CYBERSECURITY TEAM
КОМАНДА КИБЕРБЕЗОПАСНОСТИ

Проекты в области обеспечения информационной и антитеррористической безопасности

Что такое Cybersecurity Team?

Многолетний опыт совместной проектной деятельности в сфере безопасности

550+

Проектов, выполненных нашими специалистами совместно

3

Основных направления:
1. Консалтинг ИБ
2. Инструментальная защита инфраструктуры
3. Консалтинг в области антитеррористической защищённости

Консультанты и аналитики

- Международные и отечественные отраслевые стандарты
- Большой опыт по защите ГИС, ИСПДн и КИИ
- Опыт работы с отечественными регуляторами в сфере ИБ и антитеррористической безопасности

Инженеры и архитекторы

- Специализация, подтвержденная сертификатами отечественных и мировых производителей средств защиты информации
- Регулярное обучение и подтверждение квалификации
- Практический опыт внедрения большинства современных технологических решений

Основные области нашей деятельности в сфере ИБ

CYBERSECURITY TEAM
КОМАНДА КИБЕРБЕЗОПАСНОСТИ

Виды услуг, оказываемые нами, в части консалтинга и аудита информационной безопасности

Compliance

- Оценка соответствия требованиям стандартов и НПА в области безопасности
- Обеспечение выполнения законодательных, отраслевых и международных требований

Внедрение процессов

- Использование известных методологий по управлению ИБ (ISO2700x, NIST, ITIL, CIS Controls, O-ISM3)
- Проектирование бизнес-процессов и методов оценки их эффективности

Анализ угроз и уязвимости

- Разработка моделей нарушителя и угроз безопасности
- Оценка уязвимостей систем и актуальных рисков информационной безопасности

Подготовка объекта информатизации к аттестации

Защита персональных данных – ФЗ 152

Мы помогаем нашим заказчикам хранить и обрабатывать персональные данные безопасно

Для кого?
организации, осуществляющие обработку любых персональных данных субъектов

Зачем?
выполнение требований федерального законодательства, снижение рисков утечки ПДн

Когда?
при изменении процессов обработки, внедрении новых систем, в качестве подготовки к плановым проверкам

Что защищаем?
инфраструктуру, прикладные информационные системы, "на бумаге", повышение общего уровня ответственности персонала

CYBERSECURITY TEAM
КОМАНДА КИБЕРБЕЗОПАСНОСТИ

Защита персональных данных

Этапы осуществляемых работ

Комплексное обследование

Выявление процессов обработки ПДн
Оценка ИТ-инфраструктуры
Анализ имеющейся документации
Определение уровня защищенности ИС

Актуальный срез по текущему состоянию соответствия всем требованиям

Анализ угроз безопасности

Проектирование модели нарушителя
Анализ уязвимостей информационных систем
Выбор актуальных угроз

Перечень угроз безопасности, требующих первоочередной реакции

Обеспечение легитимности обработки

Формирование перечней ПДн и ИС
Формы согласий и определение порядка обработки ПД (взаимодействие с субъектами, РКН)

Полный комплект документации для предстоящих проверок

Защита персональных данных

Формирование ТЗ
Проектирование организационных и технических мер защиты
Разработка ОРД
СМР и ПНР
Испытания

Система защиты ПДн, соответствующая требованиям регуляторов

CYBERSECURITY TEAM
КОМАНДА КИБЕРБЕЗОПАСНОСТИ

CYBERSECURITY TEAM
КОМАНДА КИБЕРБЕЗОПАСНОСТИ

Безопасность КИИ – ФЗ-187

Объекты КИИ это ИС, ИТКС, АСУ ТП, функционирующие в 13 областях

здравоохранение
наука
транспорт
связь
энергетика
банковская сфера и финансовый рынок
топливно-энергетический комплекс
атомная энергетика
оборонная промышленность
ракетно-космическая промышленность
горнодобывающая промышленность
металлургическая промышленность
химическая промышленность

Значимые объекты КИИ

объект КИИ, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов КИИ

Наши компетенции

Категорирование объектов КИИ

Описание процессов, формирование перечня объектов, оценка критериев значимости объекта КИИ, подготовка форм сведений для предоставления регуляторам

Создание системы безопасности

Моделирование угроз, компьютерных атак и действий потенциального нарушителя. Формирование требований к системе безопасности. Инструментальное сканирование и анализ уязвимостей, проектирование и внедрение СЗИ, СМР и ПНР, техническое сопровождение

Интеграция с системой ГосСОПКА

Проектирование процессов информирования об инцидентах НКЦКИ и ФинЦерт, создание организационной структуры поддержки процессов обеспечения ИБ, обеспечение непрерывности, управление инцидентами

CYBERSECURITY TEAM
КОМАНДА КИБЕРБЕЗОПАСНОСТИ

Мы оказываем услуги по интеграции с ГосСОПКА

ГосСОПКА - Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак

Технические средства

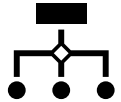
- приобретение и обслуживание средств предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на инциденты
- создание сегмента ГосСОПКА или подключение к ведомственному (коммерческому) сегменту
- защита каналов связи

Методические основы

- положение о сегменте ГосСОПКА
- должностные инструкции специалистов сегмента ГосСОПКА
- регламент взаимодействия с Главным центром
- описание мер, обеспечивающих предотвращение и (или) снижение негативного влияния инцидентов на функционирование информационных ресурсов

Процессы и процедуры

- признаки, на основе которых производится обнаружение компьютерных атак и регистрация инцидентов, описание основных типов инцидентов
- порядок действий персонала сегмента при ликвидации последствий компьютерных атак
- регламенты выполнения структурными элементами сегмента ГосСОПКИ их функций



CYBERSECURITY TEAM
КОМАНДА КИБЕРБЕЗОПАСНОСТИ

Нововведения в законодательстве РФ в области КИИ

На данный момент принято два нормативно-правовых акта РФ, которые существенным образом повлияют на необходимость модернизации существующих ИТ-инфраструктур

1. Указ Президента Российской Федерации от 30.03.2022 № 166 "О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации"

2. Указ Президента Российской Федерации от 01.05.2022 № 250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации"

Основные положения 166 Указа

На кого распространяется?

- **организации, осуществляющие закупки в соответствии с ФЗ-223, которым принадлежат объекты КИИ;**
- **органы государственной власти**

Что регулирует?

- **закупки и использование иностранного ПО на объектах КИИ**

С 31 марта 2022 года запрещено закупать иностранное ПО (в том числе в составе ПАК) в целях его использования на значимых объектах КИИ
С 31 марта 2022 года запрещено закупать услуги, необходимые для использования такого ПО на значимых объектах КИИ
БЕЗ согласования возможности осуществления закупок у уполномоченным ФОИВ.

С 1 января 2025 года запрещено использовать иностранное ПО на значимых объектах КИИ.

Правительству РФ поручено утвердить требования к указанному ПО и правила согласования закупок.
На текущий момент требования и правила не утверждены.
РИСК: сложность процедуры/невозможность согласования – риски простоя, отсутствия технической поддержки и пр.

Сформировать план мероприятий по переходу на отечественное ПО (там, где возможно), это касается и СЗИ

Сформировать план внесения изменений в ИТ-инфраструктуру (на случай необходимости полной перестройки используемых решений в производственной, хозяйственной и иной деятельности)

Основные положения 250 Указа

На кого распространяется?

- **организации, которые являются субъектами КИИ (ОГВ, государственные корпорации, стратегические предприятия и общества, юридические лица)**

Что регулирует?

Организационные меры обеспечения ИБ	• Возложить ответственность за обеспечение ИБ на заместителя руководителя • Создать структурное подразделение по обеспечению ИБ • Привлекать к обеспечению ИБ только лицензиатов ФСТЭК по ТЗКИ • Привлекать к осуществлению мероприятий по обнаружению, предотвращению и ликвидации компьютерных атак только аккредитованные центры ГосСОПКА • Возложить ПЕРСОНАЛЬНУЮ ответственность за обеспечение ИБ на руководителя
Порядок мониторинга со стороны ФСБ	• Обеспечить беспрепятственный доступ (в т.ч. удаленный) для сотрудников ФСБ к информационным ресурсам, доступ к которым обеспечивается через Интернет • Обеспечить незамедлительную реализацию мер (организационных и технических) по указанию ФСБ/ФСТЭК
Необходимость оценки уровня защищённости информационных ресурсов	• Для организаций, попавших в перечень ключевых (определяет Правительство РФ), до 1 июня 2022 осуществить мероприятия по оценке уровня защищённости ИР и предоставить доклад Правительству
Запрет использования средств защиты информации из недружественных стран	• С 1 января 2025 запрещено использовать СЗИ, страна происхождения которых числится в списке недружественных стран, либо производители которых находятся под юрисдикцией недружественных стран, подконтрольны или аффилированы с ними

Что нужно делать?

Что нужно сделать Вам – Заказчику

- Возложить ответственность за обеспечение ИБ на заместителя руководителя
- Возложить ПЕРСОНАЛЬНУЮ ответственность за обеспечение ИБ на руководителя

Чем Вам может быть полезна Cybersecurity Team

- Наша «Команда Кибербезопасности» является лицензиатом ФСТЭК в области технической защиты конфиденциальной безопасности, а следовательно, имеет право на оказание услуг по исполнению настоящих Указов
- Мы поможем обеспечить незамедлительную реализацию мер (разработать документацию, скорректировать настройки и параметры, изменить конфигурацию сети и многое другое)
- Решим задачу по запрету использования средств защиты информации из недружественных стран. Поможем спроектировать, закупить и внедрить подходящее ПО и оборудование

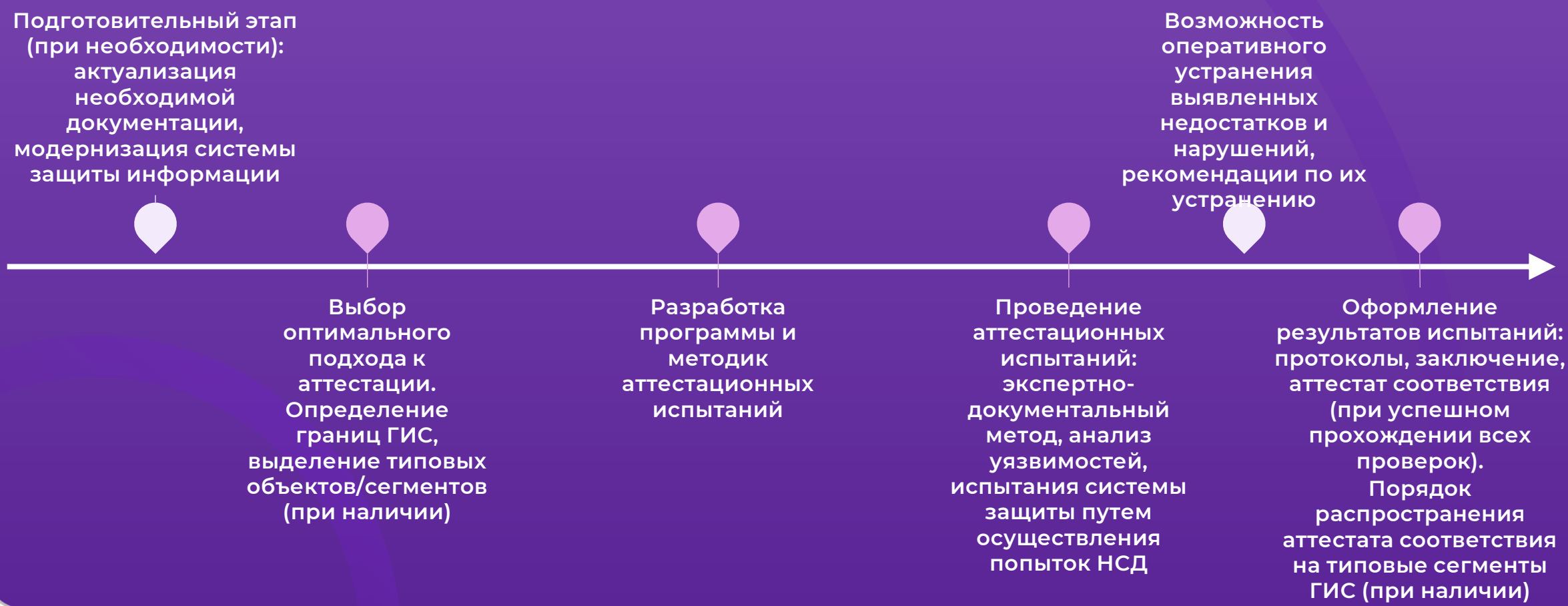
1. Сформировать план мероприятий по переходу на «дружественные СЗИ»
2. Оценить необходимость сопутствующих изменений в ИТ-инфраструктуре (например, нет СЗИ под используемую среду виртуализации) ЛИБО разработать компенсационные меры защиты
3. Реализовать необходимые организационные мероприятия (по созданию структурного подразделения, разработке приказов, выбора исполнителя работ по обеспечению ИБ)
4. Разработать план действий по оценке уровня защищенности ИР, «закрыть» существующие уязвимости, определить порядок проведения, форм ы отчётности и прочее

Защита государственных информационных систем

- Согласование со ФСТЭК и ФСБ Модели угроз безопасности информации и Частного технического задания на систему защиты
- Применение сертифицированных средств защиты информации (по уровням доверия)
- Выбор потенциала нарушителя исходя из класса защищенности ГИС
- Аттестация ЦОД, на базе которого функционирует ГИС, и (или) аттестация ГИС в составе общей инфраструктуры
- Периодический анализ угроз и уязвимостей
- Информирование и обучение персонала
- Периодический аудит, включая выявление и анализ уязвимостей (pen-тест)
- Необходимо применять маршрутизаторы, сертифицированные на соответствие требованиям по безопасности информации при подключении ГИС к Интернет

Аттестация государственных информационных систем

Мы предлагаем полный комплекс услуг по подготовке и сопровождению аттестации ГИС



CYBERSECURITY TEAM
КОМАНДА КИБЕРБЕЗОПАСНОСТИ

CYBERSECURITY TEAM
КОМАНДА КИБЕРБЕЗОПАСНОСТИ

Внедрение процессов управления безопасностью

Управление инцидентами

- Процессы регистрации, анализа, расследования инцидентов
- Процессы реагирования на компьютерные инциденты
- Аудиты безопасности
- Взаимодействие с ГосСОПКА
- SIEM и средства защиты от атак (весь спектр)

Обучение персонала

- Обязательное регулярное информирование и обучение персонала
- Создание организационной структуры по обеспечению безопасности КИИ (образование по ИБ) либо привлечение лицензиатов (ТЗКИ)
- Обязательное периодическое повышение квалификации

Обеспечение непрерывности

- Планы BCP (business continuity plan)
- Планы DRP (disaster recovery plan)
- Действия работников при возникновении инцидентов и внештатных ситуаций
- Резервирование, кластеризация, другие виды обеспечения доступности

Мы создаём системы кибербезопасности любой сложности

CYBERSECURITY TEAM
КОМАНДА КИБЕРБЕЗОПАСНОСТИ

Инструментальная защита ИТ-инфраструктуры

VPN/SSL
Антивирус
Контроль соответствия политикам безопасности
AntiDDoS
Безопасный DNS

Сегмент подключения

Граничные маршрутизаторы

Межсетевое экранирование
Обнаружение вторжений
Контроль приложений
Антиспам
URL фильтрация, Proxy
Ловушки (HoneyPot)
VPN/SSL VPN
Песочница и AntiAPT
Web Application Firewall

Внешний/внутренний периметр

Сетевое оборудование

AAA авторизация
Обнаружение аномалий на сетевом уровне
Контроль периферийных устройств

ЛВС

Контроль радиоэфира/
Обнаружение сторонних точек

БЛВС

Оборудование беспроводных сетей

Среда виртуализации

Гипервизоры

Межсетевое экранирование и обнаружение вторжений уровня гипервизора
Контроль целостности

Сегмент пользователей

Мобильные устройства

Рабочие станции

Mobile Device Management
Контроль подключаемых устройств
Контроль над утечками

Сегмент прикладных систем

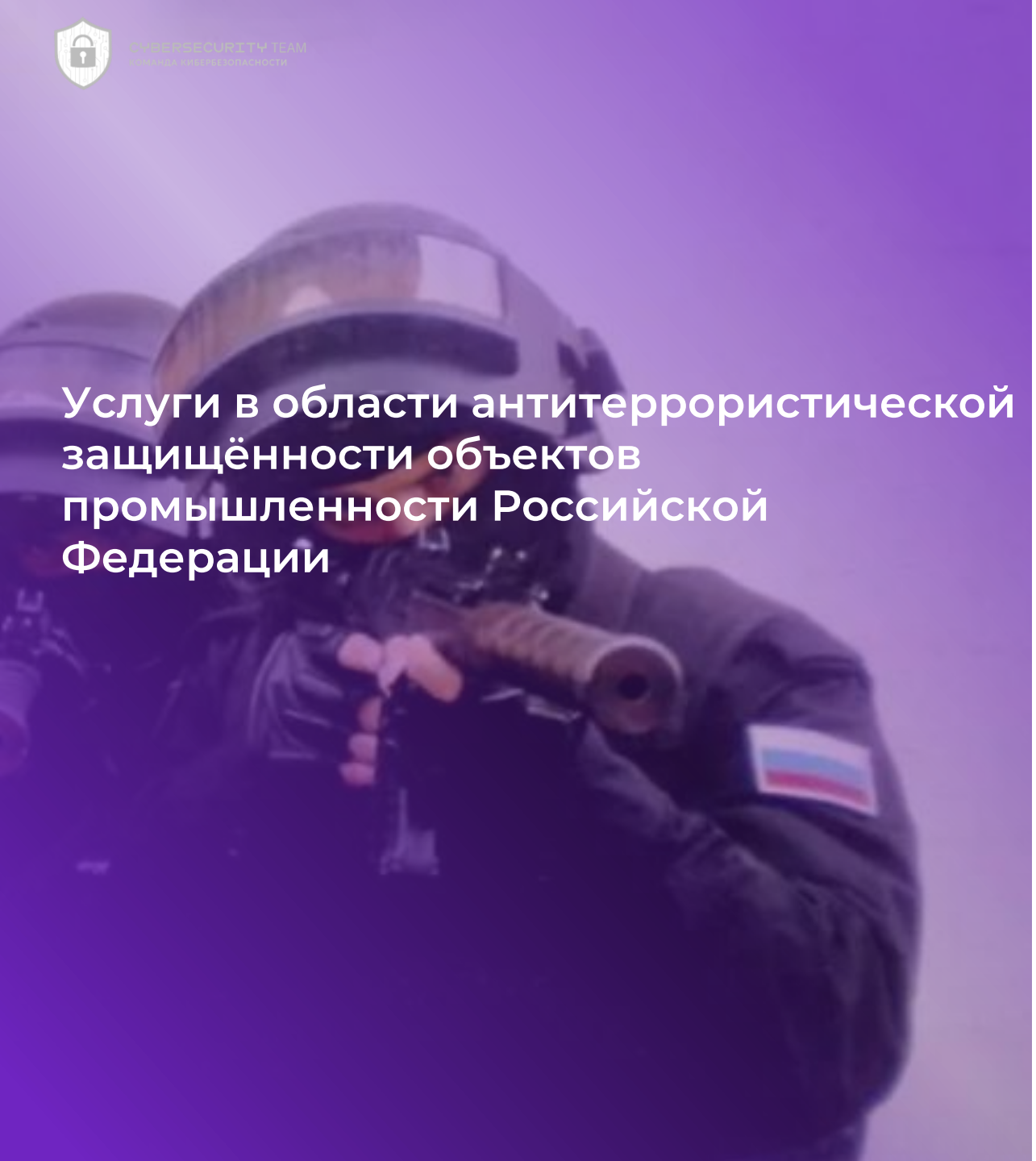
Серверное оборудование

Контроль программной среды
Межсетевое экранирование уровня баз данных

Сегмент технологических систем

АСУ ТП

Однонаправленное межсетевое взаимодействие
Контроль целостности
Инвентаризация компонентов



Услуги в области антитеррористической защищённости объектов промышленности Российской Федерации

Мы оказываем услуги по подготовке паспортов безопасности объектов (территорий) промышленности РФ, включенных в сводный перечень организаций оборонно-промышленного комплекса, утвержденный приказом Минпромторга России
от 12 октября 2022 г. № 4296

В соответствии с

- ФЗ-35 «О противодействии терроризму» от 06.03.2006
- Постановлением Правительства РФ №1413 «Об утверждении требований к антитеррористической защищённости объектов (территорий) промышленности и формы паспорта безопасности объекта (территории) промышленности

Услуги в сфере антитеррористической безопасности

CYBERSECURITY TEAM
КОМАНДА КИБЕРБЕЗОПАСНОСТИ

Виды услуг, оказываемые нами, в части подготовки паспортов безопасности объектов промышленности

Обследование

Обследование объекта (территории) промышленности, изучение документации, создание акта обследования

Категорирование

Создание специализированной комиссии и проведение категорирования объекта (территории) промышленности

Подготовка паспорта

Определение реализованных технических и организационных мер защиты объекта (территории), создание паспорта безопасности

Согласование паспорта безопасности с регуляторами: МЧС, ФСБ, Росгвардией
Передача согласованного паспорта в Минпромторг

Проектный опыт нашей команды

Структуры ООО «Газпром энергохолдинг»
Наши специалисты в течение нескольких лет оказывали услуги по техническому сопровождению и эксплуатации всей инфраструктуры кибербезопасности крупных компаний холдинга

Медиа
У нас богатый опыт работы с компаниями, производящими контент и осуществляющими теле- и радиовещание. Мы много лет помогаем им делать это безопасно

Федеральные органы исполнительной власти
Глобальный опыт в построении систем кибербезопасности федеральных масштабов для органов исполнительной власти

Промышленные холдинги
Опыт проектирования и реализации систем защиты технологических сегментов, АСУ ТП, консалтинг в сфере антитеррористической безопасности

Помогаем вам определить проблемные места в ИТ-инфраструктуре

Предлагаем методы решения, совместно выбираем наиболее подходящий

Реализуем проект и остаёмся с вами, помогая поддерживать и эксплуатировать

CYBERSECURITY TEAM
КОМАНДА КИБЕРБЕЗОПАСНОСТИ