# XII – 2024

# Кластер информационной безопасности

В рамках XII международной встречи
высоких представителей,
курирующих вопросы безопасности

Информационная безопасность России:
суверенитет, проверенный временем.

Russian Cybersecurity:
Sovereignty Approved by Time

Ciberseguridad de Rusia:
Soberanía Confirmada por el Tiempo

Cybersécurité Russe:
une Souveraineté Confirmée par le Temps

23-25 апреля

Выставочный комплекс
ЭКСПОФОРУМ

Санкт-Петербург

RU

# СОДЕРЖАНИЕ


АНО КОМИБ ..... 3

Ангара ..... 4

ВЭБ.РФ ..... 8

Лаборатория Касперского ..... 10

Код Безопасности ..... 14

Музей криптографии ..... 18

Сайберус ..... 20

Солар ..... 24

Positive Technologies ..... 28

Security vision ..... 34


# АНО КОМИБ



АНО КОМИБ — новый инструмент создания справедливой, надежной и устойчивой системы международной информационной безопасности (МИБ).

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

## АНО 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 АНО 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.

АНО 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 партнерами.

## АНО КОМИБ:

- обладает необходимыми техническими компетенциями;
- владеет необходимой экспертизой в области международных отношений для участия в формировании переговорных 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;
- хорошо представляет текущую ситуацию в российской отрасли ИБ;
- имеет сложившиеся рабочие контакты с коммерческими компаниями для привлечения заинтересованных организаций к работе в контексте достигнутых в формате G2G договоренностей.

Подробнее о нас:




# ANGARA SECURITY

Ведущий российский интегратор и провайдер более 80 услуг по информационной безопасности.

Специализируемся на защите данных и бизнес-систем, предотвращаем и расследуем кибератаки.

- Аккредитовано Минцифры РФ
- Лицензии ФСТЭК и ФСБ России
- Корпоративный центр ГосСОПКА класса «А»

## МОНИТОРИНГ И УПРАВЛЕНИЕ ИНЦИДЕНТАМИ ИБ (SOC)

**Круглосуточное выявление и верификация инцидентов ИБ в инфраструктуре, расследование и реагирование.**

Услуга оказывается с применением консистентного стека программных продуктов из решений класса IRP, SIEM и EDR, которые позволяют выстраивать гибкие процессы управления инцидентами ИБ, автоматизировать рутинные задачи аналитиков, собирать и анализировать исчерпывающий объем телеметрии как от конечных хостов, выходящий за пределы штатных возможностей аудита операционных систем, так и от используемых заказчиком средств защиты информации, а также реагировать на инциденты ИБ.

## РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ ИБ И ЦИФРОВАЯ КРИМИНАЛИСТИКА (DFIRMA)

Услуга включает в себя:

- **реагирование на инциденты** (локализация и сдерживание происходящей компьютерный атаки);
- **анализ вредоносного ПО** (определение используемых злоумышленниками инструментов, выявление IOC, создание yara-правил для сканирования инфраструктуры);
- **расследование инцидентов и цифровую криминалистику** (установление обстоятельств инцидента, сбор цифровых улик, разработка рекомендаций);
- **сопровождение внутренних расследований.**

В рамках услуги возможно проведение **анализа инфраструктуры на компрометацию** (Compromise assessment). Установление наличия или отсутствия фактов компрометации инфраструктуры путем ретроспективного поиска соответствующих индикаторов, а также иных следов.

## ЗАЩИТА БРЕНДА И OSINT

Отслеживание фактов распространения конфиденциальной информации, обнаружение кибersквотинга и фишинговых ресурсов, которые используют фирменный стиль и товарные знаки организации в мошеннических целях (имперсонация) и т.д.

Актуально в том числе при работе с внешними ИТ- и ИБ-подрядчиками: когда есть риск, что ключи, пароли, токены и другие секреты попадут в открытые репозитории подрядчиков или будут опубликованы фрагменты исходного кода внедряемых решений.

Услуга OSINT и защита бренда включает в себя поиск и анализ информации, размещенной как в индексируемых, так и в неиндексируемых сегментах сети Интернет.

## ВНУТРЕННЕЕ И ВНЕШНЕЕ ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ

Проверить, насколько ИТ-инфраструктура и процессы ИБ готовы к возможным взломам, можно путем контролируемого моделирования действий потенциальных злоумышленников. В процессе выявляем слабые места и потенциальные векторы атак.

Помимо экспертно-аналитических действий, применяются также коммерческие решения, зарекомендовавшие себя на рынке, и собственные инструменты группы компаний Angara. Уровень экспертизы специалистов подтверждает I место на Национальном киберполигоне.

## АНАЛИЗ МОБИЛЬНЫХ И ВЕБ-ПРИЛОЖЕНИЙ

Оценка защищенности приложения как отдельной информационной системы позволяет получить более полное понимание качества кода и настроек компонентов. Работы проводятся с учетом общепринятых практик и рекомендаций OWASP и SANS/CWE. Проверяются не только технические аспекты, но и бизнес-логика приложений, а также возможность проведения атак на клиентов приложений. Результат работ — список реально существующих проблемных мест и подробные инструкции по их исправлению.

## ВЫЯВЛЕНИЕ НЕСТОЙКИХ ПАРОЛЕЙ

Использование пользователями слабых или простых паролей — один из главных факторов взлома и подбора учетных записей. Мы предлагаем комплекс действий, нацеленный на проверку стойкости паролей к корпоративным информационным системам. В результате 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

Осведомленность пользователей об атаках с применением социальной инженерии может сыграть ключевую роль в процессах информационной безопасности всей компании. В рамках услуги выполняется комплекс действий, цель которых — проверить осведомленность сотрудников об атаках с применением методов социальной инженерии. Разрабатываются различные сценарии и легенды, эксплуатирующие человеческие слабости: любопытство, страх, жажда наживы и т.п.

## ANGARA ASM
## СЕРВИС УПРАВЛЕНИЯ ПЛОЩАДЬЮ ВНЕШНИХ АТАК

Сервис покажет имеющиеся уязвимости внешнего периметра с описанием их устранения. Это даст возможность сократить количество применимых векторов атак по отношению к исследуемой инфраструктуре.



Использование Angara ASM позволит обнаружить забытые VPN-сервисы ИТ-специалистов, открытые тестовые среды или среды разработчиков, а главное — увидеть уязвимости, которые влечет тот или иной неучтенный актив.

## RED TEAM OPERATIONS

Одним из способов проверить уровень процессов информационной безопасности в компании с возможностью отследить и предотвратить возможную атаку – привлечение команды пентестеров. Во время работ происходит плотное взаимодействие с командой защиты, чтобы отследить возможные пробелы в правилах корреляции, процессах реагирования на инциденты и недостатки конфигураций средств защиты информации.

## УСЛУГИ ПО ОЦЕНКЕ РИСКОВ ИБ

Современная информационная система организации представляет собой распределенную и неоднородную систему. Значительно усложняется задача правильного, эффективного и безопасного управления этой системой. Как следствие, увеличивается количество недостатков, нарушений и уязвимых мест в системе, которые представляют собой определенные риски ИБ для организации. Наши эксперты помогут создать методологическую базу по оценке рисков ИБ и провести такую оценку.

## КОМПЛЕКСНАЯ ЗАЩИТА СИСТЕМ ИНФОРМАТИЗАЦИИ

Создание комплексной системы информационной безопасности предусматривает реализацию совокупности организационных и технических мер для выполнения требований локального законодательства по созданию систем защиты и обеспечению безопасности информации в информационных системах «под ключ» с обследованием, разработкой модели угроз, разработкой ТЗ, проектированием, поставкой и внедрением систем защиты информации.

## АНАЛИЗ ИСХОДНОГО КОДА ПРИЛОЖЕНИЙ

Анализ исходного кода вашего ПО вручную и при помощи статистических анализаторов. Наши эксперты проведут верификацию выявленных подозрений на уязвимости на тестовом стенде, проранжируют подтвержденные уязвимости и сформируют рекомендации по их исправлению. Услуга может проводиться на постоянной основе.

## DevSecOps
## СОЗДАНИЕ КОНВЕЙЕРА БЕЗОПАСНОЙ РАЗРАБОТКИ

Любая разработка приложений требует включения процесса безопасности, чтобы защитить конфиденциальные данные пользователей, предотвратить утечки информации и снизить риски, связанные с кибербезопасностью. Соблюдение требований безопасной разработки положительно влияет на репутацию компании и повышает доверие со стороны клиентов и партнеров.

По итогам анализа ваших бизнес-задач и инфраструктуры предложим решения для обеспечения кибербезопасности и контроля качества кода, а также защиты окружения (контейнерные среды, репозитории).

# ВЭБ.РФ: ПОМОГАЕМ ВЫСОКОТЕХНОЛОГИЧНЫМ КОМПАНИЯМ ВЫХОДИТЬ НА ЗАРУБЕЖНЫЕ РЫНКИ

Способствуем экономическому развитию России и укреплению международных отношений. Налаживаем связи между российскими предприятиями и потенциальными клиентами в 30 странах в СНГ, Европе, Африке, Южной Америке и Юго-Восточной Азии.

## ПОМОГАЕМ:

- **Производителям и экспортерам.** Если у вас есть перспективная технология в сфере кибербезопасности, мы поможем найти потенциальных партнеров.
- **Иностранным покупателям.** Если ищете лучшие практики и надежные технологии, которые можно импортировать из России, поможем наладить отношения с поставщиками и организовать сделку.
- **Зарубежным финансовым институтам.** Если готовы поддерживать обмен передовыми технологиями, поможем с подготовкой и организацией сделок.

## ВСЕСТОРОННЯЯ ПОДДЕРЖКА

| | |
|---|---|
| **Финансовая.** Предлагаем предэкспортное финансирование инвестиционных проектов на территории России и за рубежом. Оказываем поддержку в приобретении активов в других странах. | **Документарная.** Поможем открыть аккредитив — в том числе с постфинансированием. Или получить гарантию: в обеспечении обязательств, для участие в тендере, в форме аккредитива Stand-by или другую. |
| **Представительская.** Участвуем в выставках, семинарах, деловых советах и межправительственных комиссиях. Инициируем развитие нормативно-правовой базы и работаем с деловым сообществом. | **Организационная.** Ищем деловых партнеров для российских предприятий и помогает формулировать перспективные предложения по совместной деятельности. Поможем с оформлением документов и подготовкой сделки. |

## ВКЛАД В ТЕХНОЛОГИЧЕСКИЙ СУВЕРЕНИТЕТ

50 млрд₽ — выделим на программы портфельных инвестиций в высокорисковые технологичные проекты. Первые четыре направления: кибербезопасность, телекоммуникационное оборудование, технологии в нефтесервисе и беспилотные летательные аппараты.

Цель — усилить позиции российских компаний на рынке, который раньше был занят импортными игроками.



Партнер проекта SK Capital станет ключевой площадкой для проектов по созданию технологических холдингов в стратегически важных отраслях. Объединит финансовые возможности, инвестиционную и технологическую экспертизу ВЭБ.РФ и фонда «Сколково».

## ГЛОБАЛЬНОЕ ЛИДЕРСТВО В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ

Вместе с проектом «Сайберус» работаем над национальным продуктом, направленным на защиту от киберугроз. Это инициатива, которая требует вовлечения разных участников индустрии.

Продукт предполагает комплексную систему, применимую в частных, государственных и межгосударственных целях. Включает в себя работу над законодательной базой, подготовку кадров, разработку аппаратного и программного обеспечения, непрерывную проверку защищенности и страхование остаточных кибер рисков.

Приглашаем вместе строить защиту на опережение: сохранить контроль над киберпространством, сделать невозможным наступление неприемлемых событий и оставаться на шаг впереди киберпреступников.

## ВОЗМОЖНОСТИ И ИНФРАСТРУКТУРА

**ВЭБ.РФ – перспективный и надежный партнер. Вот почему:**

| | | |
|---|---|---|
| **Суверенный рейтинг.** Международные кредитные рейтинги соответствуют рейтингам Российской Федерации | **Работаем на разных рынках.** В том числе — на рынках с высоким уровнем риска. | **Ведем сложные проекты.** Поможем организовать крупную и долгосрочную сделку со сложной структурой. |
| **Широкая сеть партнеров.** Взаимодействуем с большим количеством иностранных финансовых институтов. | **Сопровождаем на всех этапах.** Поможем с поиском партнеров, подготовкой и финансированием сделки. | |

## ПОДДЕРЖКА РОССИЙСКОГО ЭКСПОРТА

ВЭБ.РФ — лидер в сфере экспортного кредитования и ключевой элемент поддержки экспорта для ряда отраслей экономики.

Предлагаем условия, которые позволяют обеспечить конкурентоспособность отечественной продукции на зарубежных рынках.

| | |
|---|---|
| 300 инвестиционных проектов | 3,4 трлн ₽ инвестиций |

«У нас простая и понятная миссия — мы строим безопасный мир. Используя свой опыт и достижения, мы хотим сделать цифровое пространство защищенным — чтобы каждый мог наслаждаться теми безграничными возможностями, которые ему способны предложить технологии».

Евгений Касперский,
генеральный директор «Лаборатории Касперского»



kaspersky



## СТРОИМ БЕЗОПАСНЫЙ МИР УЖЕ БОЛЕЕ 25 ЛЕТ

«Лаборатория Касперского» — международная компания, работающая в сфере информационной безопасности и цифровой приватности более 25 лет. За это время мы прошли путь от производителя антивирусов для частных и корпоративных пользователей до поставщика всесторонней киберзащиты бизнеса разного размера и сферы деятельности.

Защищаем организации всех отраслей

Нефтегаз и ТЭК · Финансы · Транспорт · Телеком · Производство · ИКТ · Розница · Госорганы

Сегодня организациям необходима поддержка надежного партнера по кибербезопасности, обладающего многолетним опытом, глобальной экспертизой и пониманием современных кибервызовов как в корпоративном, так и в промышленном пространствах, а также на их пересечении.

**>220 тыс**
пользователей по всему миру защищены нашими технологиями

**>400 млн**
корпоративных клиентов по всему миру

**~5000**
высококвалифицированных специалистов

**>400 тыс**
уникальных вредоносных объектов мы обнаруживаем ежедневно

**>200**
крупных APT-группировок отслеживается нами

**50%**
наших сотрудников — R&D-специалисты и исследователи

## ЭКСПЕРТНАЯ ЗАЩИТА ДЛЯ ВАШЕГО БИЗНЕСА

Для успешного противостояния комплексным киберугрозам и эффективной адаптации к новым вызовам в условиях постоянно меняющегося ландшафта угроз вам нужны современные технологии, подкрепленные аналитическими данными об угрозах, опытные специалисты, обладающие необходимыми знаниями, и поддержка экспертов мирового уровня. В этом случае в вашем распоряжении будет весь комплекс мер противодействия самым сложным APT-угрозам и целевым атакам. «Лаборатория Касперского» предлагает полный арсенал расширенных защитных технологий, аналитики и сервисов, которые повысят эффективность вашего ИБ-отдела и команды SOC.

Обширное портфолио «Лаборатории Касперского» включает в себя передовые технологии для защиты IT- и OT-сегментов, ряд специализированных продуктов и широкий спектр экспертных сервисов, а также кибериммунные решения для борьбы со сложными и постоянно эволюционирующими киберугрозами.

## ЭКОСИСТЕМА НАСТРОЕННЫХ ИНСТРУМЕНТОВ БЕЗОПАСНОСТИ

Сегодня как никогда важен именно экосистемный подход к кибербезопасности бизнеса, который включал бы взаимодополняющие друг друга классы технологий EPP, EDR и XDR и при этом соответствовал бы требованиям регулирующих органов. «Лаборатория Касперского» следует такому подходу, воплощая его в линейке решений Kaspersky Symphony.

Линейка решений Kaspersky Symphony — это комплекс тесно интегрированных технологий и решений, основанных на экспертизе и многолетнем практическом опыте. С ее помощью компании увеличивают эффективность системы безопасности и прозрачность инфраструктуры и готовы успешно отражать атаки любого масштаба и сложности. Кроме того, она помогает обеспечивать соответствие требованиям регулирующих органов. Наиболее полно экосистемный подход воплощен в уровне Kaspersky Symphony XDR. Это решение класса XDR, которое защищает многочисленные точки входа в организацию, в том числе сеть, почту и конечные устройства, от потенциальной угрозы, обогащено знаниями глобальной системы информирования об угрозах, оберегает компанию от ошибок рядовых сотрудников (например, в результате фишинговой атаки) и готово легко встроиться в существующую систему безопасности.

## УНИКАЛЬНЫЕ АНАЛИТИЧЕСКИЕ ДАННЫЕ

Противодействие современным киберугрозам тесно связано с пониманием полной картины тактик, техник и процедур, используемых злоумышленниками. Обладая петабайтами подробных данных об угрозах, «Лаборатория Касперского» предоставляет организациям Kaspersky Threat Intelligence — достоверные аналитические данные об угрозах со всего мира в разных форматах, что помогает обеспечивать защиту даже от ранее неизвестных кибератак.

## ПЕРЕДОВЫЕ ТЕХНОЛОГИИ ЗАЩИТЫ АСУ ТП

Kaspersky Industrial CyberSecurity (KICS) — это специализированная промышленная XDR-платформа, разработанная для комплексной защиты основных компонентов систем автоматизации и управления производством на всех уровнях. Благодаря отличной интеграции компонентов платформы друг с другом вы сможете централизованно контролировать все разрозненные промышленные сети, рабочие места и системы автоматизации. Это способствует повышению осведомленности о ситуации и более эффективному противодействию сложным угрозам.

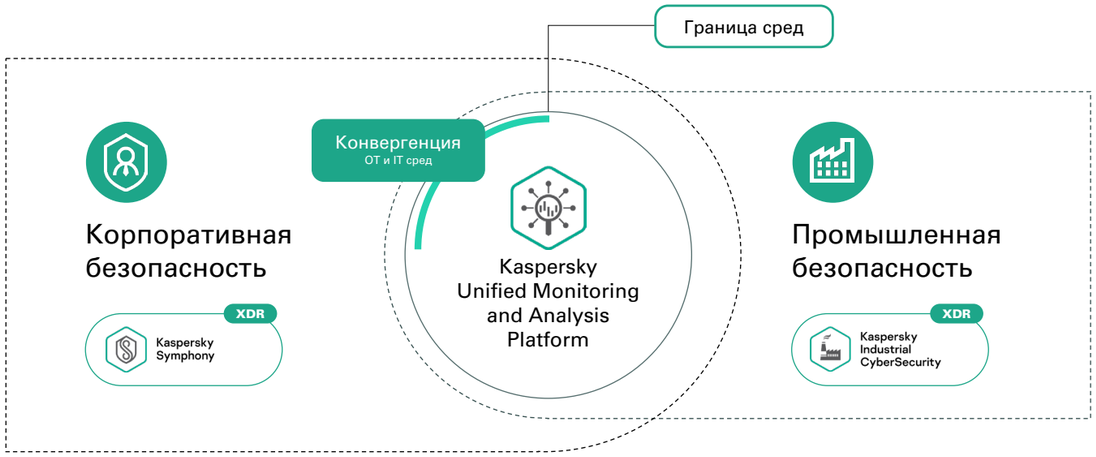


## КОМПЛЕКСНЫЙ ПОДХОД ОТ ГЛОБАЛЬНОГО ПОСТАВЩИКА В ВОПРОСЕ IT/OT-БЕЗОПАСНОСТИ

Одним из ключевых компонентов экосистемы кибербезопасности как промышленного, так и корпоративного сегмента является Kaspersky Unified Monitoring and Analysis Platform — решение класса SIEM, предназначенное для централизованного сбора, анализа и корреляции ИБ-событий из различных источников данных для выявления потенциальных киберинцидентов и своевременной их нейтрализации. Kaspersky Unified Monitoring and Analysis Platform объединяет продукты «Лаборатории Касперского» и сторонних поставщиков в единую систему ИБ, является ключевым компонентом на пути реализации комплексного защитного подхода и помогает комплексно подойти к вопросу соответствия требованиям законодательства в области ИБ.

Благодаря тесной интеграции с SIEM-системой платформа Kaspersky Industrial CyberSecurity позволяет реализовывать больше сценариев взаимодействия с решениями сторонних поставщиков и расширить действия по расследованию и реагированию. Это также позволяет защищать бизнес не только в промышленной среде, но и в той части, где промышленная среда пересекается с корпоративной, тесно взаимодействуя с корпоративной XDR-платформой Kaspersky Symphony XDR.

Цельное предложение для защиты OT и IT сегментов




## СТРАТЕГИЧЕСКИЙ ПАРТНЕР

Выбор партнера в области кибербезопасности — важный шаг для компаний, которые хотят сохранить стабильность и устойчивость в любых условиях. «Лаборатория Касперского» готова стать вашим стратегическим партнером и обеспечить защиту от угроз любой сложности, нацеленных на ваш бизнес.

- Глобальный охват и международное признание
- Доказанная эффективность технологий
- Прозрачность и соответствие стандартам
- Опыт и знания мирового уровня
- Высокий статус в индустрии ИБ
- 25 лет — Более 25 лет безупречной работы

КОД безопасности

«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.

## ЕДИНАЯ АРХИТЕКТУРА БЕЗОПАСНОСТИ:

### ЗАЩИТА РАБОЧИХ СТАНЦИЙ И СЕРВЕРОВ

— Secret Net Studio — комплексное решение для защиты рабочих станций и серверов на уровне данных, приложений, сети, операционной системы и периферийного оборудования.
— Secret Net LSP — средство защиты информации для ОС Linux
— «Соболь» — сертифицированный аппаратно-программный модуль доверенной загрузки (АПМДЗ).

### ЗАЩИТА СЕТЕВОГО ВЗАИМОДЕЙСТВИЯ

— NGFW Континент 4 — Многофункциональный межсетевой экран для защиты сетевой инфраструктуры и создания VPN-сетей с использованием алгоритмов ГОСТ.

### ЗАЩИТА ВИРТУАЛЬНЫХ ИНФРАСТРУКТУР

— vGate — Средство микросегментации и защиты жизненного цикла виртуальных машин.



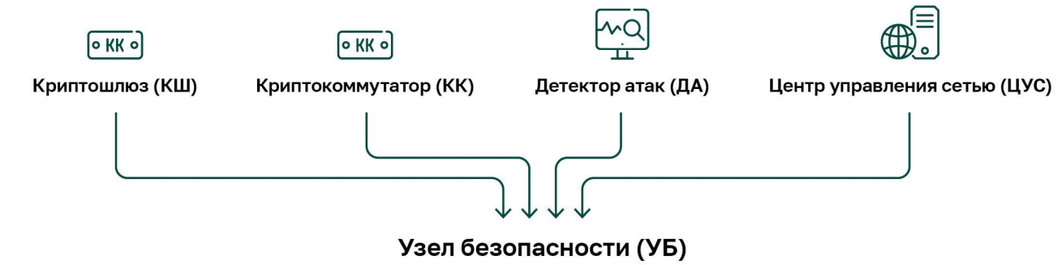
## NGFW КОНТИНЕНТ 4



### ЗАДАЧИ:

- Защита внешнего периметра сети;
- Защита сетей центров обработки данных;
- Защита геораспределенных сетей;
- Защита малых сетей;
- Защита технологических сетей.

### ВОЗМОЖНОСТИ:





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

Antivirus | GeoIP

## SECRET NET STUDIO

### ЗАДАЧИ:

- Защита рабочих станций и серверов от вирусов и вредоносных программ;
- Защита от сетевых атак;
- Защита от подделки и перехвата сетевого трафика внутри локальной сети;
- Защита информации от несанкционированного доступа;
- Защита от действий инсайдеров;
- Защита от кражи информации при утере носителей;
- Контроль утечек и каналов распространения информации.

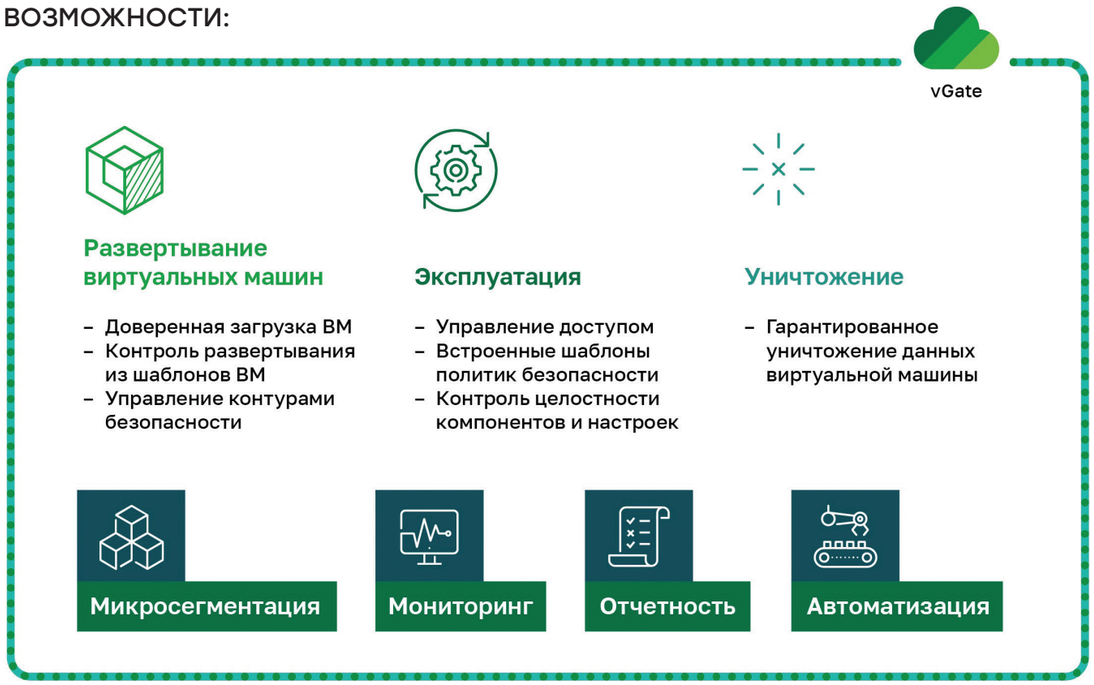
### ВОЗМОЖНОСТИ:


## vGATE

### ЗАДАЧИ:

- Контроль доступа к критичным виртуальным машинам;
- Ограничение действий администратора виртуальной среды;
- Сегментация виртуализованной сети.

### ВОЗМОЖНОСТИ:





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 года.

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 мастер-классы, кинопоказы и конференции, временные выставки и другие события, отвечающие основной миссии музея — просветительству и популяризации науки и технологий.






Сайберус

# «САЙБЕРУС»: СТРОИМ СУВЕРЕННУЮ ИНДУСТРИЮ КИБЕРБЕЗОПАСНОСТИ В СТРАНАХ-ПАРТНЕРАХ

Последние два года мир наблюдает за началом эпохи кибервойн: состояние, когда системообразующие корпорации, государственные учреждения и даже отдельные индустрии подвергаются беспрецедентным кибератакам. В этот период Россия столкнулась с рекордным количеством кибератак – число киберпреступлений в стране быстро растет, угрозы нацелены на критические объекты национальной экономики: промышленность, ВПК, энергетику, финансы, здравоохранение, строительство, сфера услуг и т.д.

Бизнес, целые индустрии и государственные учреждения России не только выстояли под натиском киберугроз, но и приобрели колоссальный опыт отражения даже самых изощренных атак. Полученные знания и методы защиты могут быть востребованы вовне, поэтому в индустрии разрабатывается модель создания и непрерывного развития суверенной кибербезопасности на уровне государства, которую «Сайберус» готов воспроизводить в странах-партнерах России совместно с локальными игроками.

## НОВАЯ МЕЖДУНАРОДНАЯ АРХИТЕКТУРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Изменение в геополитической архитектуре мира неизбежно влечет за собой изменения в других сферах. Для устойчивого развития всей системы важно, чтобы принцип уважения цифрового суверенитета всех государств стал обязательным. Ни одна страна не должна находиться в зависимости от крупных игроков, но у каждой должны быть собственные ресурсы — в первую очередь это люди, готовые создавать новые технологии и самостоятельно обеспечивать и проверять защищенность критически важных для страны областей.

Новые международные проекты в финансах, транспорте, энергетике, промышленности требуют единого подхода к системе информационной безопасности инфраструктуры, который будет учитывать суверенные интересы всех вовлеченных сторон. Поэтому необходимо, чтобы страны могли опираться на собственные решения и технологии, построенные на общих принципах.

| БЕЗОПАСНОСТЬ СЕГОДНЯ | → | БЕЗОПАСНОСТЬ БУДУЩЕГО |
|---|---|---|
| Технологическая архитектура первична, а информационная безопасность выстраивается вокруг созданного решения.<br>Требования к информационной безопасности определяются наличием технологических компонент.<br>Надежность защиты нельзя проверить до начала реальной атаки. | | Технологическая инфраструктура изначально учитывает современные требования информационной безопасности.<br>Требования к информационной архитектуре определяются перечнем недопустимых событий.<br>Надежность защиты проверяется непрерывно кибериспытаниями и оценивается в единой системе измерения результата. |

## МОДЕЛЬ СОЗДАНИЯ И РАЗВИТИЯ ЭФФЕКТИВНОЙ ИНДУСТРИИ КИБЕРБЕЗОПАСНОСТИ НА УРОВНЕ ГОСУДАРСТВА

Модель разработана лучшими экспертами российских ИБ-компаний и предлагает методологию отбора эффективных технологий для построения локальной индустрии кибербезопасности.

## ОЦЕНИВАЕМ ВАШ ТЕКУЩИЙ УРОВЕНЬ ЗАЩИЩЕННОСТИ

Проверим механизмы защиты на возможность нанесения критического ущерба через имитацию хакерской атаки.

Вместе с представителями стран-партнеров мы определяем, что надо защищать и как будем оценивать защищенность в деньгах. Инструментом проверки становится объективное **Кибериспытание** — механизм оценки защищенности ключевых систем государства.

**Кибериспытание**
Непрерывная проверка защищенности критической инфраструктуры от киберугроз. Проводится в реальных условиях силами независимых исследователей под контролем признанных ИБ-экспертов.

## ПОСТРОИМ ЗАЩИТУ, ЕСЛИ ОБНАРУЖИМ УЯЗВИМЫЕ МЕСТА

Эксперты «Сайберуса» помогают определить, какие события критически значимы для страны и разрабатывают стратегию по достижению целевого уровня безопасности.

В соответствии со стратегией формируется единое целеполагание в области ИБ. Под новые задачи выстраивается регуляторная база, которая будет обеспечивать контроль конечного результата. В дальнейшем «Сайберус» помогает выстроить защиту, используя для этого российские технологии, open-source решения и продукты местных ИБ-компаний.

## СОЗДАЕМ ЛОКАЛЬНУЮ ИНДУСТРИЮ КИБЕРБЕЗОПАСНОСТИ

Подход «Сайберуса» позволяет не только строить защиту страны на базе готовых решений, но и создавать локальную ИБ-индустрию, в первую очередь через обучение новых кадров. Увеличив количество и качество специалистов и предоставив пространство, где они могут обмениваться идеями и опытом, получится разработать новые технологии защиты и отдельные подразделения, способные отражать любые кибератаки.

Для создания нового поколения хакеров существует проект **CyberED**: онлайн-платформа по подготовке и повышению квалификации ИБ-специалистов и этичных хакеров — исследователей, которые обладают достаточно экспертизой, чтобы проверять построенные системы реалистичными кибериспытаниями. У компании более 70 программ обучения практикам наступательной кибербезопасности, защите ИТ-инфраструктуры и процессам безопасной разработки ПО, на которых преподают 80 высококвалифицированных экспертов. За 5 лет существования CyberED обучил более 5 тысяч ИБ-специалистов в России и готов предлагать свой опыт и навыки другим странам, чтобы вместе построить национальные киберармий, которые станут основой суверенитета.

Чтобы решать задачу объединения и развития ИБ-индустрии, в России открыли Кибердом. Это пространство позволяет привлекать активных ИБ-специалистов, формировать профессиональное комьюнити и вести диалог между ИБ, IT, государством и бизнесом. Концепция опробирована и готова к экспорту в другие страны.

**Кибердом**
Фиджитал-пространство для привлечения, развития и удержания ИБ-специалистов. Предоставляет инфраструктуру для тренировки навыков и повышения экспертизы.

Результатом этой работы должна стать полностью суверенная защита, когда страна-партнер способна самостоятельно закрывать 100% своих потребностей в ИБ.

## СОВМЕСТНО ЭКСПОРТИРУЕМ РЕШЕНИЯ

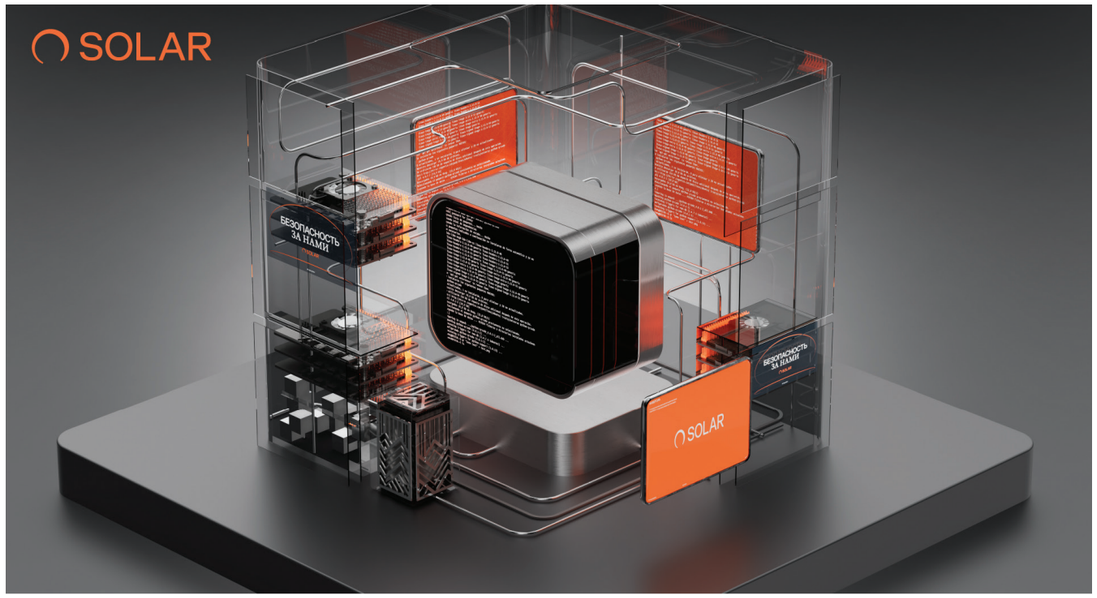
Выверенная и протестированная киберзащита страны-партнера станет востребована для экспорта в другие страны.

Рынок ИБ в странах, которые не находятся в тотальной зависимости от нескольких государств, к 2026 году составит $40 млрд. Объединенные индустрии стран-партнеров и РФ могут претендовать на 20% этого рынка.

**$8 млрд в год**
потенциальный доход от экспорта продуктов и сервисов кибербезопасности

## ИНДУСТРИЯ КИБЕРБЕЗОПАСНОСТИ СТРОИТСЯ ПО МОДЕЛИ G2G

Совместно с государственными учреждениями «Сайберус» ведет переговоры о построении локальной индустрии кибербезопасности в странах-партнерах. Сотрудничество строится по модели G2G, когда для заключения сделок предполагается участие ведущих госкорпораций.




## О КОМПАНИИ

ГК «Солар» — архитектор комплексной кибербезопасности. Ключевые направления деятельности — аутсорсинг ИБ, разработка собственных продуктов, обучение ИБ-специалистов, аналитика и исследование киберинцидентов.

С 2015 года предоставляет ИБ-решения организациям от малого бизнеса до крупнейших предприятий ключевых отраслей. Под защитой «Солара» — более 850 значимых компаний России. Предлагает сервисы крупнейшего в России коммерческого SOC — Solar JSOC, экосистему управляемых сервисов ИБ — Solar MSS. В линейке собственных продуктов — DLP-решение Solar Dozor, шлюз веб-безопасности Solar webProxy, межсетевой экран нового поколения Solar NGFW, IdM-систему Solar inRights, PAM-систему Solar SafeInspect, анализатор кода Solar appScreener и другие. Развивает платформу для практической отработки навыков защиты от киберугроз «Солар Кибермир» и центр исследования киберугроз Solar 4RAYS.

Группа компаний инвестирует в развитие отрасли кибербезопасности и помогает решать проблему кадрового дефицита.

## ЗАЩИЩАЕМ ЦИФРОВОЕ БУДУЩЕЕ

**№1**
на рынке сервисов кибербезопасности

**2000+**
сотрудников

**850+**
организаций под защитой

**24/7**
обеспечение кибербезопасности

**600+**
реализуемых проектов в течение года

**200+ млрд**
анализируемых событий в сутки





## ПРЕДЛОЖЕНИЕ ГК «СОЛАР» ДЛЯ ГОСУДАРСТВЕННЫХ ЗАКАЗЧИКОВ

ГК «Солар», в рамках расширения экономического сотрудничества Российской Федерации с зарубежными странами, готова представить комплексное решение — «Платформу обеспечения кибербезопасности национального уровня».

## «ПЛАТФОРМА» ПРЕДНАЗНАЧЕНА ДЛЯ:

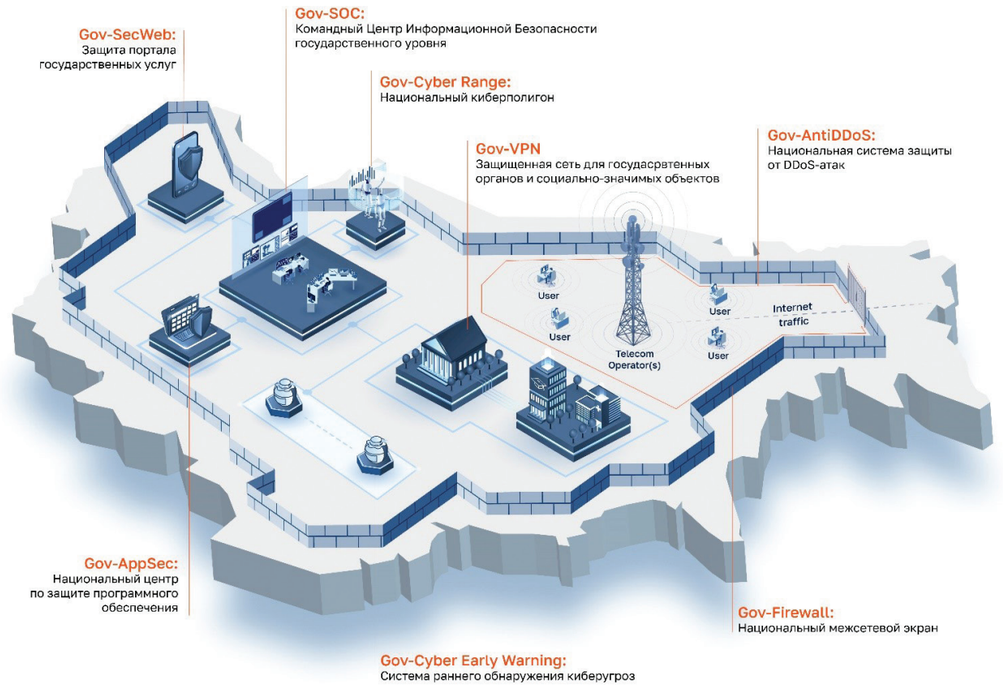
Органов государственной власти, министерств и ведомств

Организаций с критически важной информационной инфраструктурой (финансовый сектор, ТЭК, ВПК)

Социально значимых объектов (образование, здравоохранение и т.п.)

В рамках внедрения «Платформы» ГК «Солар» осуществляет трансфер передовых технологий в области кибербезопасности, создает высокотехнологичную инфраструктуру для ее обеспечения, готовит высококвалифицированных специалистов, в том числе путем разработки и запуска специализированных программ обучения в местных учебных заведениях, а также осуществляет дальнейшую техническую и экспертную поддержку всего комплекса решений.

## «ПЛАТФОРМА» ВКЛЮЧАЕТ В СЕБЯ СЛЕДУЮЩИЕ КОМПОНЕНТЫ:



## GOV-SOC: КОМАНДНЫЙ ЦЕНТР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВЕННОГО УРОВНЯ

Является операционным центром, осуществляющим противодействие киберугрозам любого уровня сложности (исходящих как от одиночных хакеров, так и хакерских групп, поддерживаемых государственными спецслужбами), которые потенциально могут привести к атакам политического, террористического, промышленного и криминального характера.

## GOV-APPSEC: НАЦИОНАЛЬНЫЙ ЦЕНТР ПО ЗАЩИТЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Обеспечивает выполнение взаимосвязанных организационных и технических мероприятий, направленных на разработку и использование безопасного ПО любого типа. Организационные мероприятия включают разработку нормативной базы, определение подходов, методологию и классификацию ПО, составление единого реестра безопасного ПО, а также создание аккредитованных лабораторий, осуществляющих контроль безопасности ПО в масштабах страны. Технические мероприятия подразумевают применение специальных средств автоматической проверки бинарного и исходного кода на наличие уязвимостей, закладок и не декларированных возможностей.

## GOV-FIREWALL: НАЦИОНАЛЬНЫЙ МЕЖСЕТЕВОЙ ЭКРАН

Информационная система мониторинга и управления национальным Интернет трафиком, организуемая в целях борьбы с терроризмом, детской порнографией, незаконным оборотом наркотиков, обеспечивающая реагирование на массовые атаки в сети Интернет, злоупотребления его ресурсами, незаконную деятельность, и позволяющая осуществлять блокировку и снижение (деградацию) скорости доступа к выделенным интернет-ресурсам и мобильным приложениям для предупреждения противоправных действий.

## GOV-VPN: ЗАЩИЩЕННАЯ СЕТЬ ДЛЯ ГОСУДАРСТВЕННЫХ ОРГАНОВ И СОЦИАЛЬНО-ЗНАЧИМЫХ ОБЪЕКТОВ

Виртуальная защищенная сеть (сети), обеспечивающая безопасные и защищенные коммуникации для государственных органов и социально-значимых объектов (например, между образовательными и медицинскими учреждениями), а также предназначенная для предоставления безопасного доступа к информационным системам и к сети Интернет. Кроме того, отдельные узлы Защищенной сети могут быть обеспечены сервисом контентной фильтрации, позволяющим блокировать в автоматическом режиме законодательно запрещенные ресурсы и информацию (например, материалы экстремистского характера, порнографические материалы, информация о наркотиках и их распространении, призывы к суициду и т.п.).



## GOV-SECWEB: КОМПЛЕКСНАЯ СИСТЕМА ЗАЩИТЫ ИНТЕРНЕТ-ПОРТАЛОВ, ПРЕДОСТАВЛЯЮЩИХ ГОСУСЛУГИ НАСЕЛЕНИЮ

Данная система представляет из себя совокупность организационных мероприятий и технических средств, направленных на обеспечение безопасной коммуникации граждан с государственными структурами в сети Интернет. Система защищена от любых попыток взлома портала и несанкционированного получения личных (персональных) данных легитимных пользователей, имеющих доступ к Системе.

## GOV-CYBER EARLY WARNING: СИСТЕМА РАННЕГО ОБНАРУЖЕНИЯ КИБЕРУГРОЗ

Предназначена для выявления ранее неизвестных типов и видов атак на системы информационной безопасности организаций. Система представляет собой размещенные в различных точках страны и объединенные между собой отдельные серверы, группу серверов или виртуальное автоматизированные рабочие места пользователей, к которым намеренно предоставляется относительно простой доступ потенциальных злоумышленников посредством заранее подготовленных для этого «ложных» уязвимостей. В процессе попытки проникновения Система выявляет злоумышленников и позволяет изучить методику и технику их действий по осуществлению атак на информационные системы, а также выявить используемое вредоносное программное обеспечение и оборудование, чтобы отработать и применить к «боевым» системам методы противодействия подобным атакам.

## GOV-CYBER RANGE: НАЦИОНАЛЬНЫЙ КИБЕРПОЛИГОН

Программно-технический комплекс, предназначенный для повышения готовности государства к отражению кибератак и укрепление национальный безопасности, включающий типовые инфраструктуры объектов с критической информационной инфраструктурой, и являющийся площадкой для проведения киберучений любого масштаба для отработки навыков взаимодействия при кибератаках, обучения специалистов актуальным практическим навыкам защиты от кибератак.

## GOV-ANTI-DDOS: НАЦИОНАЛЬНАЯ СИСТЕМА ЗАЩИТЫ ОТ DDOS-АТАК

Комплексная система защиты от атак типа Distributed Denial of Services (далее DDoS) обеспечивает надежную защиту от массированных распределенных атак на критическую инфраструктуру государства на уровнях L3/L4 модели OSI. Развернутая система нейтрализует даже самые сложные и массированные атаки до 7,6 Тбит/с и обеспечивает круглосуточную доступность интернет-ресурсов пользователям.

# positive technologies

Positive Technologies — лидер рынка результативной кибербезопасности. Компания является ведущим разработчиком продуктов, решений и сервисов, позволяющих выявлять и предотвращать кибератаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики. Наши технологии используют более 4000 организаций по всему миру. Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI), у нее более 205 тысяч акционеров.

Более чем за 20 лет работы компания выработала визионерский подход к созданию своих решений. Сегодня технологии и подходы компании кардинально меняют индустрию и повышают защищенность компаний, а через них — отраслей и государств: результативная кибербезопасность становится доступна любой организации в мире.

Опыт компании включает широчайший спектр работ по защите крупных федеральных и мировых событий: Олимпийские игры в Сочи, Универсиады в Казани и Красноярске, Чемпионат мира по футболу, выборы Президента, Игры будущего в Казани 2024 и пр.

При разработке решений Positive Technologies опирается на многолетнюю практику и уникальные знания сотрудников исследовательского центра — одного из крупнейших в мире. В нем работают белые хакеры (white hats), исследующие защищенность различных систем, и эксперты по кибербезопасности, которые расследуют реальные инциденты и знают, как атакуют злоумышленники. На базе продуктовой линейки Positive Technologies сформировано несколько решений, которые аккумулируют опыт по защите бизнеса в различных сферах и специфику российских и международных стандартов безопасности.

К сегодняшнему дню компания имеет наиболее широкий на отечественном рынке спектр технологий защиты, которые в том числе в течение последних двух лет и доказали свою эффективность на практике и стали стандартом де-факто в ряде направлений. Технологии Positive Technologies востребованы и конкурентоспособны на зарубежных рынках и имеют потенциал к тому, чтобы вывести российскую сферу кибербезопасности в число экспортозначимых направлений отечественной экономики.

## МЕТАПРОДУКТЫ

Новый класс решений — метапродукты — ориентирован на результативный подход к кибербезопасности. Первый из них — **MaxPatrol O2** — позволяет автоматически выявлять и предотвращать атаки до того, как будет нанесен неприемлемый для компании ущерб. MaxPatrol O2 заменяет целую команду центра мониторинга кибербезопасности, а чтобы им управлять, достаточно одного человека. Такая система защиты требует от специалистов минимума знаний и усилий. Чтобы продемонстрировать эффективность результативного подхода к ИБ, компания проводит киберучения, в том числе на собственной инфраструктуре, и публично тестирует свои продукты.



## ПРОДУКТОВЫЙ ПОРТФЕЛЬ



Защита периметра
Централизованное управление

### PT NGFW

Первый российский межсетевой экран нового поколения с высоким уровнем производительности, надежности и стабильности. При создании PT NGFW мы учитываем не только экспертизу наших специалистов с опытом работы в ведущих мировых компаниях — производителях сетевого оборудования, но и мнение непосредственных пользователей из числа клиентов и партнеров Positive Technologies.

Показывает, что происходит в сети
Обнаруживает сложные целевые атаки

### PT Network Attack Discovery

Система глубокого анализа сетевого трафика (network traffic analysis, NTA) для выявления атак на периметре и внутри сети. Обеспечивает видимость происходящего в сети, обнаруживает активность злоумышленников, в том числе в зашифрованном трафике, и помогает в расследованиях.

Зашита от целевых и массовых атак

### PT Sandbox

Песочница, позволяющая защитить инфраструктуру компании от целевых и массовых атак с применением вредоносного ПО и эксплуатацией уязвимостей нулевого дня. Проверяет в изолированной виртуальной среде поступающие в компанию файлы и ссылки, выдает вердикт об их вредоносности или легитимности, блокирует угрозы.

Более 400 встроенных правил обнаружения нарушений ИБ
Простота внедрения и масштабирования

### PT ISIM

Система анализа трафика сетей АСУ ТП. Позволяет находить следы нарушений информационной безопасности в технологических сетях, помогает на ранней стадии выявлять кибератаки, активность вредоносного ПО, неавторизованные действия персонала (в том числе злоумышленные) и обеспечивает соответствие требованиям законодательства.

Блокировка атак нулевого дня
Защита от DDoS-атак уровня приложений

### PT Application Firewall

Межсетевой экран уровня веб-приложений. Предназначен для защиты веб-ресурсов организаций от кибератак (DDoS-атак (L7) и атак нулевого дня), а также от угроз из списков OWASP Top 10 и WASC. Визионер магического квадранта Gartner.

Удобная совместная работа

### PT Application Inspector

Инструмент для выявления уязвимостей в приложениях. Принцип работы продукта основан на сочетании статического (SAST), динамического (DAST), интерактивного (IAST) методов и анализа сторонних компонентов (SCA).

Автоматическое подтверждение уязвимостей

Позволяет специалистам по ИБ выявлять и подтверждать уязвимости в исходном коде, а разработчикам — ускорить исправление кода на ранних стадиях разработки.

Настраивается индивидуально под требования заказчика

### PT BlackBox

Сканер безопасности приложений, работающий методом черного ящика. Дает рекомендации по устранению проблем. Упрощает работу специалистов R&D.

Безопасность облаков

### PT Container Security

Высокотехнологичное, инновационное решение для комплексной защиты инфраструктуры гибридного облака. Обеспечивает безопасность разработки программных систем, использующих механизмы контейнерной виртуализации.

Позволяет приоритизировать уязвимости по уровню их опасности для бизнес-процессов

### MaxPatrol VM

Система, позволяющая выстроить процесс управления уязвимостями и контролировать защищенность IT-инфраструктуры компании. Продукт собирает, обновляет и хранит полную информацию об активах, на основе этих данных определяет новые уязвимости на узлах и предоставляет пользователю информацию о них, включая знания о трендовых и наиболее опасных уязвимостях (то есть тех, которые необходимо закрыть в первую очередь).

Для небольших IT-инфраструктур

Доступный старт в мир SIEM

### MaxPatrol SIEM

Система мониторинга событий информационной безопасности. Постоянно пополняется знаниями экспертов о способах детектирования актуальных угроз и адаптируется к изменениям в защищаемой сети. В 2020 году количество продаж MaxPatrol SIEM выросло на 85%. За счет этого компания вошла в тройку мировых вендоров с наибольшим годовым приростом продаж SIEM-решений. Согласно исследованию IDC Global, Positive Technologies — единственный российский вендор в топ-20 мирового рынка SIEM-систем (2021).

Собирает важные данные для проведения расследований

### MaxPatrol EDR

Система защиты устройств компании и сотрудников от сложных и целевых атак. MaxPatrol EDR поможет оперативно выявлять сложные угрозы и целевые атаки, обеспечит уверенное реагирование и автоматизацию рутинных операций с учетом особенностей инфраструктуры и процессов построения ИБ в вашей компании.

Возможность сканирования сети в режиме тестирования

### MaxPatrol 8

Система, используемая для оценки защищенности IT-инфраструктуры. Позволяет определить эффективность процессов ИБ, а также обеспечивает выполнение требований стандартов.



Проверяет на наличие уязвимостей

### XSpider

Сканер уязвимостей, позволяющий оценить уровень защищенности сети компании. Проверяет рабочие станции, серверы, сетевые устройства и веб-приложения. Исследует узлы без применения заранее установленных агентов.

## СЕРВИСНЫЙ ПОРТФЕЛЬ

- **Обнаружение сложных инцидентов, реагирование на них и расследование, а также мониторинг защищенности корпоративных систем** от экспертного центра безопасности Positive Technologies (PT Expert Security Center, PT ESC). Сервисы безопасности на базе продуктов, которые предлагает PT ESC, доказали свою эффективность во время экспертного сопровождения зимней Олимпиады-2014 в Сочи и Чемпионата мира по футболу — 2018, когда специалисты помогли отразить 38 тысяч кибератак на сервисы транспортной дирекции.

- **Непрерывный анализ защищенности бизнеса** помогает непрерывно оценивать уязвимость компании для действий злоумышленников, своевременно предотвращать атаки и устранять их последствия. Спектр услуг включает три направления: Pentest 360, эмуляцию APT и red team vs. blue team.

- **Исследование угроз и уязвимостей аппаратных решений** — услуги экспертной команды Positive Technologies, которые помогут устранить риски ИБ, связанные с уязвимостями аппаратных платформ.

Под эгидой Positive Technologies создана **платформа Standoff 365**, предназначенная для повышения защищенности бизнеса с помощью практических киберучений и исследований систем безопасности. Все решения платформы помогают:

- бизнесу — на практике проверять устойчивость систем к киберугрозам и усиливать навыки своих специалистов по ИБ для повышения качества защиты компании;

- исследователям безопасности — изучать различные инфраструктуры, улучшать свои методы поиска уязвимостей и получать вознаграждения.

К сегодняшнему дню на платформе зарегистрированы более 8 000 активных пользователей. В число продуктов платформы входят:

- **Кибербитва Standoff** — международное офлайн-мероприятие, которое с 2016 года объединяет специалистов по ИБ и исследователей безопасности для проверки и оттачивания своих навыков на примере максимально реалистичной инфраструктуры. В ходе кибербитвы компании проверяют зрелость своей службы информационной безопасности в условиях атак от практикующих пентестеров, а исследователи безопасности — соревнуются между собой в умении выявлять уязвимости в разных системах защиты, чтобы переложить этот опыт на свои компании.

За 8 лет было проведено 12 битв, в которых совокупно приняло участие более 1 500 исследователей безопасности и 100 команд специалистов по ИБ. Кибербитва Standoff является самым масштабным и узнаваемым ивентом в своем сегменте.

- **Онлайн-полигон Standoff** — виртуальная копия IT-систем компаний для проверки навыков исследователей безопасности и специалистов по ИБ. Киберполигон доступен круглый год в режиме 24/7 и позволяет специалистам отделов безопасности компаний на практике тренироваться в выявлении, расследовании и отражении атак, чтобы переносить этот опыт на повседневные задачи, а исследователям безопасности — тестировать гипотезы по реализации недопустимых событий, используя разные векторы атак, и оттачивать свои навыки выявления уязвимостей. Киберполигон включает более 400 виртуальных машин, объединенных в единую инфраструктуру.

- **Bug Bounty Standoff** — платформа для поиска уязвимостей в системах компаний. По правилам программы компания размещает свои приложения или инфраструктуры в публичном или приватном доступе, чтобы проверить их надежность. Компания может перечислить конкретные уязвимости или события, которые нужно реализовать исследователям безопасности для получения вознаграждения. Задача исследователей — выявить уязвимости или реализовать недопустимое событие, после чего подготовить и отправить пошаговый отчет. Компания платит только в случае реализации конкретного события и сдачи отчета, который полностью описывает весь ход атаки. В рамках дополнительной услуги «триаж» компаниям помогают проверить корректность отчета и дают рекомендации по устранению выявленной уязвимости. За 2 года существования программы было сдано более 4 500 отчетов об уязвимостях. На данный момент на платформе представлены 55 программ.

Команда Positive Technologies знает об информационной безопасности многое и с удовольствием делится опытом с другими:

- уже 12 лет проводит собственный научно-практический форум Positive Hack Days — крупнейшее мероприятие в области информационной безопасности в России и СНГ. Компания привлекает к диалогу небезразличных к вопросам кибербезопасности людей со всего мира, в том числе экспертов в области ИТ и ИБ, руководителей бизнеса и представителей государственных структур, белых хакеров. В рамках PHDays проходят сотни выступлений и мастер-классов, а также практические конкурсы по анализу защищенности промышленных систем управления, банковских сервисов, мобильной связи и веб-приложений. В 2023 году форум впервые прошел в формате открытого городского фестиваля по кибербезопасности и объединил экспертов в сфере ИБ, людей, развивающих технологии, жителей и гостей города Москвы;

- аккумулирует самые свежие новости индустрии на портале SecurityLab.ru;

- разрабатывает учебные программы для ведущих вузов страны и помогает растить первоклассных специалистов со студенческой скамьи: материалами, подготовленными экспертами компании в рамках образовательной программы Positive Education, пользуются более 65 вузов России.

# Security Vision

Security Vision — российская компания, разрабатывающая платформу для роботизации до 95% программно-технических функций оператора информационной безопасности. Единая платформа для всех продуктов (включая разработки партнеров) обеспечивает непрерывный анализ, реагирование на угрозы и киберинциденты и надежную защиту информационных активов крупнейших государственных и коммерческих структур, среди которых — Сбербанк, 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.

Security Vision — 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 – 2023 в номинации «Информационная безопасность».

## SECURITY VISION В ЦИФРАХ:

**120+**
профессионалов в команде

**30+%**
из ТОП100 компаний России являются Заказчиками

**7/10**
из списка ТОП10 Банков являются Заказчиками

**14/20**
из списка ТОП20 Банков являются Заказчиками

**1**
собственный ЦОД

**30+**
компетентных и обученных компаний-партнеров

**2010**
год первых исследований в автоматизации

**5+**
MSSP провайдеров ИБ-услуг используют платформу для оказания сервиса

Решения Security Vision развиваются в трех направлениях согласно классическому треугольнику связей:

**1** ТЕХНОЛОГИИ + **2** ПРОЦЕССЫ + **3** ЛЮДИ

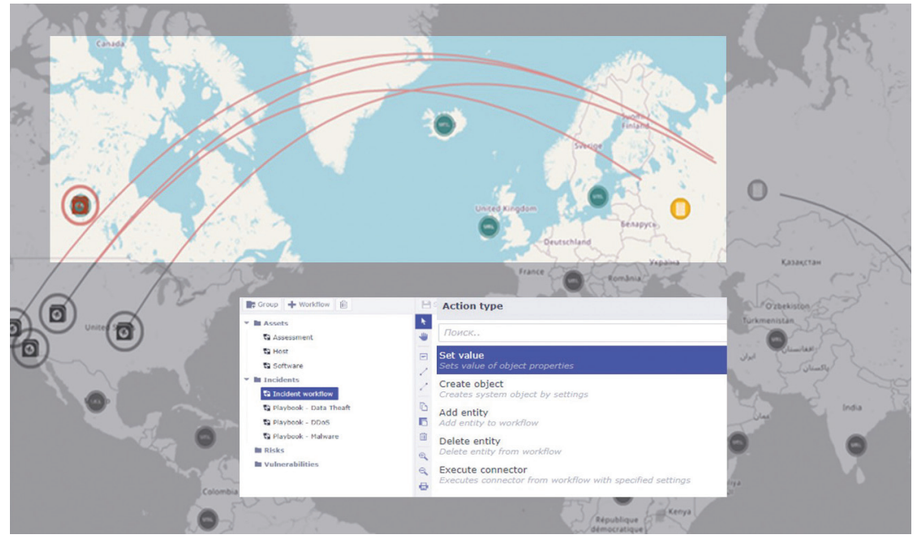
Все решения могут использоваться как самостоятельные продукты или как модули в рамках единой инсталляции при решении комплексных задач. Основные задачи и возможности решений приведены в каталоге ниже.





## 1. SOT – SECURITY ORCHESTRATION TOOLS

Данное направление объединяет продукты для управления практической безопасностью и создания экосистемы разрозненных продуктов с их последующей оркестрацией.




### 1.1 NG SOAR (NEXT GENERATION SECURITY ORCHESTRATION, AUTOMATION AND RESPONSE)

Комплексный продукт в виде набора модулей: **SOAR** (1.3) + **SIEM** (Security Information and Event Management со встроенными baseline правилами корреляции) + **VM** (1.3) + **VS** (Vulnerability Scanner для поиска технических уязвимостей) + **AM** (1.4)

### 1.2 SOAR (SECURITY ORCHESTRATION, AUTOMATION AND RESPONSE)

**Управление инцидентами ИБ** при сборе данных от подключенных средств защиты информации (SIEM, UEBA, AV/EDR, NGFW, WAF, Proxy и др.) и ИТ-систем, а также сбором окрестности инцидентов посредством встроенных механизмов. Реагирование выстроено по методологии NIST с построением цепочки атаки, встроенными классификатором (200+ типов инцидентов) и базой MITRE ATT&K (100+ техник и тактик). Динамические плейбуки с поддержкой объектно-ориентированного реагирования выстраиваются автоматически в зависимости от типа инцидента и окружения (внутренний/внешний хост, учетная запись, адрес электронной почты, URL-адрес, ВПО, процесс, уязвимость). На различных этапах обработки инцидентов встроены рекомендации по реагированию от экспертов и автоматическая настройка SLA.

### 1.3 VM (VULNERABILITY MANAGEMENT)

**Управление уязвимостями** с возможностью подключения внешних сканеров (например, по API для сбора данных и запуска сканирований) загрузки отчетов (например, XML) и встроенной базой CVE (БДУ ФСТЭК, NVD by NIST, бюллетени Microsoft и др. источники). Поддержка внешних аналитических сервисов (VulDB, Vulners,

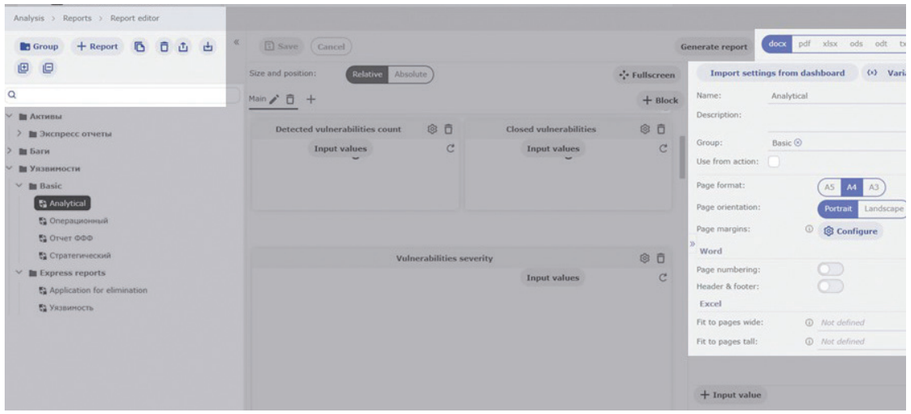
AttackersKB, OpenCVE и др.), дополняющих качество исходных отчетов. Решение автоматически определяет SLA в заявках на устранение по набору различных параметров (например, CVSS и данные ИТ активов) с созданием тикетов как внутри решения, так и в сторонних ITSM/SD системах (Jira, Naumen и др.).

### 1.4 AM (ASSET MANAGEMENT)

**Управление активами и инвентаризацией** с поддержкой регулярного безагентского поиск новых объектов, настраиваемого распределение по категориям без ограничений количества объектов, их типов, сегментов сети, пользователей и ролей для компаний любого масштаба. Инвентаризация может выполняться как автономно (исполнение PS, SSH скриптов) или при помощи сторонних решений, например: AV/EDR, DLP, VM, LPAD, SIEM и др. Решение обеспечивает контроль состава и состояния активов (оборудование, учетные записи, ПО и др.) из единого веб-интерфейса с возможностью запуска скриптов автоматизации в рамках сбора сведений и проведения расследований, в т.ч. активные действия для реагирования.

## 2 GRC – GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE

Данное направление объединяет продукты, предназначенные для решения задач «бумажной» безопасности и управления бизнес-процессами в компании.




### 2.1 CM (COMPLIANCE MANAGEMENT)

**Управление соответствием выбранным нормативно-методическим рекомендациям** (мерам и требованиям ISO, Personal data, etc.) с созданием рабочих процессов, карточек и опросных листов, направляемых всем участникам аудита (с привлечением экспертной группы или без привлечения) для последующей оценки на соответствие. Поддерживает возможности постановки и отслеживания задач по устранению замечаний для подключения исполнителей, а также гибкие редакторы отчетов и дашбордов для формирования отчетности и аналитики в реальном времени.



### 2.2 CERT (COMPUTER EMERGENCY RESPONSE TEAM)

**Взаимодействие с регуляторами** (например FinCERT или ГосСОПКА) с отправкой сведений об инцидентах оператором, которая может осуществляться как в автоматическом, так и в полуавтоматическом режимах по основному (API) или резервному (корпоративная почта) каналам для отказоустойчивости, а также формирование на основании полученной информации (обратный канал) новых задач, заявок или инцидентов — в зависимости от выстроенных внутренних процессов заказчика.

### 2.3 RM (RISKS MANAGEMENT)

**Управление рисками** (кибербезопасности или операционными) с ведением справочника результатов моделирования угроз (объекты воздействия, угрозы ИБ, потенциал нарушителя, меры защиты, способы реализации и др.) согласно собственной или встроенной методологии. Поддерживаются формирование экспертной группы, заполнение опросных листов, оценка вероятности реализации угроз и эффективности мер защиты с привлечением экспертов и владельцев информационных систем по качественной/количественной или комбинированной методике.

### 2.4 BCP (BUSINESS CONTINUITY PLANNING)

**Управление непрерывностью бизнеса** с алгоритмами BIA (Business Impact Analysis) для оценки критичности бизнес-процессов и объектов, BCP (Business Continuity Plan) для планирования требований и приоритетов в случае НШС, регулярными тестированиями планов с оценкой ключевых показателей эффективности согласно различным стандартам (ISO 22301, ГОСТ 22301, Положение ЦБ 787-П, Указание ЦБ 4148-У, ПП РФ N 730). Поддерживает возможности постановки и отслеживания задач по устранению замечаний для подключения исполнителей, а также гибкие редакторы отчетов и дашбордов для формирования отчетности и аналитики в реальном времени.

## 3 SDA – SECURITY DATA ANALYSIS

Данное направление объединяет решения, решающие аналитические задачи для помощи сотрудникам в решении технических задач с применением технологий машинного обучения для обработки big data.

### 3.1 TIP (THREAT INTELLIGENCE PLATFORM)

**Анализ угроз кибербезопасности и проведение киберразведки** с формированием базы на всех уровнях анализа угроз: технический (хэш, IP-адрес, URL, домен, email), тактический (процесс, JARM, ключ реестра), операционный (уязвимости, ВПО) и стратегическом (стратегическая атрибуция данных о злоумышленниках и угрозах). Решение включает 50+ интеграций (с возможностью разрабатывать новые) для получения событий из решений различных классов (SIEM, NGFW, Proxy/Email-сервера и др.), при помощи универсальных форматов (Syslog, CEF, LEEF, EMBLEM, Event log), а также оптимизацию данных для долгосрочного хранения. Для обнаружения и реагирования встроены продвинутые механики в комбинации: DGA-механизмы с использованием машинного обучения, match и retro-поиск по собранным данным обнаруживают совпадение по любым параметрам объектов.

### 3.2 UEBA (USER AND ENTITY BEHAVIOR ANALYSIS)

**Поведенческий анализ** со сбором «сырых» событий от различных источников через интеграции с СЗИ и другими источниками событий ИБ (при сборе события преобразуются в инциденты при накоплении их количества, например, при превышении объемных показателей, и суммарного веса. Поддерживаются белые списки (для исключений) и списки критичных систем (для автоматического создания инцидентов без учета событий и их веса), а также различные технологии анализа: правила корреляции (~30 штук) в комбинации с методами математической статистики (~50 правил) и машинного обучения на основе open-source датасетов (ddos, bot, lateral, malware, suspicious и др.), эмуляции сценариев атак на киберполигоне Security Vision, а также «обучение» системы на трафике клиента (модели «с учителем»).

---

Платформа Security Vision — это база для коробочных и проектных модулей (см. выше), а также low-code / no-code среда для проведения собственной разработки. Для создания контента в платформу вшиты специальные конструкторы, доступные пользователям любого продукта:

- **Конструктор объектов** — карточки и таблицы для отображения разных типов данных, кнопок, чатов, логов и т.д. Например, активы, пользователи, уязвимости, инциденты или заявки на устранение

- **Конструктор рабочих процессов** — для упорядочивания и/или автоматизации разных действий. Например, жизненный цикл актива, процесс принятия заявки в работу или автоматизация назначения SLA

- **Конструктор коннекторов** — интеграции, доступные из коробки и настраиваемые при помощи low-code через интерфейс по разным типам транспорта. Например, взаимодействие по API, проприетарному протоколу, работа с БД напрямую или парсинг файла

- **Конструктор ролевой модели и меню** — для разграничения зон ответственности и кастомизации пунктов меню. Например, руководитель, ИТ-специалист, L1/L2 специалисты ИБ или аналитик рисков

- **Конструктор виджетов и аналитики** — BI для отображения в графиках и интерактивных дашбордах нужных данных. Например, круговой график по типам активов, диаграмма по количеству инцидентов или расположение объектов на карте мира, города или офиса

- **Конструктор отчетов** — редактор для создания шаблонов документов. Например, еженедельная выгрузка в doc экспресс-отчета по активу/инциденту или в xls еженедельного отчета по нужным объектам.

# XII

## Кластер информационной безопасности

В рамках XII международной встречи высоких представителей, курирующих вопросы безопасности

23-25 апреля

Выставочный комплекс ЭКСПОФОРУМ

Санкт-Петербург

expo.komib.ru

2024