ITCOM SECURITY

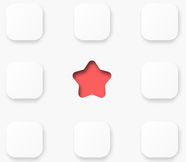
Поможем сохранить отказоустойчивость бизнеса

О компании

ITCOM Security — компания, предлагающая 30+ актуальных решений в области информационной безопасности. С нами вы получите баланс высокой экспертизы и оптимальной стоимости работ. Мы оказываем услуги и поставки как по отдельно взятым решениям, так и готовы реализовать большой комплексный проект.

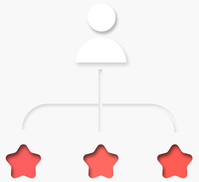
9 лет

Средний профильный стаж работы наших инженеров ИБ



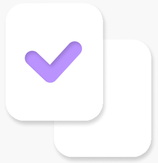
40+ проектов

Разного уровня сложности в среднем реализуем каждые полгода



50+ партнеров

Больше половины из них – разработчики отечественных решений



Наша деятельность лицензирована ФСТЭК и ФСБ

В штате только эксперты с профильной специализацией и высшим образованием в области защиты информации

Наши ведущие эксперты имеют многолетний опыт работы со всеми категориями защищаемой информации

Ключевые партнеры

Услуги и поставки

Оказываем услуги по разработке (построению) системы защиты информации под «ключ»

Защита ИТ-инфраструктуры

- Защита конечных точек (EDR) и антивирусы
- Защита систем виртуализации
- Защита почтовых систем (E-mail Security)
- Управление доступом (IDM, SSO)
- Противодействие целевым атакам (AntiAPT)
- Многофакторная аутентификация (MFA)
- Защита доступа в сеть интернет (SWG)
- Безопасность Zero Trust (ZTNA)

Защита приложений

- Защита Web-приложений (WAF)
- Безопасность мобильных устройств
- Защита баз данных и приложений (DAF, DBF)

Защита от утечек и контроль пользователей

- Защита от утечек информации (DLP)
- Контроль действий привилегированных пользователей (PAM)
- Контроль активности и мониторинг действий пользователей (UAM)

Сетевая безопасность

- Защита каналов связи (VPN)
- Защита от DDoS
- Межсетевые экраны нового поколения (NGFW)
- Обнаружение и защита от вторжений и нетипичных действий (IDS, IPS)

Мониторинг и управление инцидентами ИБ

- Системы мониторинга и реагирования на инциденты ИБ (SIEM)
- Системы реагирования на инциденты информационной безопасности (IRP/SOAR)
- Расследование инцидентов ИБ
- Построение SOC

Обучение и повышение квалификации

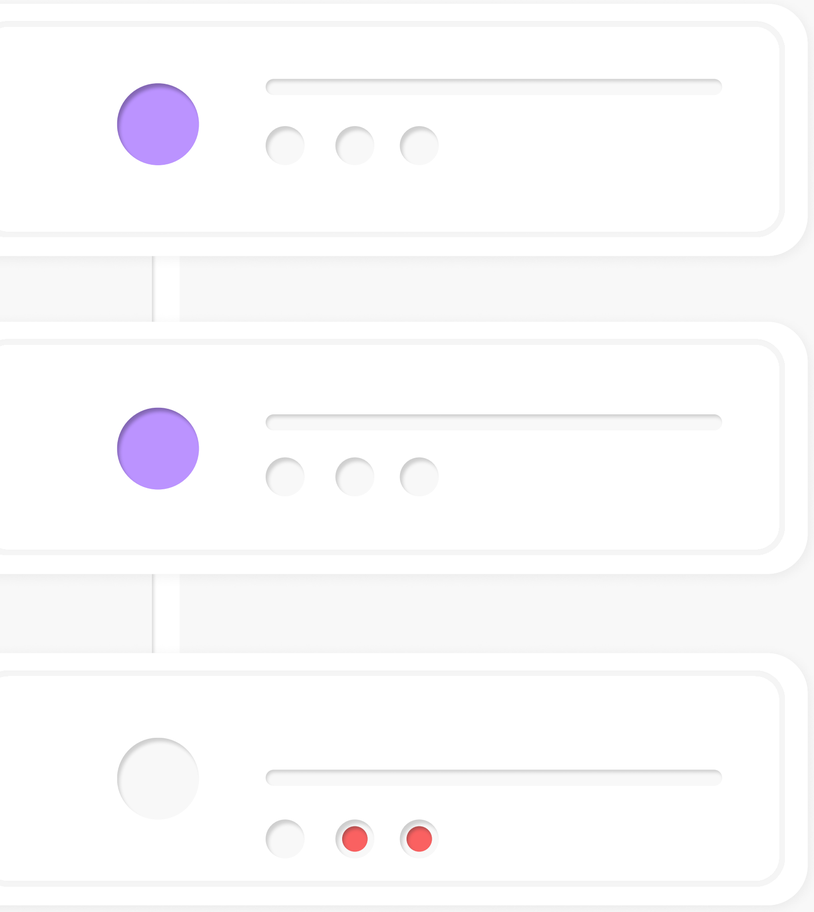
- Лицензированные курсы ИБ
- Сертифицированные вендорские курсы ИБ
- Авторские курсы ИБ

Консалтинг ИБ и аудит

- Анализ защищенности ИС
- Тестирование на проникновение
- Аудит для НФО (757-П)
- Аудит для КФО (683-П)
- Защита от НСД
- Сопровождение ОКЗИ
- Соответствие ПДн (152-ФЗ)
- Помощь в получении лицензии ФСТЭК
- Аттестация АРМ
- Аутсорсинг ИБ
- Системы обучения пользователей (Security Awareness)

Проектирование и ввод в эксплуатацию системы защиты конфиденциальной информации АСУ ТП и объектов КИИ

- Обеспечение защиты информации при эксплуатации АСУ ТП
- Обеспечение безопасности объектов КИИ



Защита ИТ-инфраструктуры

Защита конечных точек (EDR) и антивирусы

Защита систем виртуализации

Защита почтовых систем (E-mail Security)

Управление доступом (IDM, SSO)

Противодействие целевым атакам (AntiAPT)

Многофакторная аутентификация (MFA)

Защита доступа в сеть интернет (SWG)

Безопасность Zero Trust (ZTNA)

Защита конечных точек (EDR) и антивирусы

Большое количество конечных устройств (ПК, ноутбуки, планшеты и т. д.) подвержены атакам через бреши и уязвимости. Большинство устройств применяется пользователями с не очень высокой квалификацией.

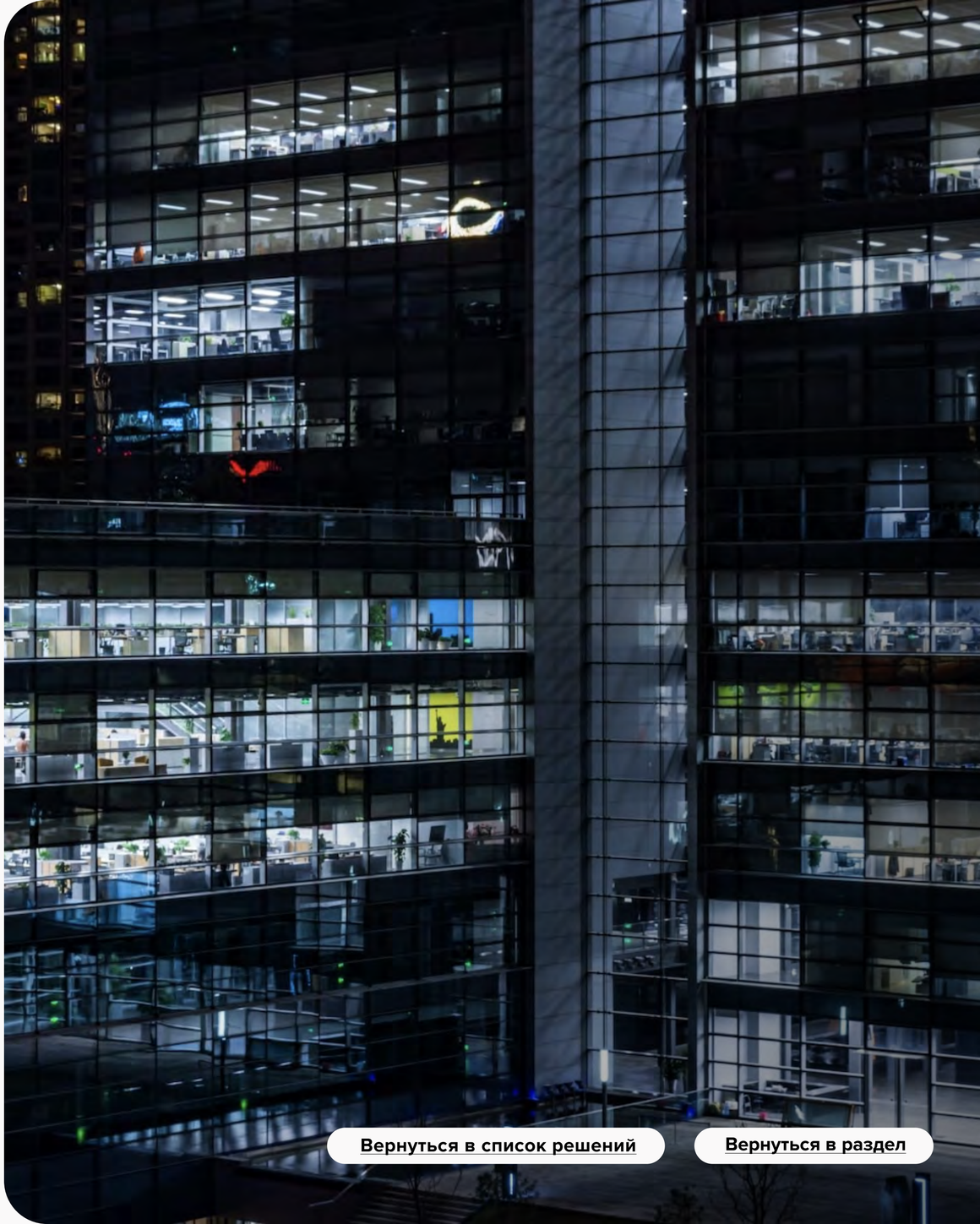
Да и «зоопарк» установленного ПО, обилие каналов связи и портов делают конечные точки самым уязвимым местом ИТ-инфраструктуры.

Мы предлагаем:

Комплексное решение, которое избавит вас от большого количества независимых агентов (IPS-систем, антивирусов, средств управления патчами и обновлениями, систем шифрования и т.д.), благодаря которому снижается нагрузка на административные и вычислительные системы.

Могут быть полезны:

- Защита от НСД
- Security Awareness



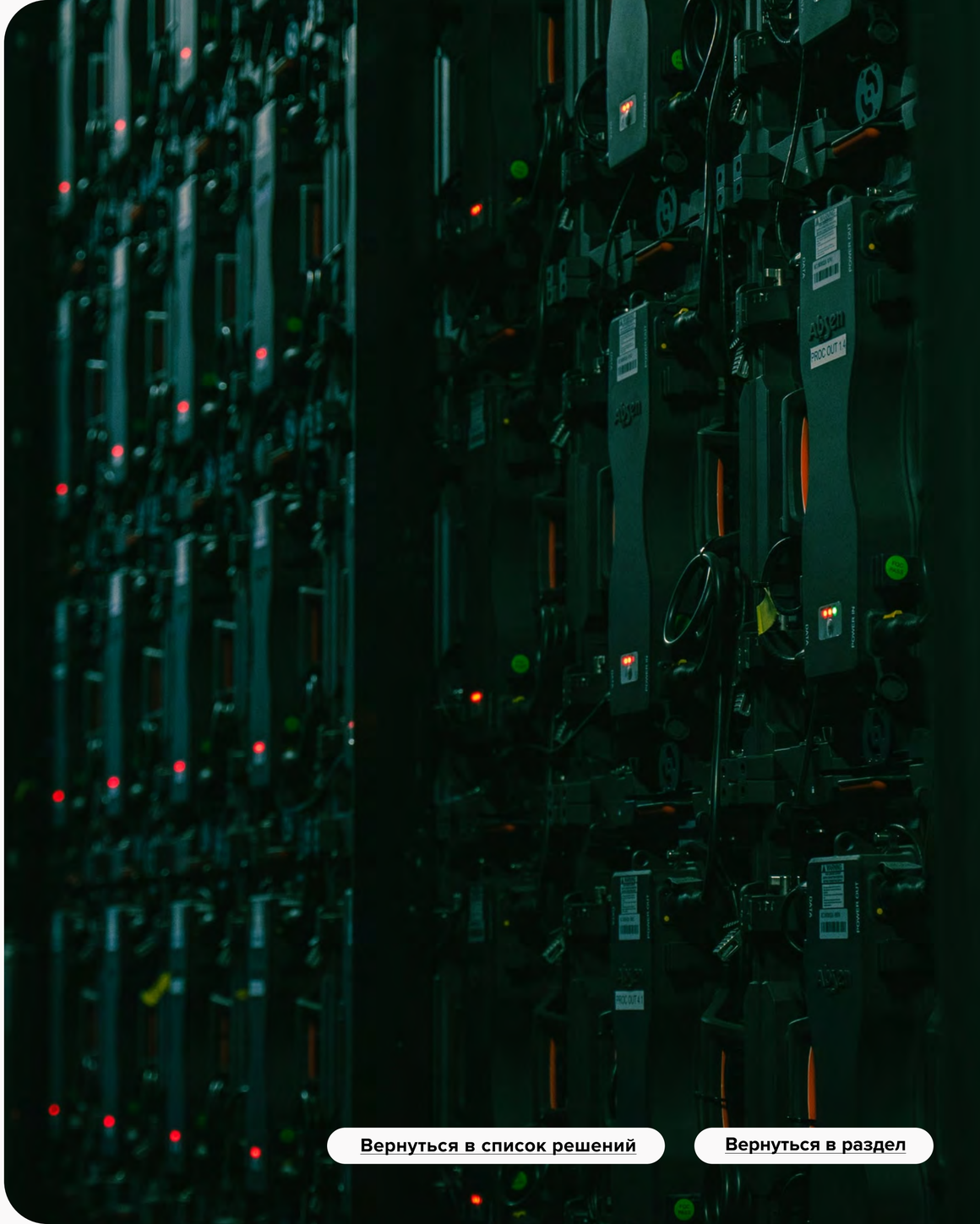
Вернуться в список решений
Вернуться в раздел

Защита систем виртуализации

Виртуальная среда представляет собой динамическую и сложную инфраструктуру, контроль которой – объемная и сложная задача, ведь классические средства защиты виртуализации не сильно эффективны. Это связано как со спецификой новых угроз, так и с отсутствием в ряде случаев совместимости (ведь классические средства ИБ заточены под физические ресурсы).

Мы предлагаем:

Быстрое развертывание комплексных многокомпонентных продуктов для защиты средств виртуализации с функционалом выявления несанкционированной активности, расширенным мониторингом и управлением конфигурациями.



Могут быть полезны:

- NGFW
- Защита от DDoS

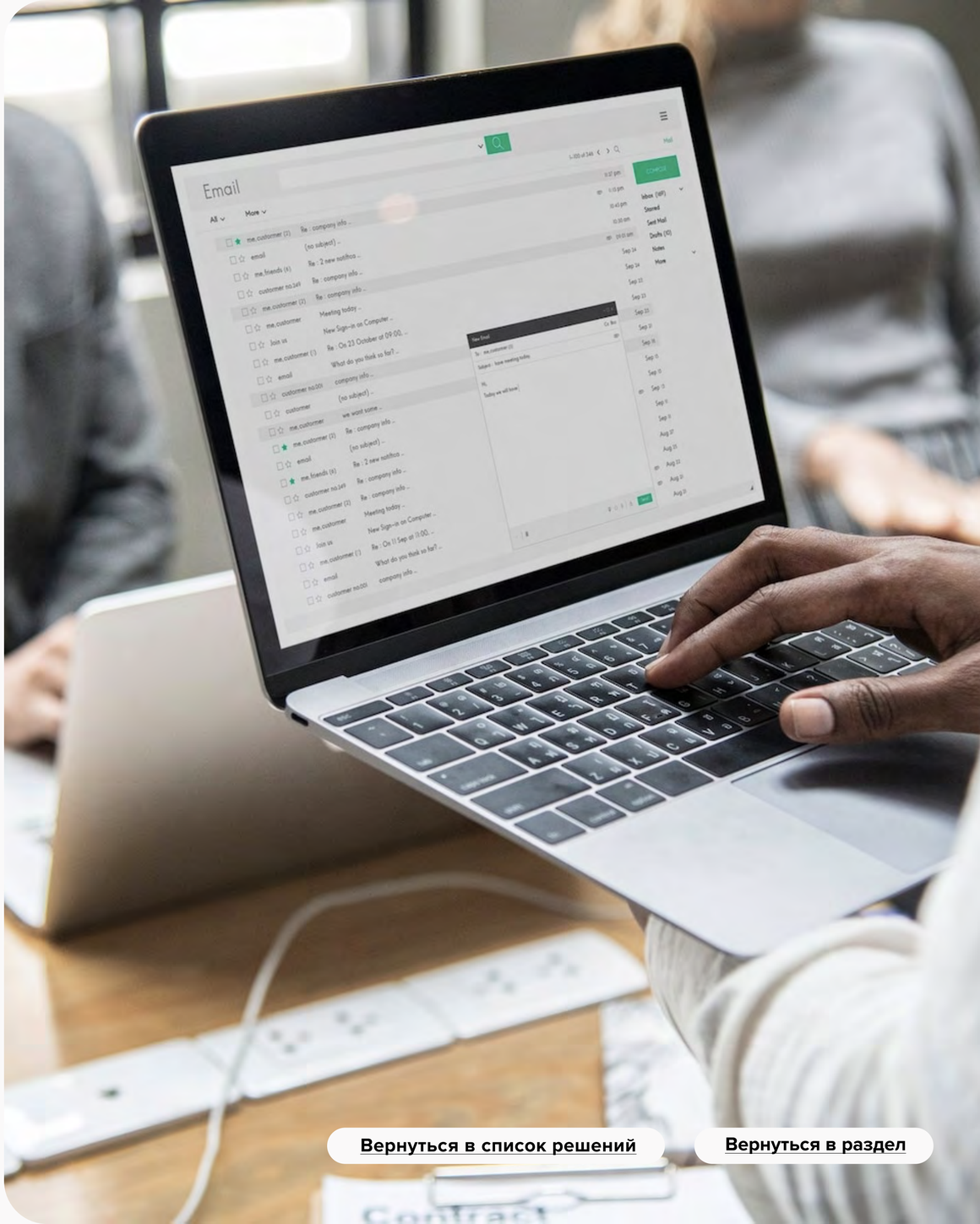
Вернуться в список решений
Вернуться в раздел

Защита почтовых систем (E-mail Security)

С каждым годом растет количество целевых атак и подозрительных сообщений, при которых классические AntiSpam решения «слабы». Это может нанести серьезный ущерб. А государственным или финансовым организациям необходимо соответствовать требованиям законодательства (187-ФЗ, ПП РФ №1236, ГОСТ Р 57580.1-2017 и др.)

Мы предлагаем:

Оптимальный вариант защиты корпоративной электронной почты, исходя из потребностей бизнеса и ИБ. Внедрим решение, предоставим техническое сопровождение и обучим ваших сотрудников.



Могут быть полезны:

- Защита web-приложений
- Защита БД и приложений

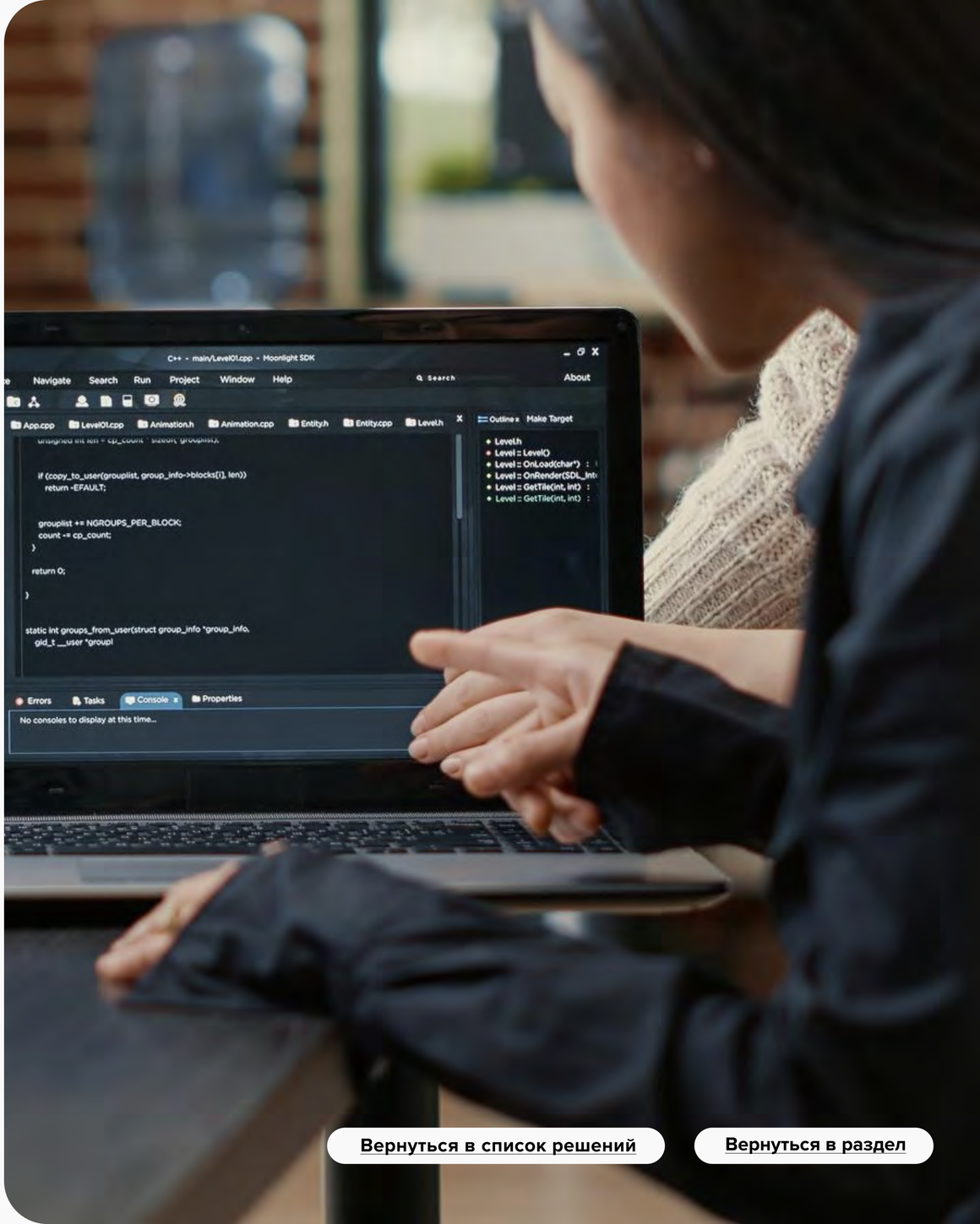
Вернуться в список решений
Вернуться в раздел

Управление доступом (IDM, SSO)

Неправомерный доступ сотрудников к информационным системам либо компрометация данных чреваты искажением и потерями важных данных, которые могут перерасти в потери финансовые и репутационные.

Мы предлагаем:

Внедрение централизованной системы управления идентификационными данными и правами доступа в информационные системы. Простой и понятный инструмент для контроля соблюдения политик безопасности, а Single Sign-On поможет отказаться от хранения пользовательских паролей и исключить компрометацию учетных данных сотрудников.



Могут быть полезны:

- Защита от утечек
- Контроль действий привилегированных пользователей

Вернуться в список решений
Вернуться в раздел

Противодействие целевым атакам (AntiAPT)

Целевые атаки становятся все быстрее и изощренней. Для их обнаружения и дальнейшего отражения нужен широкий набор различных средств защиты. Однако рынок информационной безопасности уже предлагает и комплексные решения.

Мы предлагаем:

Комплексное решение по обеспечению защиты ИТ-инфраструктуры от направленных и Zero-day атак для быстрого обнаружения присутствия злоумышленника в сети и воссоздания полной картины атаки для детального расследования (в т. ч. с применением систем глубокого анализа сетевого трафика и песочниц).

Могут быть полезны:

- Системы мониторинга SIEM
- Системы реагирования на инциденты ИБ

Вернуться в список решений
Вернуться в раздел

Многофакторная аутентификация (MFA)

Данный компонент управления доступом требует от пользователей подтверждения своей личности с использованием как минимум двух различных факторов проверки, прежде чем тот получит доступ к информационным системам компании. Если скомпрометирован один фактор – у злоумышленника есть как минимум еще один более сложный барьер, который нужно преодолеть, прежде чем он сможет получить доступ к учетной записи цели.

Мы предлагаем:

Современную реализацию методов MFA для защиты против изощренных атак в замен устаревшей однофакторной аутентификации по имени пользователя и паролю, которая может быть легко взломана злоумышленником с помощью широко доступных хакерских инструментов.

Могут быть полезны:

- Контроль активности и мониторинг действий пользователей (UAM)

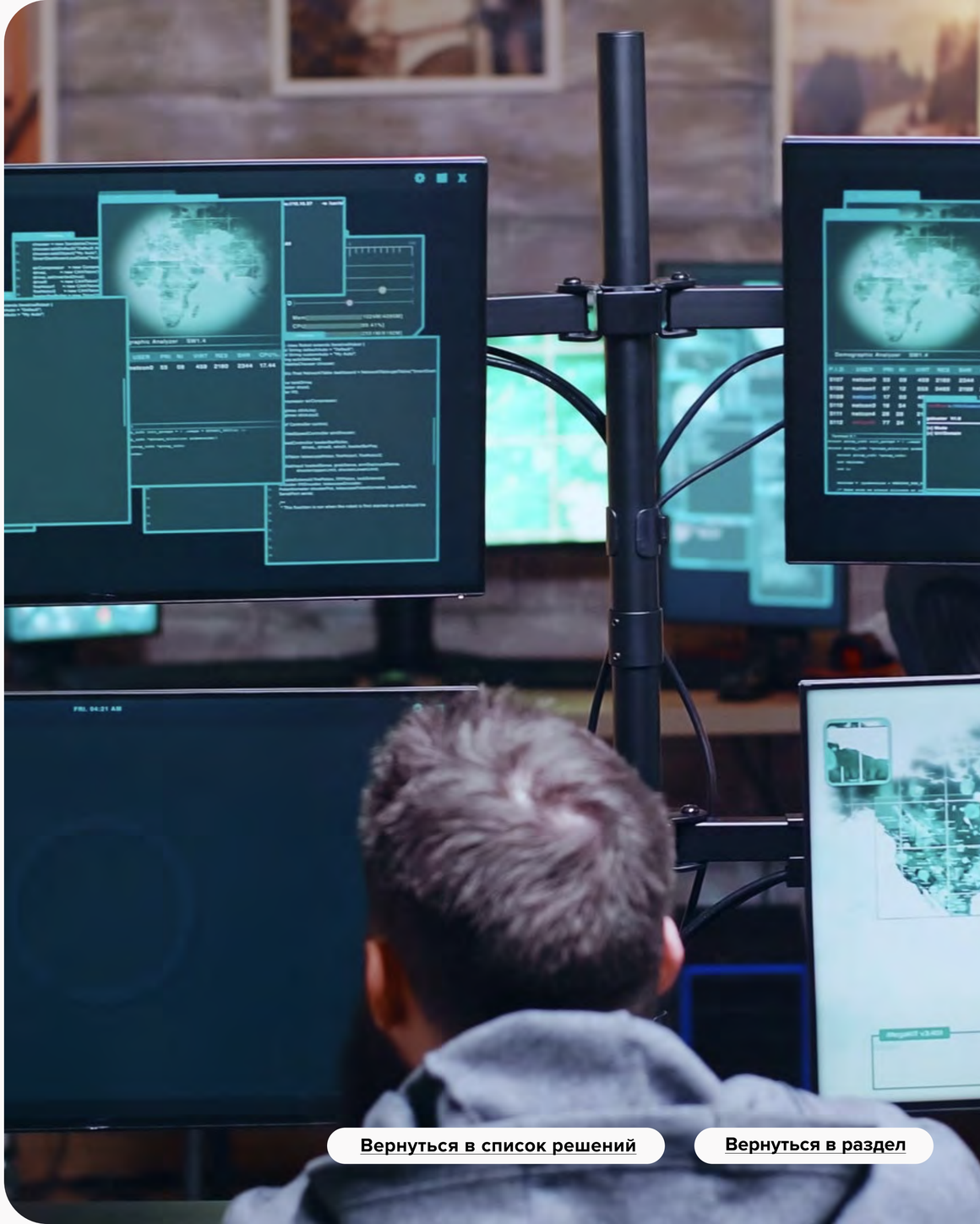
Вернуться в список решений
Вернуться в раздел

Защита доступа в сеть интернет (SWG)

Бесконтрольный доступ сотрудников и приложений
к веб-ресурсам и отсутсвие защиты веб-трафика
от вредоносного ПО и рекламы — рай для злоумышленника
и инсайдера с последующими серьезными финансовыми
и репутационными рисками для компании.

Мы предлагаем:

Внедрение и поддержку релевантной вашим потребностям
централизованной системы контроля доступа
к web-ресурсам, защиту web-трафика с последующей
интеграцией с DLP-системой.



Вернуться в список решений
Вернуться в раздел

Могут быть полезны:

- Защита каналов связи
- Тестирование на проникновение

Безопасность Zero Trust (ZTNA)

С ростом количества мобильных гаджетов и облачных сервисов злоумышленникам стало значительно проще проникать внутрь доверенной зоны и беспрепятственно перемещаться по ней.

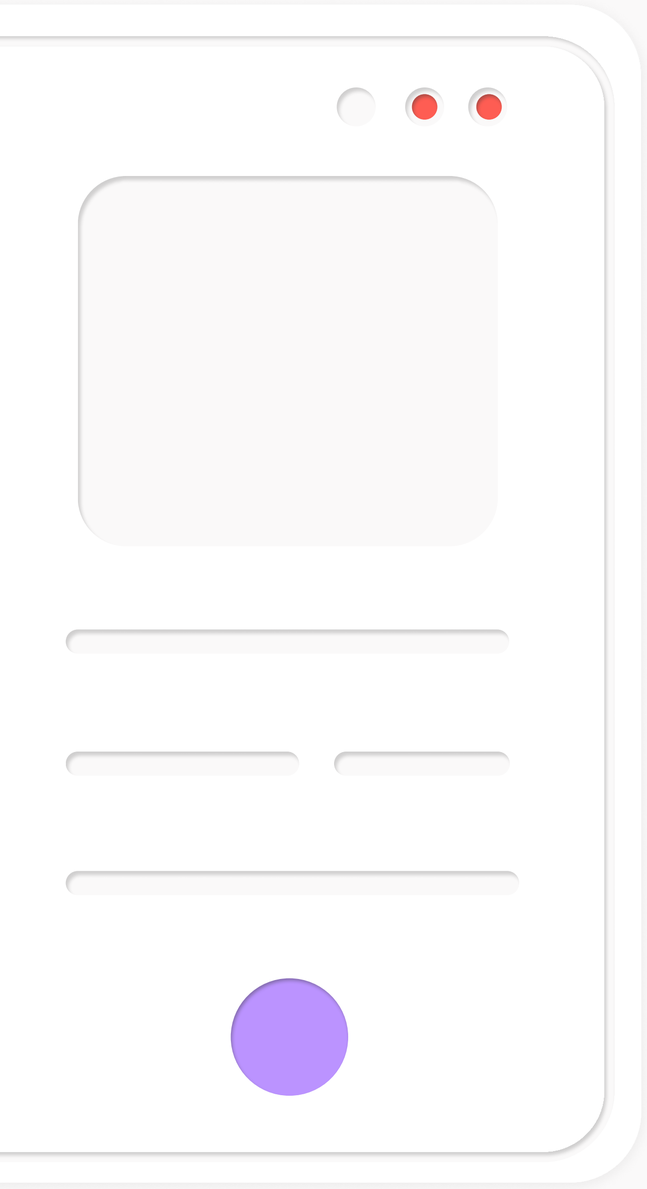
Мы предлагаем:

Внедрение концепции ZTNA для воссоздания периметра в текущих реалиях и обеспечения безопасности «поверхности защиты», микросегментацию, построение минимально приемлемых уровней привилегий пользователей, аутентификацию с позиции «нулевого доверия» и полноценное управление всеми устройствами и приложениями.

Могут быть полезны:

- Контроль действий Привилегированных пользователей
- Контроль активности и мониторинг действий пользователей

Вернуться в список решений
Вернуться в раздел



Защита приложений

Защита Web-приложений (WAF)

Безопасность мобильных устройств

Защита баз данных и приложений (DAF, DBF)

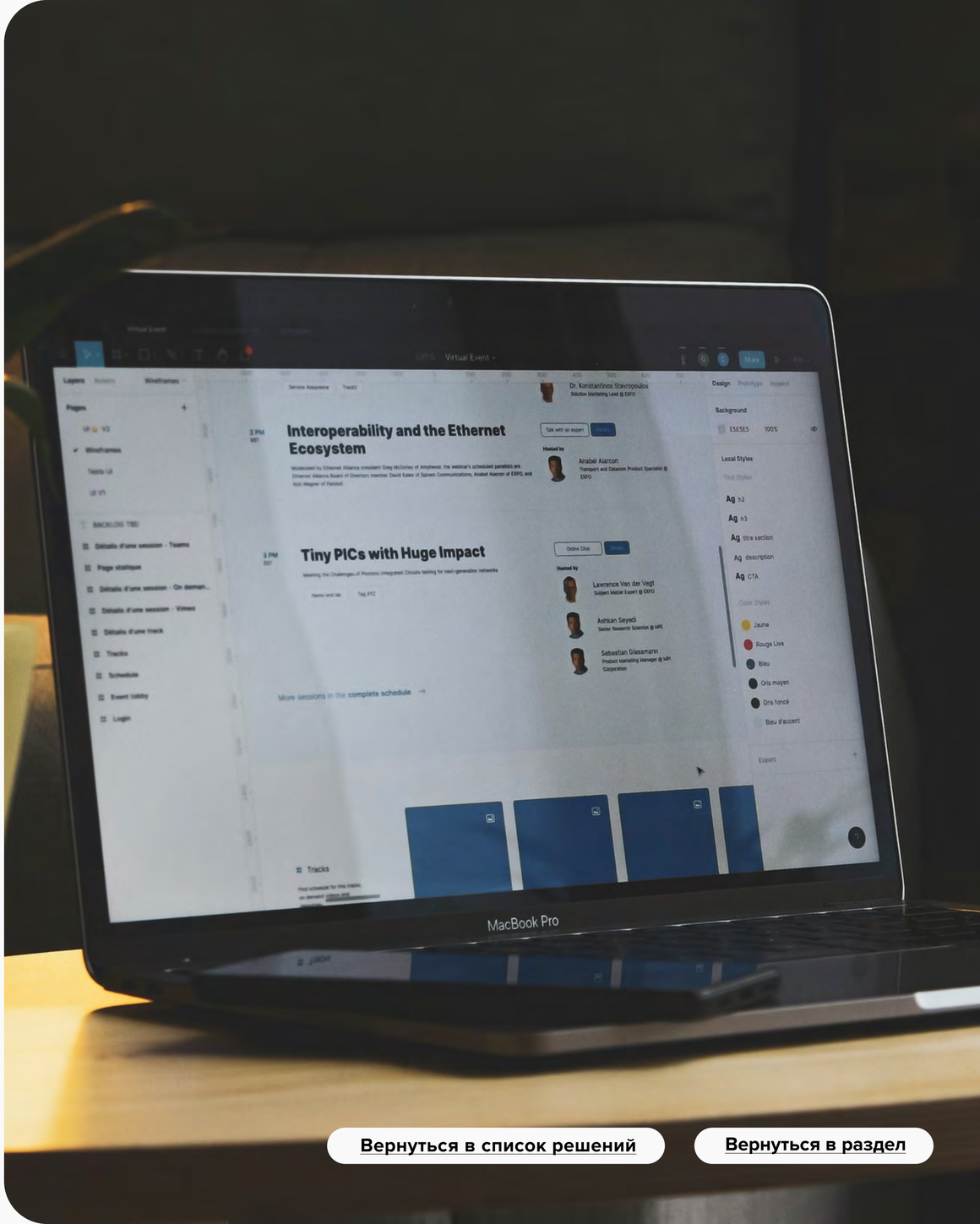
Защита web-приложений (WAF)

Веб-приложения — популярная среда для атак. Во многих компаниях есть веб-продукты в том или ином виде: приложения, микросервисы, API.

При этом большинство приложений уязвимы для атак злоумышленников.

Мы предлагаем:

Подбор индивидуального варианта защиты веб-приложений, исходя из потребностей бизнеса и ИБ. Внедрение решения и техническое сопровождение.



Могут быть полезны:

- Защита почтовых систем (E-mail Security)

Вернуться в список решений
Вернуться в раздел

Безопасность мобильных устройств

Мобильные устройства скрывают в себе целый ряд серьезных рисков, с помощью которых злоумышленник может получить доступ к корпоративным системам и сервисам.

Мы предлагаем:

Комплекс мер в виде внедрения и обеспечения политик ИБ, технические меры защиты при физическом доступе к устройству, антиспам и антивирусную защиту, защиту передаваемой информации с мобильного устройства в канале связи и по протоколам, включая шифрование.

Все это позволяет снизить риск уязвимости и обеспечить защиту корпоративных ресурсов

Могут быть полезны:

- Безопасность Zero Trust (ZTNA)

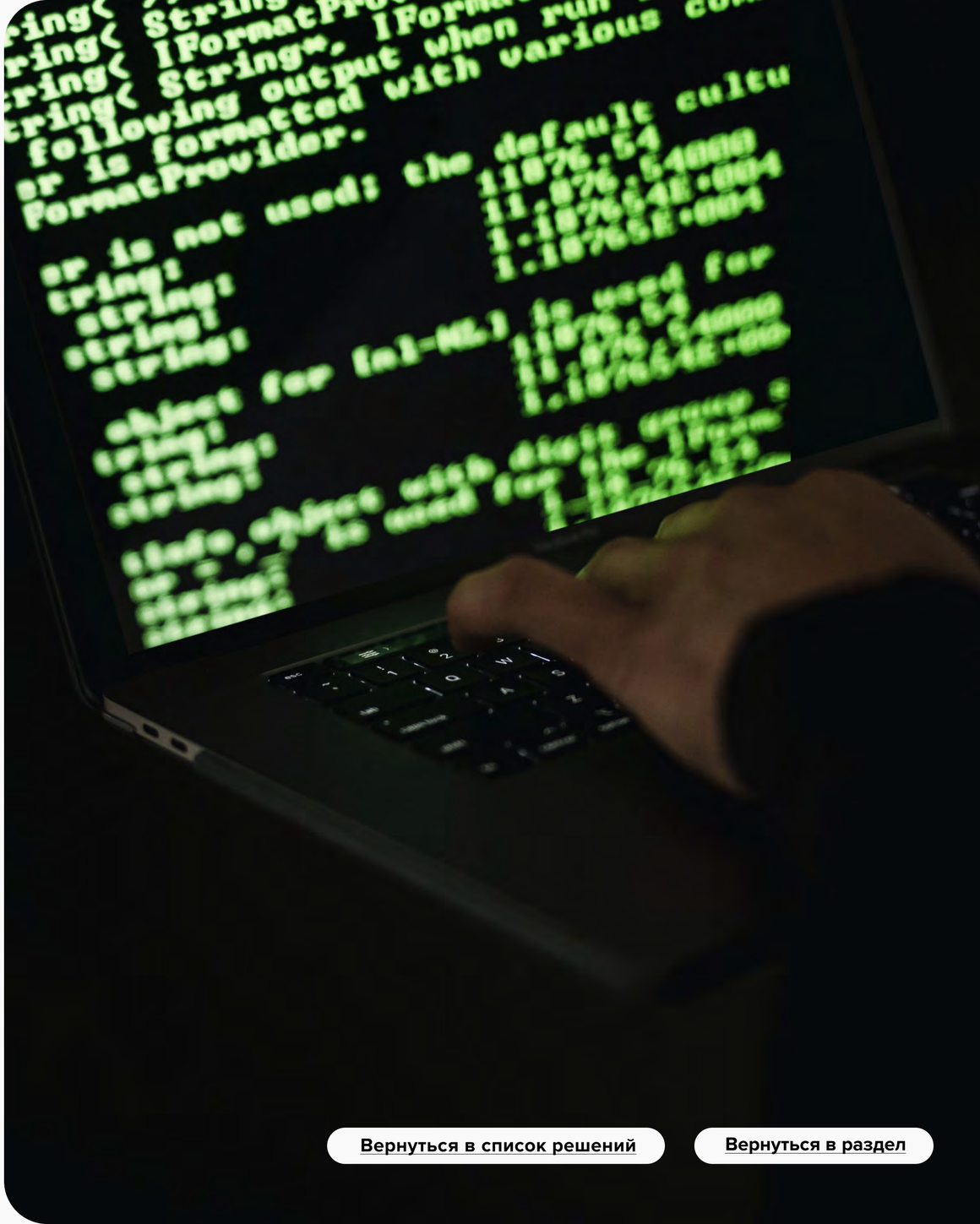
Вернуться в список решений
Вернуться в раздел

Защита баз данных и приложений (DAF, DBF)

Получая доступ к приложению, злоумышленник может не только деактивировать его работу, но и завладеть ценной информацией, что грозит крупными финансовыми и репутационными рисками.

Мы предлагаем:

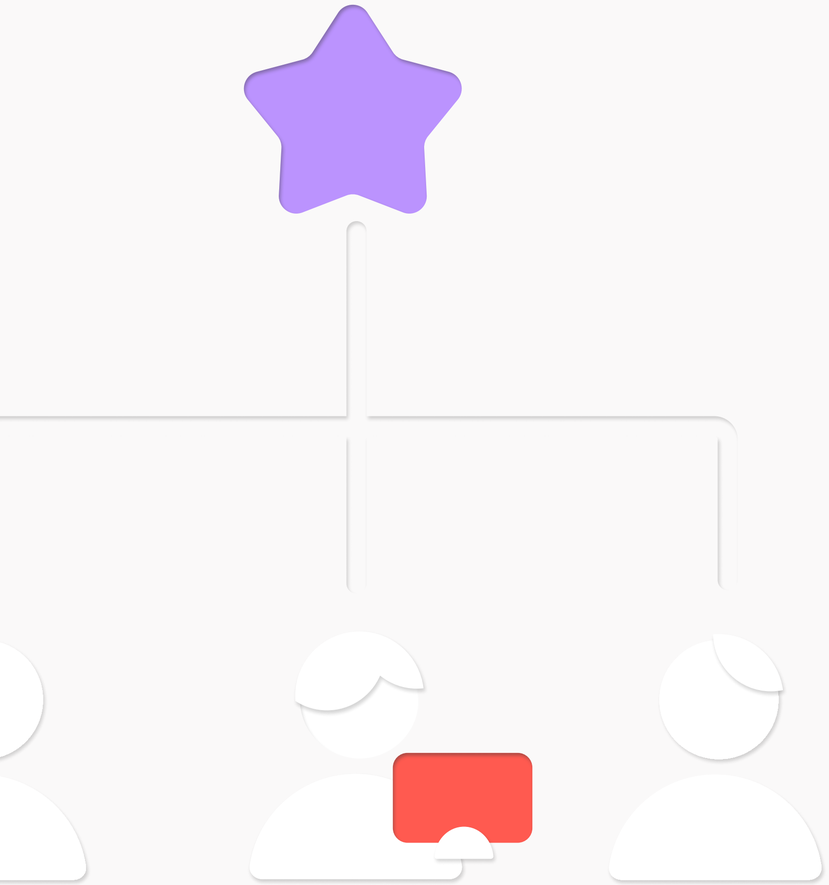
Внедрение, настройку и сопровождение систем аудита и блокировки сетевого доступа к базам данных и бизнес-приложениям. За счет непрерывного мониторинга обращений к базам данных и веб-приложениям детектируем подозрительные действия в реальном времени, купируем нетипичные либо неавторизованные запросы и ответы, обезличиваем данные при передаче и защищаем от внешних атак.



Вернуться в список решений
Вернуться в раздел

Могут быть полезны:

- Защита почтовых систем (E-mail Security)



Защита от утечек и контроль пользователей

Защита от утечек информации (DLP)

Контроль действий привилегированных пользователей (PAM)

Контроль активности и мониторинг действий пользователей (UAM)

Защита от утечек информации (DLP)

Утечка данных — одна из самых больших проблем в интернет-бизнесе. DLP-системы особенно актуальны в рамках обеспечения защиты в соответствии с требованиями N°152-ФЗ о «Защите персональных данных», N°98-ФЗ о «Коммерческой тайне», N° 149-ФЗ об «Информации и защите информации».

Мы предлагаем:

Контроль всех каналов и способов передачи данных в электронном виде. Использование контентного, лингвистического, транслитерационного анализа, а также выявление замаскированного текста для обнаружения информации независимо от способов передачи, видов и форматов хранения. Вы получите интерактивную блокировку каналов утечки (копирования, передачи, распечатки и пр.), а не только детектирование действий.

Могут быть полезны:

- Управление доступом (IDM, SSO)
- Контроль активности и мониторинг действий пользователей (UAM)

Вернуться в список решений
Вернуться в раздел

Контроль действий привилегированных пользователей (PAM)

Контроль привилегированных пользователей (Privileged Account Management) направлен на мониторинг действий сотрудников, имеющих расширенные права. Так вы сможете обезопасить свой бизнес, даже если часть задач в администрировании систем необходимо передать сторонним организациям.

Мы предлагаем:

Внедрение PAM-системы для централизованного управления учетными записями, аудита действий пользователей с расширенными правами, контроля доступа к административным ресурсам, а также контроля аутентификации и авторизации, настроек защиты с помощью паролей.

Вернуться в список решений
Вернуться в раздел

Могут быть полезны:

- Безопасность Zero Trust (ZTNA)
- Управление доступом (IDM, SSO)

Контроль активности и мониторинг действий пользователей (UAM)

От внешних угроз бизнес можно обезопасить с помощью брандмауэра, антивируса и т. д.

Но что делать с внутренней угрозой, которая может исходить от сотрудников или специалистов, привлеченных на аутсорсе?

Мы предлагаем:

Подбор и внедрение решений по отслеживанию действий и поведения сотрудников. UAM-системы обеспечивают мониторинг работников и сторонних пользователей, поиск внутренних угроз и оптимизацию производительности каждого рабочего места.

Могут быть полезны:

- Многофакторная аутентификация (MFA)
- Безопасность Zero Trust (ZTNA)

Вернуться в список решений
Вернуться в раздел

Сетевая безопасность

Защита каналов связи (VPN)

Защита от DDoS

Межсетевые экраны нового поколения (NGFW)

Обнаружение и защита от вторжений
и нетипичных действий (IDS, IPS)

Защита каналов связи (VPN)

VPN необходим для компаний, работающих в сфере, подпадающей под нормативные акты с требованиями к защищенным каналам связи.

При наличии систем по работе с ПД, ГИСов или объектов КИИ требуются сертифицированные средства защиты каналов связи.

Мы предлагаем:

Внедрение технологии VPN (Virtual Private Network) для создания зашифрованного канала связи поверх открытых сетей передачи данных. Исключение несанкционированного перехвата информации третьими сторонами.

Могут быть полезны:

- Многофакторная аутентификация (MFA)
- Защита доступа в сеть интернет (SWG)

Вернуться в список решений
Вернуться в раздел

Защита от DDoS

Атакам на «отказ в обслуживании интернет-ресурса» подвержены любые организации, присутствующие в интернете. Вопрос не в том, атакуют вас или нет, а в том, когда это случится. Доступность интернет-ресурса — ключевой фактор сохранения и увеличения прибыли, которую сайт приносит бизнесу.

Если ваш сайт долго загружается или вовсе недоступен, посетители перейдут на другой ресурс.

Мы предлагаем:

Подбор оптимального для вашего бизнеса Anti-DDoS решения, которое спасет компаниюот финансовых потерь.

Могут быть полезны:

- Защита систем виртуализации (VDI)

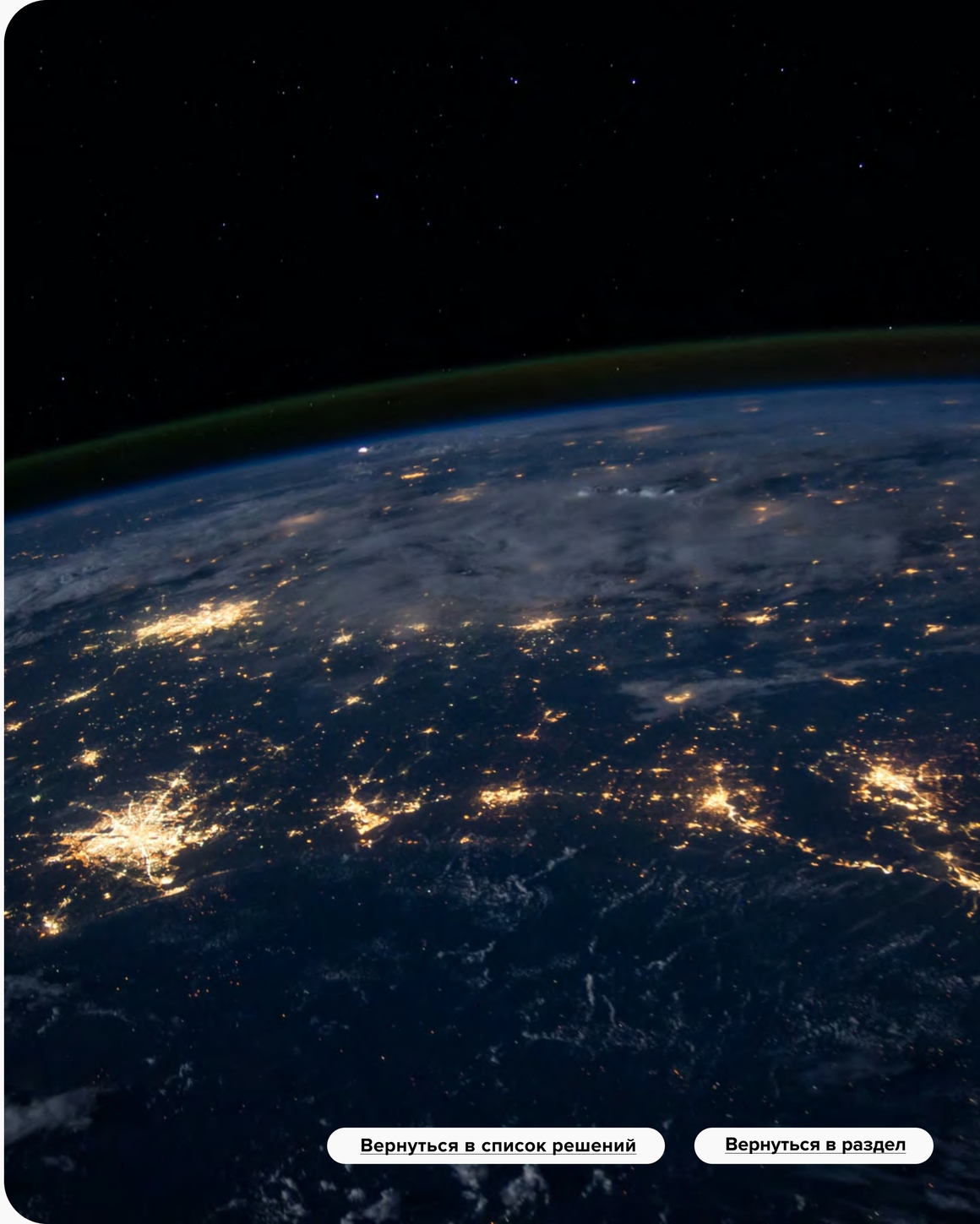
Вернуться в список решений
Вернуться в раздел

Межсетевые экраны нового поколения (NGFW)

NGFW нацелен на защиту периметра сети и включает в себя целый ряд важных функций в виде: межсетевого экранирования, предотвращения сетевых вторжений, антивирусной проверки трафика, защиты от угроз «нулевого дня», контроля доступа пользователей и приложений в сеть интернет, безопасного удаленного доступа, расшифровки HTTPS-трафика и т.д.

Мы предлагаем:

Подбор, интеграцию и настройку решения
по комплексной защите периметра вашей компании
с использованием межсетевых экраном нового поколения
(NGFW), а также обучение ваших сотрудников
и техническую поддержку.



Могут быть полезны:

- Защита систем виртуализации (VDI)

Вернуться в список решений
Вернуться в раздел

Обнаружение и защита от вторжений и нетипичных действий (IDS, IPS)

IDS (система обнаружения вторжений) — система сетевой безопасности, предназначенная для выявления сетевых атак и аномалий.

IPS (система предотвращения вторжений) — система сетевой безопасности, предназначенная для обнаружения несанкционированных действий и атак, а также автоматизированного противодействия им.

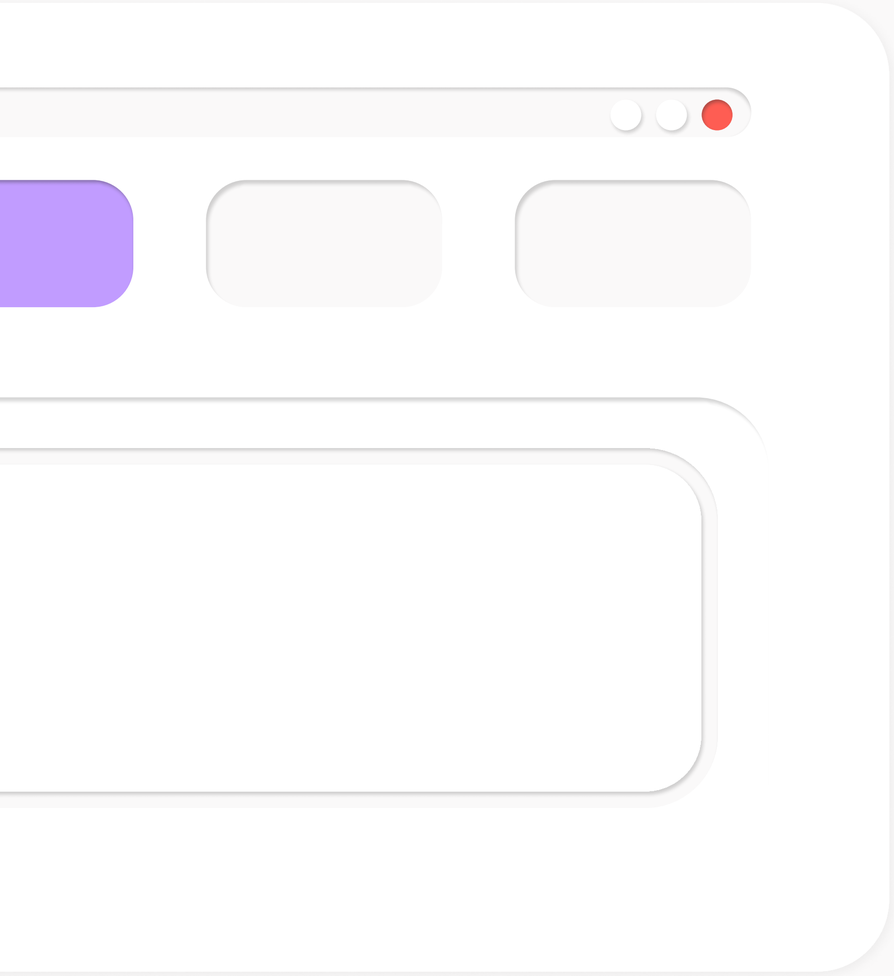
Мы предлагаем:

Решения по отслеживанию трафика (сравниваем с актуальной базой данных атак), а также по блокировке небезопасного трафика с дальнейшей генерацией события ИБ для администратора.

Могут быть полезны:

- Противодействие целевым атакам (AntiAPT)

Вернуться в список решений
Вернуться в раздел



Мониторинг и управление инцидентами ИБ

Системы мониторинга и реагирования на инциденты ИБ (SIEM)

Системы реагирования на инциденты информационной безопасности (IRP/SOAR)

Расследование инцидентов ИБ

Построение SOC

Системы мониторинга и реагирования на инциденты ИБ (SIEM)

Количество кибератак стабильно растет, поэтому скорость обнаружения угроз и оперативное реагирование со стороны службы информационной безопасности на вероятные инциденты становятся особенно важными.

Мы предлагаем:

Внедрение SIEM-системы позволит сократить риски ИБ благодаря своевременному выявлению и обработке инцидентов, а также ускорить их расследование. Автоматический контроль точности выполнения требований законодательства, международных стандартов и нормативных актов.

Могут быть полезны:

- Противодействие целевым атакам (AntiAPT)
- Безопасность Zero Trust (ZTNA)

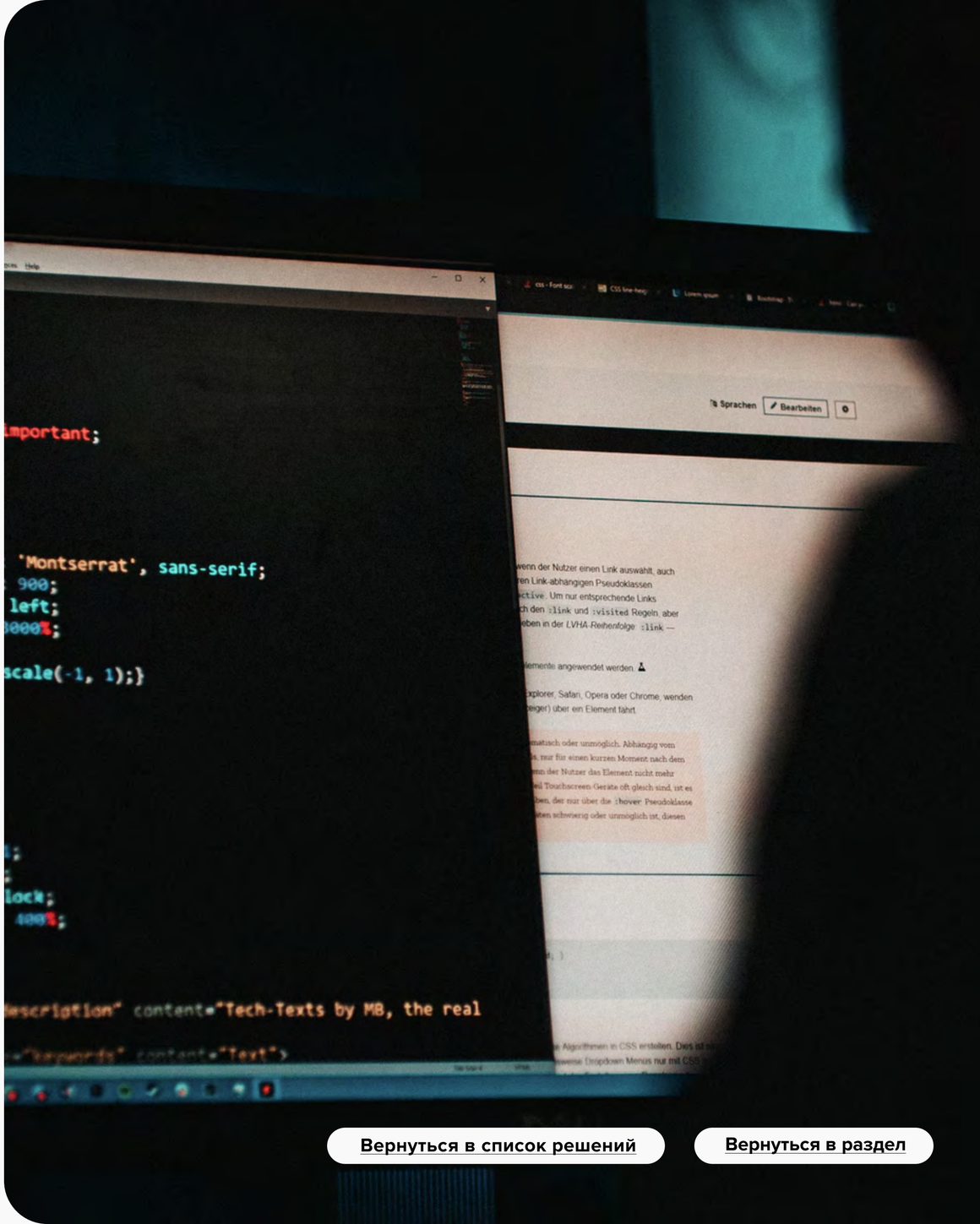
Вернуться в список решений
Вернуться в раздел

Системы реагирования на инциденты информационной безопасности (IRP/SOAR)

Из-за растущего числа кибератак под угрозой находятся данные и информационные системы всех компаний, работающих в интернете. Если быстро обнаружить и среагировать на потенциальную угрозу, то защита информации будет легче и эффективнее.

Мы предлагаем:

Внедрение IRP/SOAR-системы для повышения скорости выявления кибератак. Софт снижает со специалистов SOC нагрузку и избавляет от массы рутинных задач.



Могут быть полезны:

- Противодействие целевым атакам (AntiAPT)

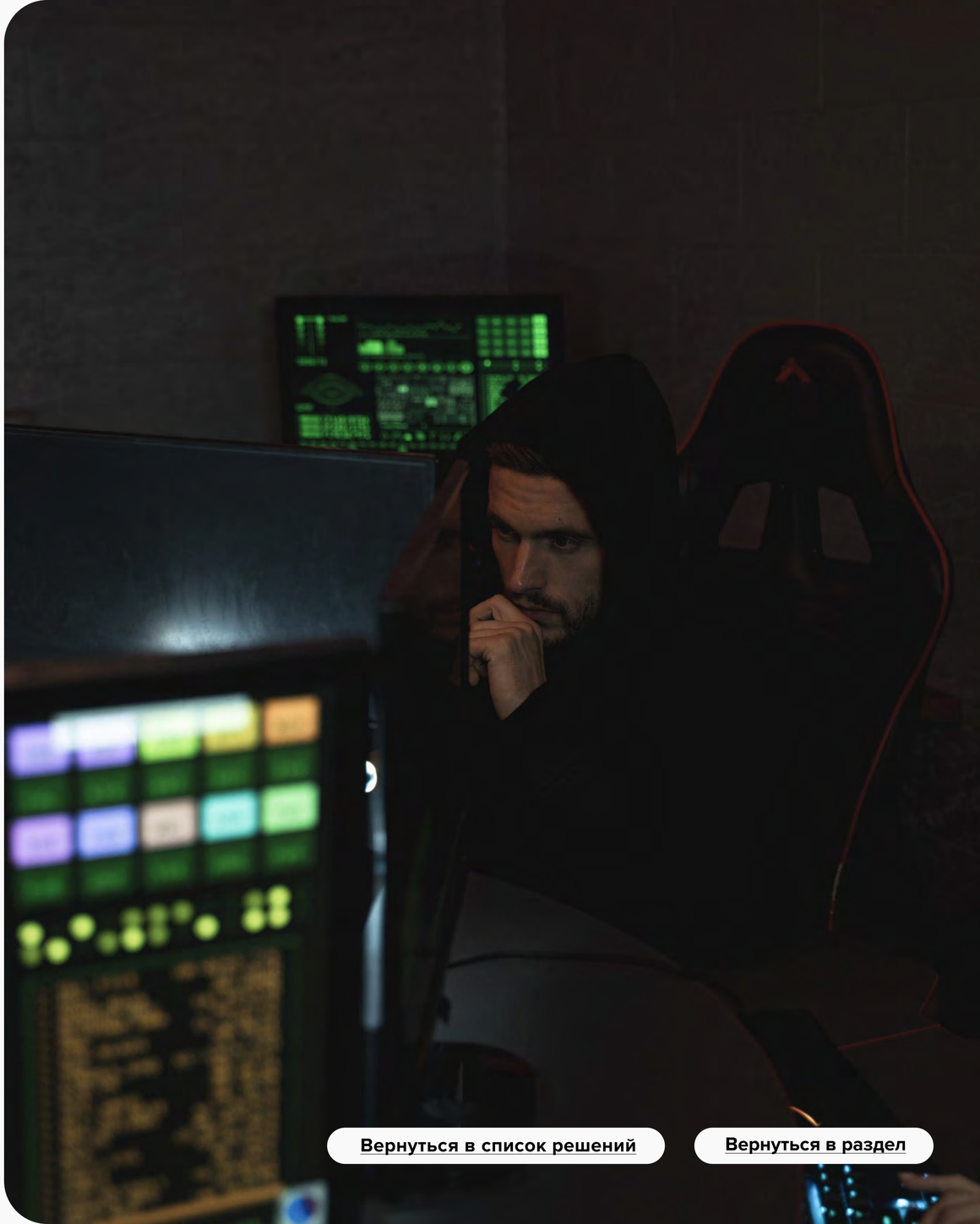
Расследование инцидентов ИБ

Все компании, работающие в сети, могут столкнуться с кибератаками, несанкционированным доступом и другими инцидентами ИБ.

От скорости и правильности их расследования может зависеть дальнейшая безопасность ваших данных.

Мы предлагаем:

Профессиональное расследование инцидентов ИБ, включая: локализацию и ликвидацию последствий, выявление виновных лиц и их мотивов, помощь в привлечении их к ответственности и анализ инцидентов, принятие мер по предупреждению и предотвращению подобного в дальнейшем.



Могут быть полезны:

- Системы мониторинга и реагирования на инциденты ИБ (SIEM)

Вернуться в список решений
Вернуться в раздел

Построение SOC

Полноценный центр мониторинга необходим не только крупным IT-компаниям, но и быстрорастущим стартапам, ведь количество кибератак, несанкционированных доступов и других инцидентов ИБ увеличивается с каждым годом.

Поэтому защита информации актуальна, как никогда.

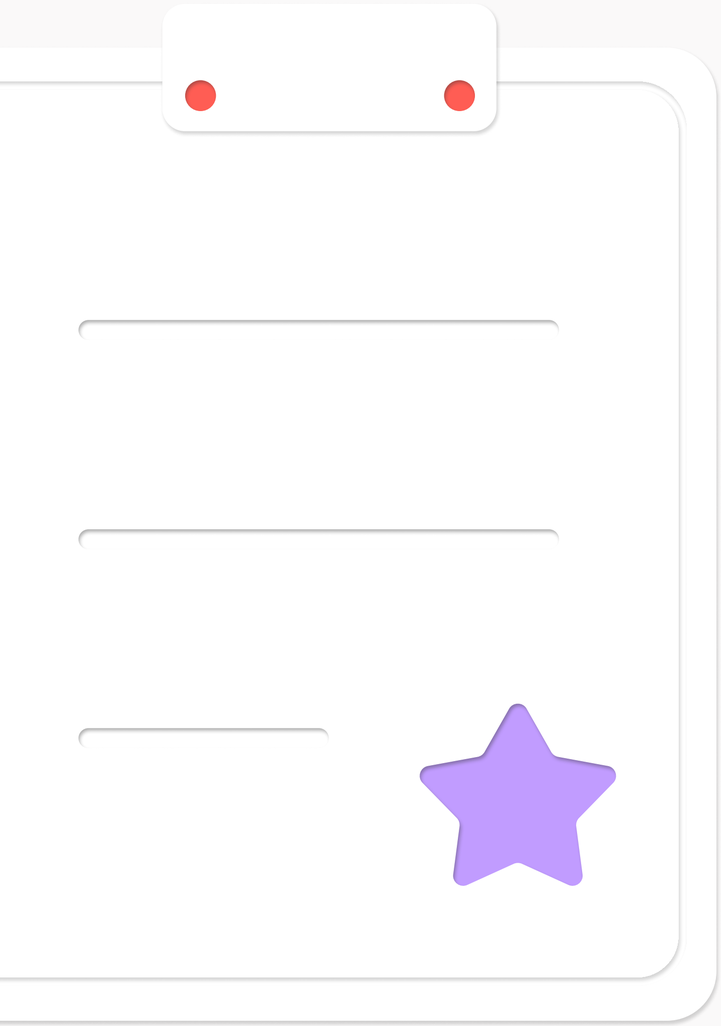
Мы предлагаем:

Квалифицированную экспертную помощь в построении SOC (Security Operation Center) на базе вашей компании. SOC обеспечивает централизованный сбор и анализ информации об инцидентах ИБ, а также своевременное реагирование на них.

Могут быть полезны:

- Системы мониторинга и реагирования на инциденты ИБ (SIEM)

Вернуться в список решений
Вернуться в раздел



Обучение и повышение квалификации

Лицензированные ФСТЭК и ФСБ курсы

Авторские курсы ИБ

Сертифицированные вендорские курсы ИБ

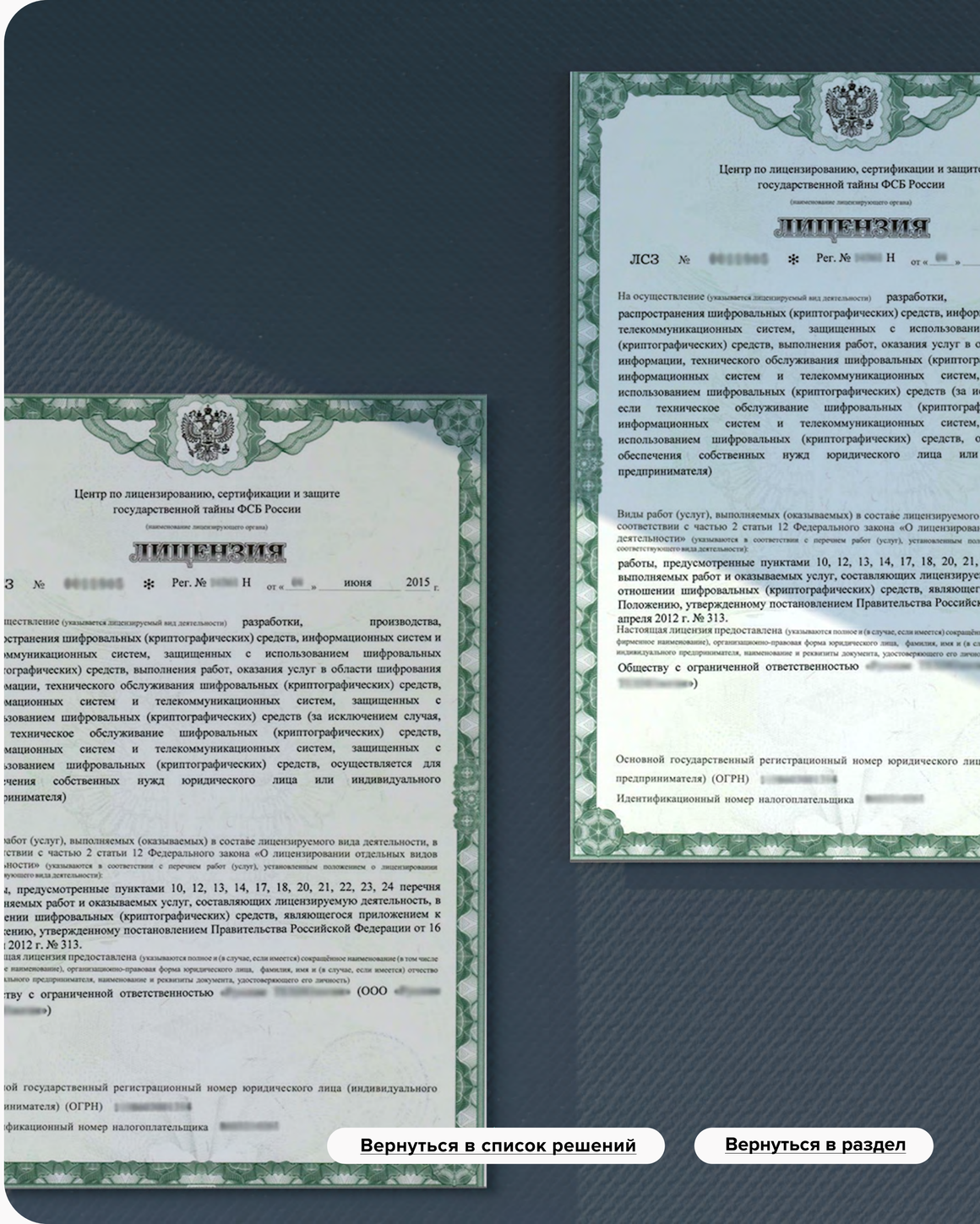
Лицензированные ФСТЭК и ФСБ курсы

Обучение информационной безопасности актуально, поскольку стремительно растет потребность в защите корпоративных данных от несанкционированного доступа, кибератак и иных угроз. Информационные технологии развиваются быстро, поэтому специалистам необходимо регулярно повышать квалификацию.

Мы предлагаем:

Полноценные обучающие курсы по информационной безопасности, лицензированные ФСТЭК и ФСБ.

Вы получите только актуальные знания и навыки, гибкий подход и график обучения, все необходимые обучающие материалы и авторскую методику преподавания.



Могут быть полезны:

- Авторские курсы ИБ
- Сертифицированные вендорские курсы ИБ

Вернуться в список решений
Вернуться в раздел

Авторские курсы ИБ

Сфера информационной безопасности довольно обширна, поэтому даже специалистам с базовыми знаниями в этой области всегда есть куда расти и развиваться. Новые знания позволят внедрить новые технологии, методы в компанию.

Мы предлагаем:

Авторские курсы, на которых обучающиеся получают знания в узкоспециализированной области информационной безопасности.

Например, вы можете освоить криптографические методы и средства защиты информации или особенности корпоративной защиты внутренних угроз ИБ.

Могут быть полезны:

- Лицензированные ФСТЭК и ФСБ курсы
- Сертифицированные вендорские курсы ИБ

Вернуться в список решений
Вернуться в раздел

Сертифицированные вендорские курсы ИБ

IT-компаниям часто требуется обучение сотрудников, повышение квалификации и т. д., ведь информационные технологии, включая ИБ, быстро меняются. Но что делать, если нет собственных ресурсов для проведения курсов?

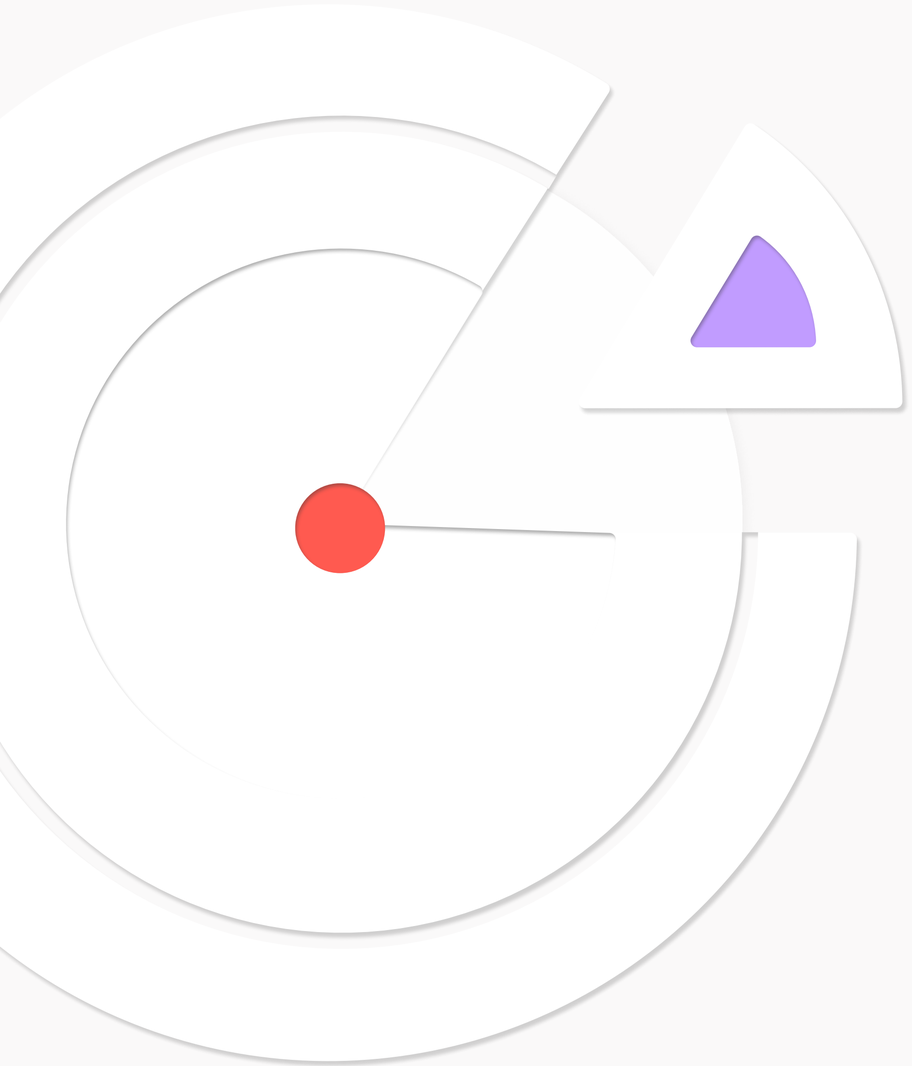
Мы предлагаем:

Проведение сертифицированных вендорских курсов по ИБ на аутсорсе. У нас полноценный учебный комплекс, есть все необходимые материалы, ресурсы и интерактивная онлайн-платформа. Преподаватели с высокой квалификацией и богатым практическим опытом работы.

Могут быть полезны:

- Лицензированные ФСТЭК и ФСБ курсы
- Авторские курсы ИБ

Вернуться в список решений
Вернуться в раздел



Консалтинг ИБ и аудит

Анализ защищенности ИС

Тестирование на проникновение

Аудит для НФО (757-П)

Аудит для КФО (683-П)

Защита от НСД

Сопровождение ОКЗИ

Соответствие ПДн (152-ФЗ)

Помощь в получении лицензии ФСТЭК

Аттестация АРМ

Аутсорсинг ИБ

Системы обучения пользователей (Security Awareness)

Анализ защищенности ИС

Многие уязвимости и слабости информационной системы могут оставаться незамеченными месяцами, а то и годами, пока не дадут о себе знать. Не ждите, когда пробел в системе станет причиной несанкционированного доступа, хищения данных и т. д.

Мы предлагаем:

Всесторонний анализ защищенности сетевого периметра, беспроводной инфраструктуры, ПО, веб-приложений и сайтов, АСУ ТП и т. д.

Определим возможные действия злоумышленников, предоставим экспертную оценку эффективности использованных мер защиты и рисков для инфраструктуры организации, а также проведем сканирование и инвентаризацию всех возможных способов несанкционированного доступа.

Могут быть полезны:

- Обеспечение защиты информации при эксплуатации АСУ ТП

Вернуться в список решений
Вернуться в раздел

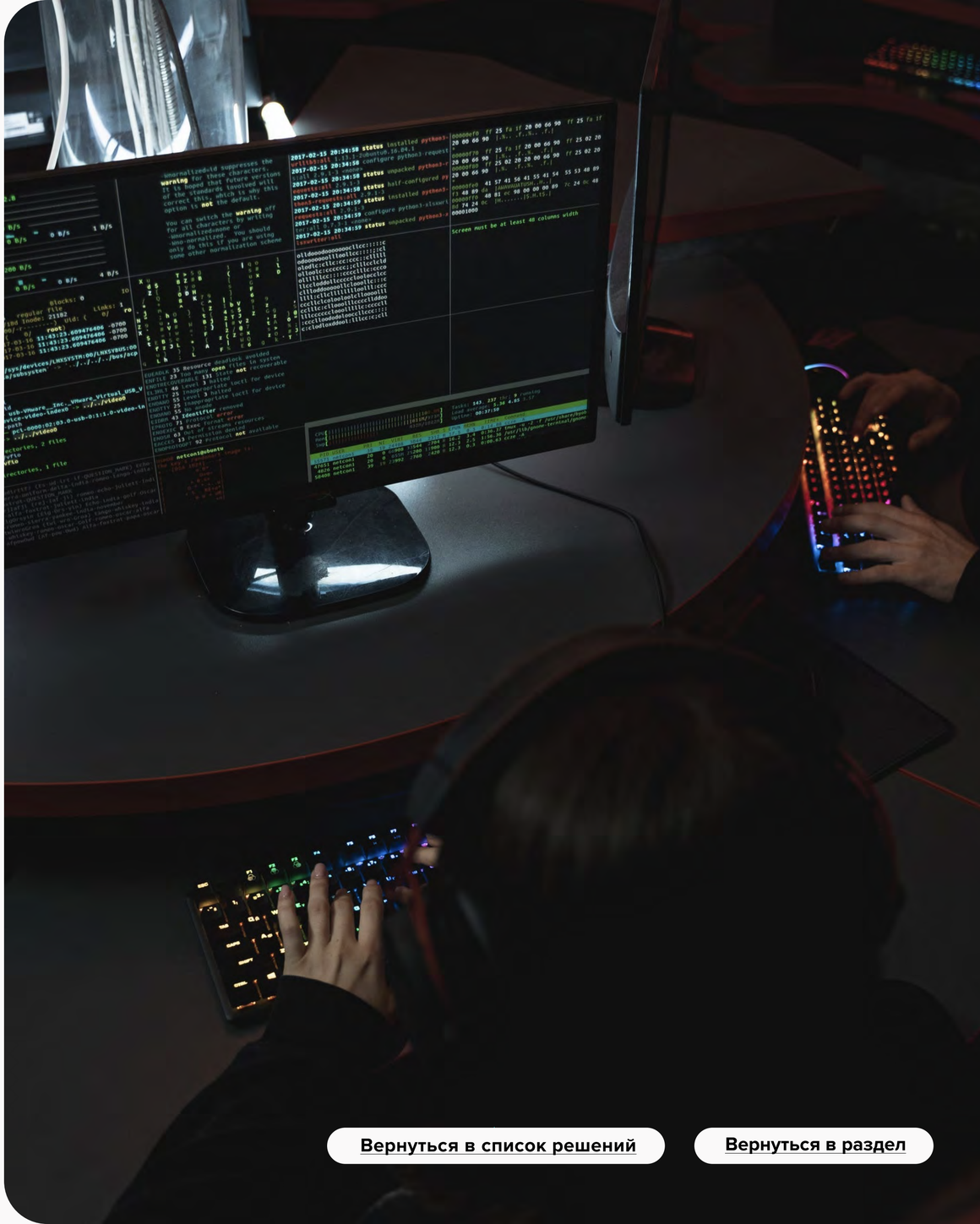
Тестирование на проникновение

Смоделированная атака злоумышленников — один из лучших способов выявления уязвимостей системы и определения возможных действий киберпреступников.

Мы предлагаем:

Проведение комплексного пентеста, а также социотехнического или технического теста для определения слабых мест в защите информационной системы.

Вы получите отчет с описанием методики и хода тестирования, экспертными выводами с оценкой уровня защищенности, описанием недостатков СУИБ и рекомендациями по устранению обнаруженных недочетов.



Могут быть полезны:

- Защита доступа в сеть интернет (SWG)
- Аудит для КФО (683-П)

Вернуться в список решений
Вернуться в раздел

Аудит для НФО (757-П)

Согласно Положению ЦБ РФ №757-П обеспечивать защиту данных теперь должны не только банки, но и НФО (некредитные финансовые организации).

Мы предлагаем:

Оценку уровня защиты в соответствии с требованиями ГОСТов, пентест (внешний и внутренний) для категорий, выбранных заказчиком.

Также мы поможем улучшить защитные средства и подготовим отчет в соответствии с требованиями Центробанка.

Могут быть полезны:

- Аудит для КФО (683-П)

Вернуться в список решений
Вернуться в раздел

Аудит для КФО (683-П)

Положение ЦБ РФ №683-П устанавливает обязательные требования к обеспечению защиты информации для кредитных организаций. Для успешного ведения банковской деятельности необходимо обеспечить соответствующий уровень защищенности.

Мы предлагаем:

Определение систем, которые нуждаются в проверке, анализ и оценку защиту ПО, информационных систем, технологические и иные меры защиты информации.

В услугу входит также консультация и аудит для заказчика по нормативам ГОСТов, подготовка отчетной документации для Центробанка.

Вернуться в список решений
Вернуться в раздел

Могут быть полезны:

- Аудит для НФО (757-П)

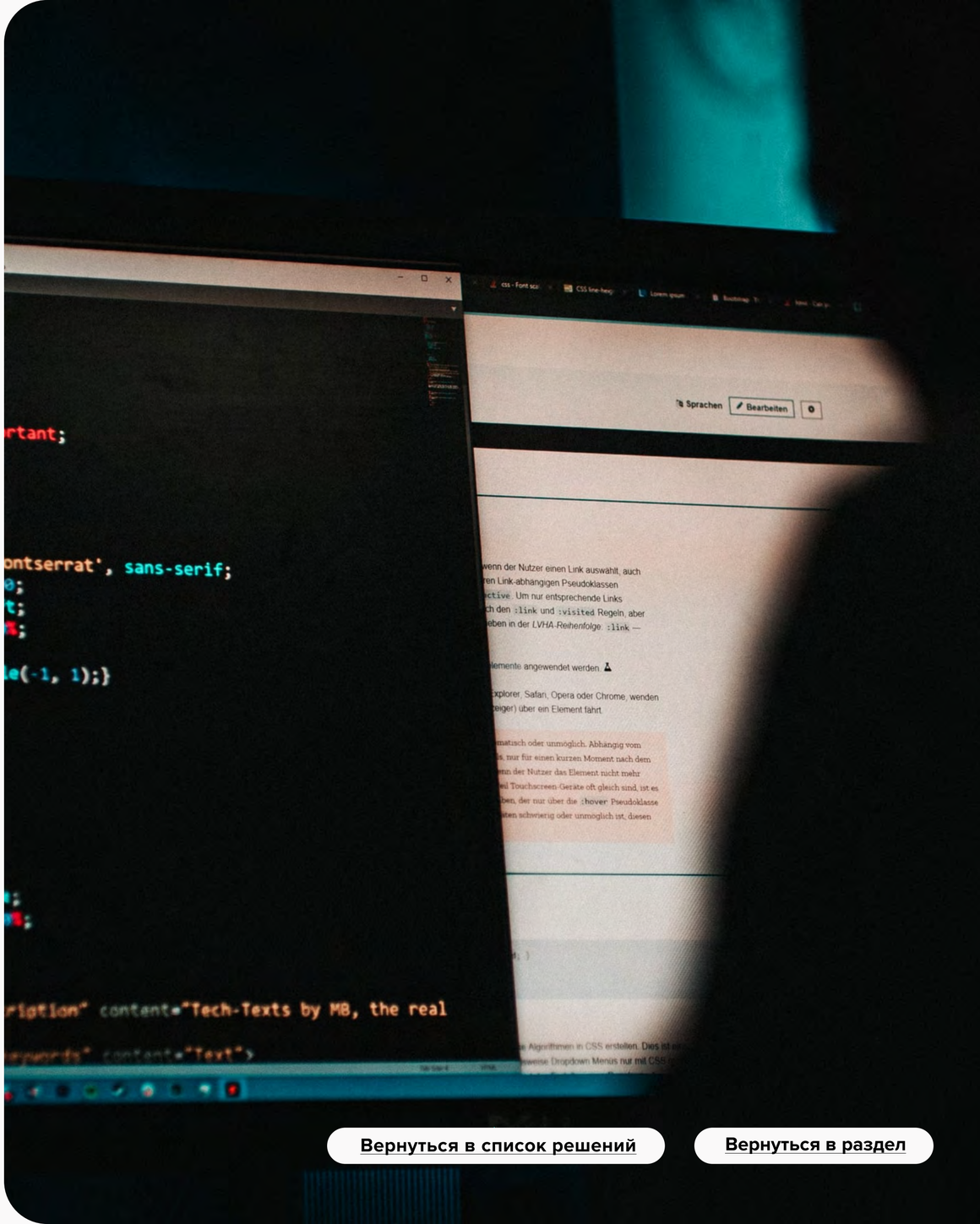
Защита от НСД

Несанкционированный доступ — частая причина хищения и утери данных, сбоев в работе систем и т. д.

СЗИ (средства защиты информации) должны не только надежно защищать ИС, но и соответствовать нормам госстандартов.

Мы предлагаем:

Внедрение специализированных программных и программно-аппаратных средств, обеспечивающих защиту от актуальных угроз. Подбор комплексных решений, подходящих именно вашей компании, установка и настройка с учетом вашей информационной инфраструктуры и требований государственных регуляторов.



Могут быть полезны:

- Защита конечных точек (EDR) и антивирусы

Вернуться в список решений
Вернуться в раздел

Сопровождение ОКЗИ

Любые организации, использующие криптографические средства защиты информации (СКЗИ), могут не создавать на базе собственной компании ОКЗИ, а отдать эту работу на аутсорсинг.

Мы предлагаем:

Проверку готовности обладателей конфиденциальной информации к самостоятельному использованию СКЗИ, разработку мероприятий по обеспечению функционирования и безопасности, контроль за соблюдением условий использования СКЗИ, разработку схемы организации криптографической защиты конфиденциальной информации и т. д.

Могут быть полезны:

- Соответствие ПДн (152-ФЗ)

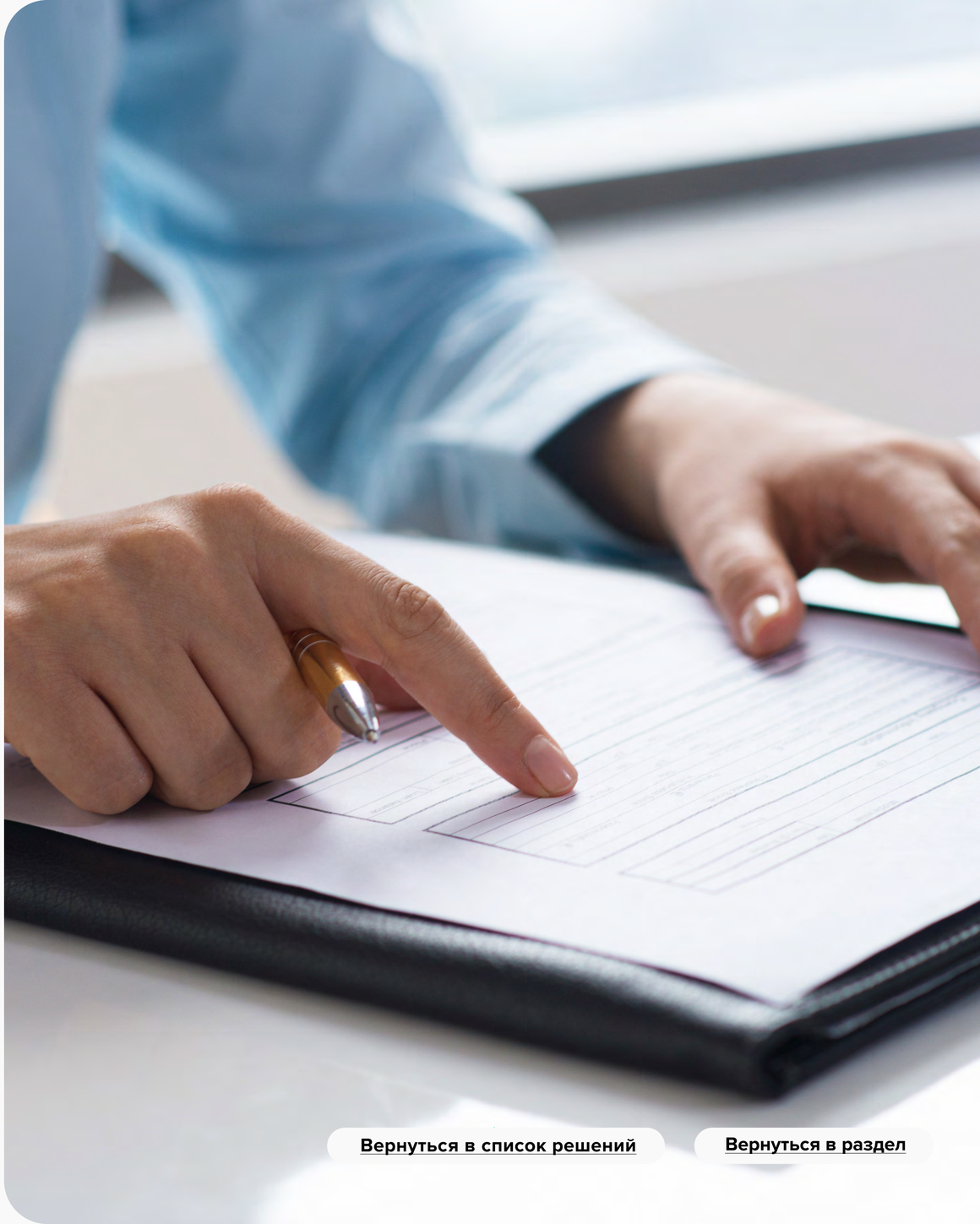
Вернуться в список решений
Вернуться в раздел

Соответствие ПДн (152-ФЗ)

152-ФЗ «О персональных данных» обязаны соблюдать все организации, которые взаимодействуют с персональными данными, получают к ним доступ. Причем не имеет значение, как они получили их — напрямую от пользователей/ сотрудников или через третьих лиц.

Мы предлагаем:

Сбор и анализ информации о порядке и способах обработки ПДн, проверку внутренних нормативных и организационно-распорядительных документов на соответствие требованиям законодательства. Установим уровни защищенности ПДн, разработаем и актуализируем документацию, создадим и модернизируем СЗПДн, а также проведем оценку эффективности реализованных мер по обеспечению безопасности ПДн.



Могут быть полезны:

- Сопровождение ОКЗИ

Вернуться в список решений
Вернуться в раздел

Помощь в получении лицензии ФСТЭК

Оказываете услуги в сфере защиты конфиденциальной информации (коммерческая тайна, персональные данные и т. д.).

Значит вам обязательно требуется лицензия ФСТЭК на техническую защиту конфиденциальной информации (ТЗКИ).

Мы предлагаем:

Аттестацию защищаемых помещений (ЗП) и автоматизированных рабочих мест (АРМ) вашей компании, профпереподготовку сотрудников по ИБ, организацию закупки ПО. Также мы обеспечим контрольно-измерительным оборудованием, соберем и проанализируем пакет документов на соответствие вашей организации требованиям ФСТЭК. Организуем взаимодействие с госорганами.

Могут быть полезны:

- Лицензированные ФСТЭК и ФСБ курсы ИБ

Вернуться в список решений
Вернуться в раздел

Аттестация АРМ

Аттестация АРМ (автоматизированного рабочего места) проводится в обязательном порядке, если ваша компания ведет деятельность в области ИБ, а также при работе с персональными данными (ПДн).

Мы предлагаем:

Оценку защищенности АРМ, с помощью которой подтверждается или опровергается соответствие требованиям безопасности информации.

Мы разработаем программу и методику аттестационных испытаний. Проведем их и выдадим соответствия при положительной исходе либо предоставим рекомендации по исправлению недочетов.

Вернуться в список решений
Вернуться в раздел

Могут быть полезны:

- Сопровождение ОКЗИ
- Соответствие 152-ФЗ

Аутсорсинг ИБ

Если в штате вашей компании нет или не хватает специалистов, ресурсов для обеспечения информационной безопасности, мы поможем.

Качественная работа по обеспечению ИБ сокращает риски потери/утечки данных, НСД, и гарантирует высокую защищенность информации.

Мы предлагаем:

Мы предоставим в аренду системы защиты информации, обеспечим поддержку и администрирование установленных СЗИ. Также в рамках аутсорсинга ИБ проводится мониторинг событий ИБ и выявление инцидентов.

Могут быть полезны:

- Авторские курсы ИБ

Вернуться в список решений
Вернуться в раздел

Системы обучения пользователей (Security Awareness)

Недостаточный уровень профессиональной подготовки и квалификации сотрудников в области ИБ часто приводит к появлению «брешей» в системе безопасности компании. Отсюда вытекают проблемы с утечкой, хищением данных, взломом информационных систем и т. д. Поэтому важно постоянно углублять, расширять и актуализировать знания и навыки сотрудников.

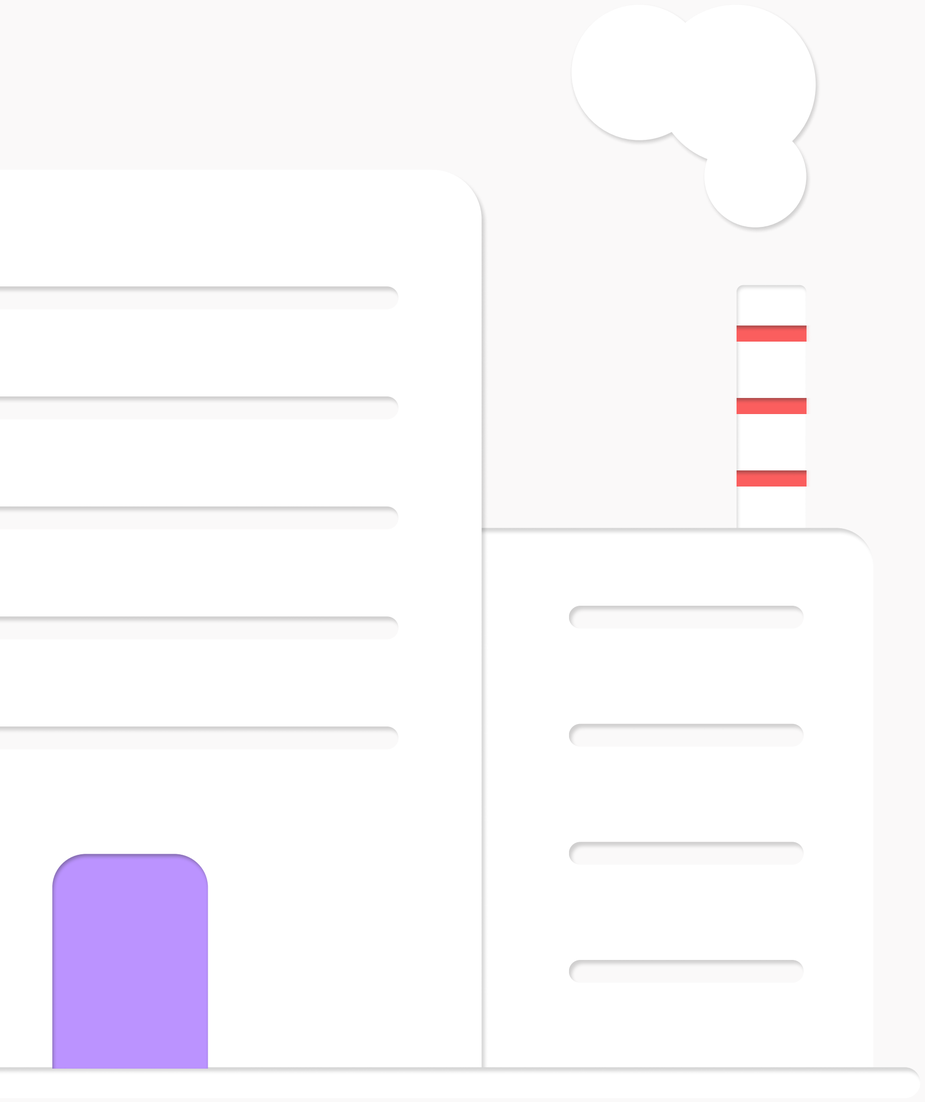
Мы предлагаем:

Теоретическое и практическое обучение ваших сотрудников информационной безопасности. Проверку уровня подготовки перед началом обучения для выявления областей знаний, которые необходимо подтянуть в первую очередь. Организуем проверку знаний, чтобы выявить, нужно дальнейшее обучение для конкретного сотрудника или нет.

Могут быть полезны:

- Защита конечных точек (EDR) и антивирусы
- Авторские курсы ИБ

Вернуться в список решений
Вернуться в раздел



Проектирование и ввод в эксплуатацию системы защиты конфиденциальной информации АСУ ТП и объектов КИИ

Обеспечение защиты информации при эксплуатации АСУ ТП

Обеспечение безопасности объектов КИИ

Обеспечение защиты информации при эксплуатации АСУ ТП

Серверы, рабочие станции, информационные системы предприятия – абсолютно все подвергается натиску со стороны хакеров.

Такие атаки парализуют предприятия и приводят к значительному экономическому ущербу.

Мы предлагаем:

Комплекс мер и решений «под ключ» по обеспечению безопасности значимых объектов КИИ (АСУ ТП, ИС, ИТС) в полном соответствии с 187-ФЗ, 22-ФЗ, 116-ФЗ и Приказом ФСТЭК №31 от 14 марта 2014 года.

Могут быть полезны:

- Категорирование КИИ
- Анализ защищенности

Вернуться в список решений
Вернуться в раздел

Обеспечение безопасности объектов КИИ

В соответствии с №187-ФЗ все компании, являющиеся объектами критической инфраструктуры, обязаны пройти процедуру категорирования, в рамках которой устанавливается соответствие объекта КИИ конкретной категории значимости или ненужность присвоения подобной категории.

Мы предлагаем:

Услуги опытной команды по выполнению требований законодательства о безопасности КИИ, включая Приказы ФСТЭК №239 от 25.12.2017 и №75 от 28.05.2020.

Выявление возможных угроз, разработку методов их устранения для избежания штрафов и санкций со стороны регулирующих оранов.

Могут быть полезны:

- Анализ защищенности ИС

Вернуться в список решений
Вернуться в раздел