитализация и безопасность бизнеса

Гастроужин для CEO: глубинные инсайты, меняющие представление о киберзащищённости

Круглые столы с участием CEO про исследования ущерба бизнеса от утечек

Форсайты и сессии для прокачки CEO в ИБ с экспертами индустрии

Образовательный трек

Академия Кибердома: программы повышения киберграмотности для топ- и мидл-менеджмента

Демо-дни для вузов и выпускников школ: разработка образовательной траектории для молодых специалистов

Студенческие питч-кэмпы: помощь бизнесу в воронке эффективных молодых кадров и стажёров

Проверка и оценка защищённости бизнеса

Хакерские соревнования, Bug Bounty и кибериспытания

Партнёрские мероприятия для тестирования продуктов вендоров и информационных систем бизнеса

Аналитическая панель топ-вендоров по инфополю в атаках для бизнеса

Киберграмотность для бизнеса и общества

Telegram-канал Кибердома: экспертный контент о развитии личной и корпоративной цифровой безопасности

Видеоподкаст на YouTube: интервью с экспертами о цифровом мошенничестве, кибербуллинге и на другие актуальные темы

Family Day: интерактивные семейные мероприятия для практического обучения по борьбе с кибермошенничеством

Киберквизы: лекция по киберграмотности и квиз для надёжного закрепления полученных знаний

Путь от цифрового государства к киберустойчивому

Проект АО “Кибериспытание” (КИ) предлагает универсальную систему измерения для любых компаний и организаций, стандартизированный процесс, который описан в методологии Кибериспытания и позволяет компании не просто убедиться в своей защищенности, но и поддерживать её на высоком уровне.

Основные составляющие Кибериспытания

Кибериспытание — это новый инструмент оценки защищенности, включающий в себя все лучшее от уже существующих методов:

1. Концентрация на результатах, а не формальностях. Исследователи ищут не отдельные уязвимости, а полноценные векторы атаки, которые могут привести к критическим последствиям — недопустимым событиям. Результаты Кибериспытания понятны не только специалистам, но и топ-менеджменту, регулятору.

2. Контролируемость и прозрачность. Режим Кибериспытания предполагает фиксацию всех действий исследователей в системе с возможностью на стороне организации остановить их буквально «по нажатию кнопки».

3. Достоверность оценки. «Экзаменаторами» компании будут не отдельные команды или аттестационные центры, а сообщество этичных хакеров страны. Результаты их работы контролируются и оцениваются независимым Экспертным Советом Кибериспытания, куда входят ведущие представители сообщества ИБ.

4. Польза не только для компании, но и для всей отрасли. Как только Кибериспытание набирает критическую массу и становится стандартом по отрасли, в гонку за повышением уровня защищенности включаются все ее игроки, поскольку никто не хочет быть последним.
Эту практику можно экстраполировать сначала на отдельные отрасли, а затем и на весь бизнес в целом.

Кибериспытание — это не защита условного серверного оборудования или информационных систем, это защита людей. Сотрудники, которые привыкли к постоянному стресс-тестированию со стороны этичных хакеров, получают привычки цифровой гигиены.

Кибериспытание в цифрах

АО «Кибериспытание» появилось в 2024 году. За это время было проведено более 100 проектов в разных отраслях.

- Исследователи продемонстрировали реализацию недопустимых событий более чем в 40 компаниях;
- В 40% случаев инициаторами проведения Кибериспытания выступили не специалисты по информационной безопасности, а владельцы бизнеса;
- Для всех участников был составлен индивидуальный план развития результативной кибербезопасности.

При успешном прохождении Кибериспытания организация получает скоринговый балл, который отражает объективный уровень защищенности компании на определенную сумму. Чем выше эта сумма, потенциальная награда для исследователя, тем больший интерес этичные хакеры проявили к компании. Устойчивость к их атакам — доказательство состоятельности компании с точки зрения информационной безопасности.

Этапы проведения Кибериспытания

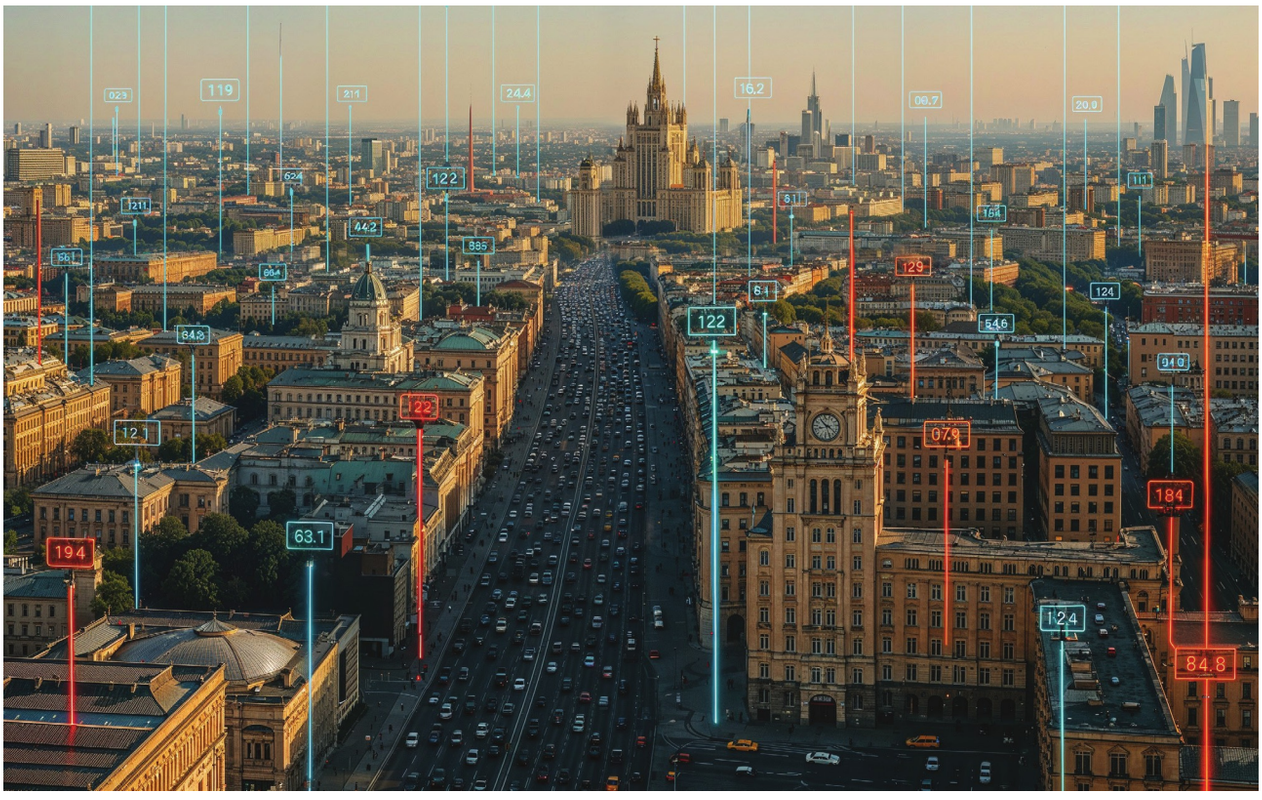
Кибериспытание позволяет не только оценивать защищенность организации, но и создать непрерывный процесс повышенной готовности для всех — от линейных сотрудников и специалистов по кибербезопасности до топ-менеджмента компании.

В зависимости от уровня информационной безопасности и специфики организации Кибериспытание может проводиться в разных форматах, общее описание всех этапов выглядит следующим образом:

1. Подготовительный этап.
Передача рекомендаций по подготовке к КИ, формулирование недопустимого события. Например, демонстрация возможности остановки производства на предприятии.

2. Основной этап.
Привлечение этичных хакеров к проведению Кибериспытания. Фиксация результатов их деятельности и верификация их экспертным советом. Проверка демонстрации реализации недопустимого события и промежуточных отчетов.

3. Заключительный этап.
Подведение результатов Кибериспытания и оценка их состоятельности. Разработка рекомендаций и присвоение оценки (скорингового балла) уровня защищенности организации.



Кибериспытание — концепция, которая неизбежно приведет к росту уровня безопасности сначала в отдельной отрасли, затем в смежных отраслях, а в итоге — выйдет на уровень страны, станет единой мерой и «градусником» кибербезопасности.

В 2024 проект Кибериспытание запустил грантовую программу, в рамках которой компании могли проверить, смогут ли их взломать белые хакеры за 1 млн рублей.

Security Vision

ЕДИНАЯ ПЛАТФОРМА ДЛЯ ВСЕЙ ЭКОСИСТЕМЫ ПРОДУКТОВ

Набор готовых модулей

No-code / low-code инструменты разработки

Встроенный аналитический движок

Полная кастомизация и управление решением

Платформа автоматизации ИБ и ИТ

ОБЪЕКТЫ	карточки и таблицы для описания любых сущностей и их взаимосвязей
ИНТЕГРАЦИИ	коннекторы для двустороннего подключения любых сторонних решений
АНАЛИТИКА	конструктор виджетов и дашбордов для сквозной интерактивной аналитики
РАБОЧИЕ ПРОЦЕССЫ	движок для управления любыми процессами и автоматизации до 95% действий, связанных с задачами ИТ и ИБ специалистов
ОТЧЁТЫ	редактор шаблонов документов и таблиц для выгрузки данных в виде файлов
РОЛИ	управление доступом к данным и персональная витрина для пользователей

Решения для ENTERPRISE и SMB

Помимо классических энтерпрайз решений линейка продуктов Security Vision включает «коробочные» облегченные версии решений, подходящие для небольших организаций и включающие основные функции кроме тех, что необходимы в первую очередь крупным структурам:

VS Basic

SOAR Basic

КИИ Basic

SGRC Basic

Выбор
БОЛЕЕ 100 ЗАКАЗЧИКОВ из различных сфер экономики

АО «ГОЗНАК»

ФГБУ НИИ «ИНТЕГРАЛ»

ФЕДЕРАЛЬНАЯ СЛУЖБА ОХРАНЫ РФ

ПРАВИТЕЛЬСТВО КРАСНОЯРСКОГО КРАЯ

ПРАВИТЕЛЬСТВО ТЮМЕНСКОЙ ОБЛАСТИ

ПРАВИТЕЛЬСТВО ЯРОСЛАВСКОЙ ОБЛАСТИ

СОВЕТ ФЕДЕРАЦИИ ФЕДЕРАЛЬНОГО СОБРАНИЯ РФ

АО «ДОМ.РФ»

АО НПП «ИСТОК ИМ. ШОКИНА»

ПАО «СЕВЕРСТАЛЬ»

ООО «ЕВРАЗ»

АО КОНЦЕРН «РОСЭНЕРГОАТОМ»

АО ОХК «УРАЛХИМ»

ПАО ГМК «НОРИЛЬСКИЙ НИКЕЛЬ»

ПАО «ИНТЕР РАО»

ПАО «РУСГИДРО»

ПАО «СБЕРБАНК»

АО «АЛЬФА-БАНК»

ПАО «РОСБАНК»

АО «Т-БАНК»

АО «БАНК ГПБ»

ПАО БАНК «ФК ОТКРЫТИЕ»

АО «СМП БАНК»

ООО «ИНФОСЕКЬЮРИТИ СЕРВИС»

АО «АБ РОССИЯ»

ООО «X5 GROUP»

ПАО «МАГНИТ»

ГРУППА «ЧЕРКИЗОВО»

ХОЛДИНГ «ЧЕРНОГОЛОВКА»

ООО ГК «РУСАГРО».

АО «ПОЧТА РОССИИ»

ХОЛДИНГ « CAPITAL GROUP »

ГОСКОРПОРАЦИЯ «РОСТЕХ»

АО «ПЕРВЫЙ КАНАЛ»

ПАО «МЕГАФОН»

ПАО «ВЫМПЕЛКОМ»

ООО «СОЛАР СЕКЬЮРИТИ»

ООО «АТ ГРУП»

ООО «ТТК-СВЯЗЬ» (ТРАНСТЕЛЕКОМ)

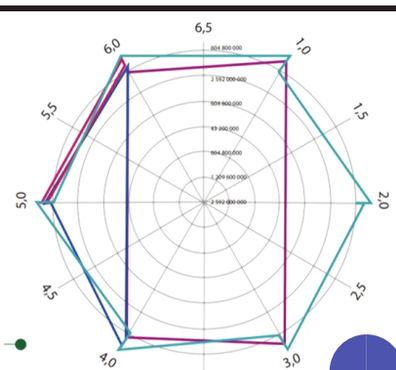
ООО «ИНФОСЕКЬЮРИТИ СЕРВИС»

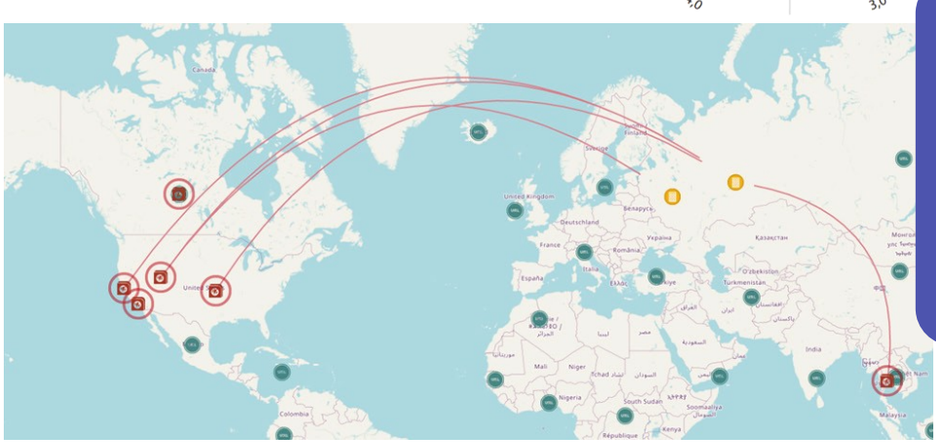
КОММЕРЧЕСКИЙ SOC «РОСТЕХ»

Единый центр мониторинга и управления

Единая модель данных с учетом бизнес-сущностей

ИИ-инструменты и конструкторы для полной управляемости





SECURITY VISION

ОТДЕЛЬНЫЕ ПРОДУКТЫ И ГОТОВЫЕ СБОРКИ (КОМПЛЕКТЫ)

NG SOAR

Комплект расширенного управления инцидентами с ИИ (встроенные помощники и интеграция со сторонними LLM-моделями) для максимальной автоматизации реагирования на всех этапах обработки инцидентов и атак с динамически-формируемыми сценариями и объектно-ориентированным подходом.

Комплект включает SIEM решение, единую ресурсно-сервисную модель, модуль управления активами и инвентаризацией (AM/CMDB), а также двусторонние интеграции с центрами мониторинга и реагирования (CERT) для автоматизированного получения данных, задач и оперативного оповещения об инцидентах

NG VM

Комплексное решение для поиска и устранения уязвимостей, включающее модули управления активами и настройками безопасности технологических платформ (комплаенс конфигураций и харденинг), а также сканер безопасности, осуществляющий поиск технических уязвимостей объектов инфраструктуры, программ и ОС, контейнеров и веб-приложений с автоматическим созданием и назначением задач, патчингом и закрытием заявок при успешных повторных сканированиях

NG SGRC

Комплекс риск-ориентированного центра управления стратегической безопасностью, включающий аудит и комплаенс соответствия НМД для ИТ- и ОТ-сегментов компаний разного масштаба и сфер деятельности на основе стандартов из пакета экспертизы и/или реализации собственной методики. Комплект поддерживает количественную и качественную оценку рисков с расчетом вероятностей и ущерба сценариев реализации рисков, выработкой и внедрением мер защиты для повышения киберустойчивости организации и процессы обеспечения непрерывности бизнеса и самооценки уровня защищенности

О компании

30+ из ТОП100 компаний России являются заказчиками

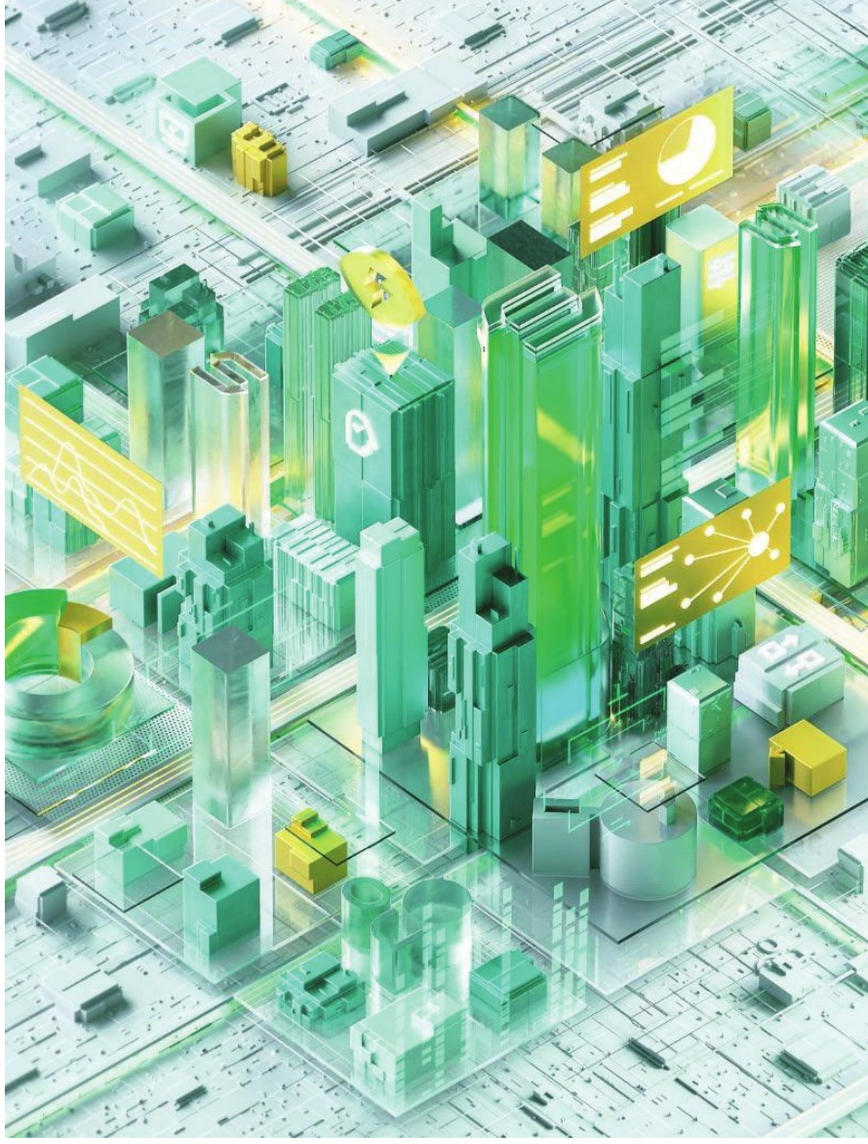
7 из ТОП10 банков являются заказчиками

10+ MSSP провайдеров ИБ ИБ-услуг используют платформу для оказания сервиса

30+ компетентных и обученных компаний компаний-партнеров

26 профессиональных наград в области ИБ

Имеет все необходимые для работы разрешительные лицензии ФСТЭК и ФСБ



О платформе

Платформа автоматизации и роботизации процессов обеспечения информационной безопасности Security VisionVision– ИТ -платформа low code /no code , позволяющая роботизировать до 95% программно программно-технических ИТ/ИБ функций в круглосуточном режиме

Является 100% российской разработкой, включена в базу данных Минкомсвязи РФ и в Единый реестр российского ПО для ЭВМ и БД

Выполнена на уровне мировых аналогов, получила широкое признание экспертного сообщества

Среди заказчиков - Сбербанк, Альфа Альфа-Банк, Евраз , Черкизово, ФСО России, Тинькофф банк, Газпромбанк, Северсталь, МКБ, Норникель , Совет Федерации, Гознак, Почта России, Магнит и многие другие государственные органы и коммерческие структуры

Обладатель 26-ти профессиональных наград, в том числе:
«За укрепление безопасности России»,
«Импортозамещение »,
Национальная премия «Приоритет»,
TAdviser IT Prize в номинации «ИБ-решение года в России»,
Премия Рунета в номинации «Информационная безопасность»

Платформа развивается в трех направлениях:

- Технологии
- Процессы
- Люди

SOAR

Реагирование на инциденты информационной безопасности при помощи динамических плейбуков с применением СЗИ, выстраиванием цепочки атак и объектно-ориентированным подходом к ликвидации инцидентов и устранению последствий.

FinCert

Двустороннее взаимодействие с центрами Центрального банка: управление задачами, передача информации об инцидентах и получение оперативных уведомлений/бюллетеней по установленным регламентам регулятора.

SOT, Security Orchestration

ГосСОПКА

Двустороннее взаимодействие с центрами реагирования НКЦКИ: управление задачами, передача информации об инцидентах и получение оперативных уведомлений/бюллетеней по установленным регламентам регулятора.

AM

Описание ИТ-ландшафта, обнаружение новых объектов в сети, категорирование активов, инвентаризация и управление жизненным циклом оборудования и ПО на АРМ и серверах организаций.

VM

Выстраивание процесса обнаружения и устранения технических уязвимостей, сбор информации с имеющихся сканеров защищённости, платформа управления обновлениями, экспертных внешних сервисов и других решений.

VS

Сканирование информационных активов с обогащением из внешних сервисов анализа защищённости инфраструктуры, использование комплекса значений для управления уязвимостями.

SPC

Оценка конфигураций информационных активов в соответствии с принятыми в организации стандартами безопасности для выстраивания взаимодействий с профильными технологическими платформами и приведения параметров к эталонным значениям.

КИИ

Аудит и исполнение требований ФЗ-187 «О безопасности критической информационной инфраструктуры Российской Федерации» и других нормативных документов, включая процессы категорирования и управления задачами для соответствия.

Security Vision

GRC, Security Orchestration Tools

СМ

Аудит соответствия и комплаенс различным методологиям и стандартам, как включённым в модуль экспертизы (приказы ФСТЭК 17, 21, 31, 239, ГОСТ 57580, PCI DSS, NIST, CIS, ФЗ №152 и №63 и др.), так и других документов заказчиков.

RM

Формирование реестра рисков, угроз, мер защиты, КИР и других параметров контроля, качественная и количественная методики оценки (FAIR, Монте-Карло и др.), формирование перечня мер для изменения уровня риска, контроль исполнения.

BCM

Автоматизация процесса обеспечения непрерывности и восстановления деятельности (ОНиВД) после наступления чрезвычайных ситуаций, включающий в себя BIA и BCP для обеспечения полного цикла.

ORM

Формирование реестра, учёт событий операционного риска (СОР) и других параметров контроля, оценка для соответствия требованиям №716-П ЦБ РФ для формирования перечня мер изменения уровня риска с контролем исполнения задач.

SA

Организация процесса оценки состояния информационной безопасности с выбором методик оценки на основе стандартов из пакета экспертизы или собственных процессов для организации в целом, так и для отдельных её элементов.

SDA, Security Data Analytics

TIP

Анализ угроз кибербезопасности со сбором фидов из любых внешних источников и обнаружением совпадений внутри защищаемого периметра при помощи комбинации технологий и применения ИИ.

UEBA

Поведенческий анализ для поиска аномалий в активности пользователей и устройств с применением различных моделей машинного обучения, корреляционных правил, статистических методов и других управляемых методик.