



ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЗАДАЧА СО СРОКОМ «ВЧЕРА»

АНДРЕЙ ПЕТРЕНКО

КООРДИНАТОР КЛЮЧЕВЫХ ПРОЕКТОВ КОМПАНИИ НПЦ «КСБ»

ЧТО ПРОИСХОДИТ?

РОССИЯ. КИБЕРБЕЗОПАСНОСТЬ 2023 ГОД

10%

к числу инцидентов
к 2022 году

51%

инцидентов – утечки
конфиденциальной
информации

+24%

новых уязвимостей
к 2022 году
(+7000)

44%

инцидентов –
нарушение основной
деятельности
организаций

РОССИЯ. КИБЕРБЕЗОПАСНОСТЬ ОСОБЕННОСТИ 2023 ГОДА

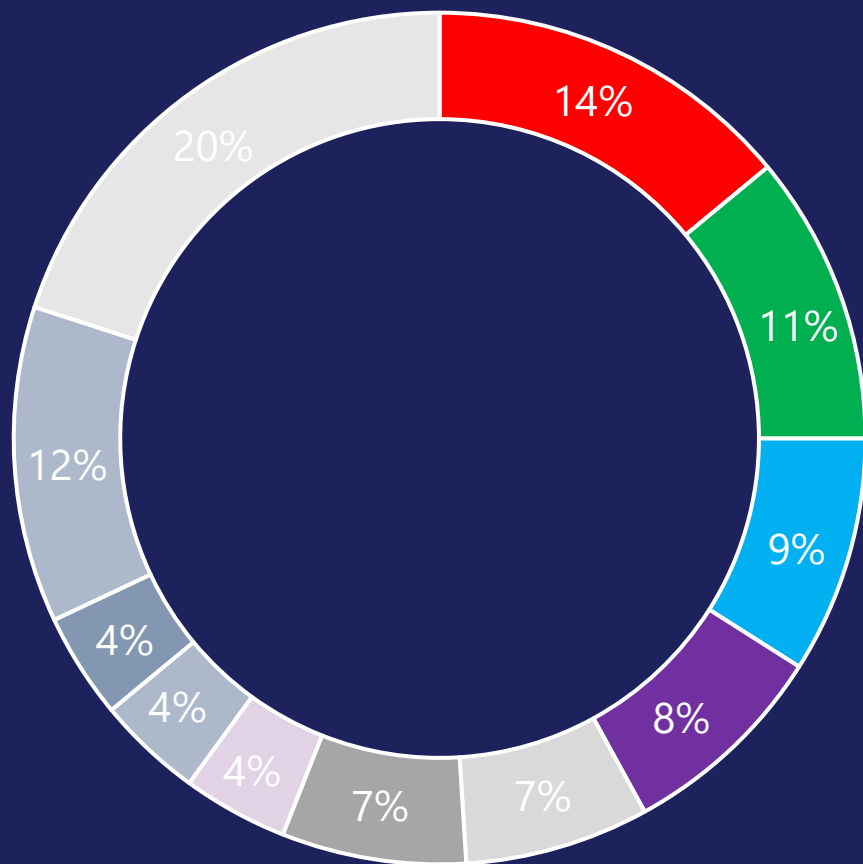
SEO poisoning

использовании поисковой
оптимизации (SEO) для опережения
выдачи незаконного домена
над законным

QR-фишинг

атакующие используют QR-коды,
чтобы обойти антиспам-фильтры
и другие средства защиты

НАПРАВЛЕНИЯ АТАК

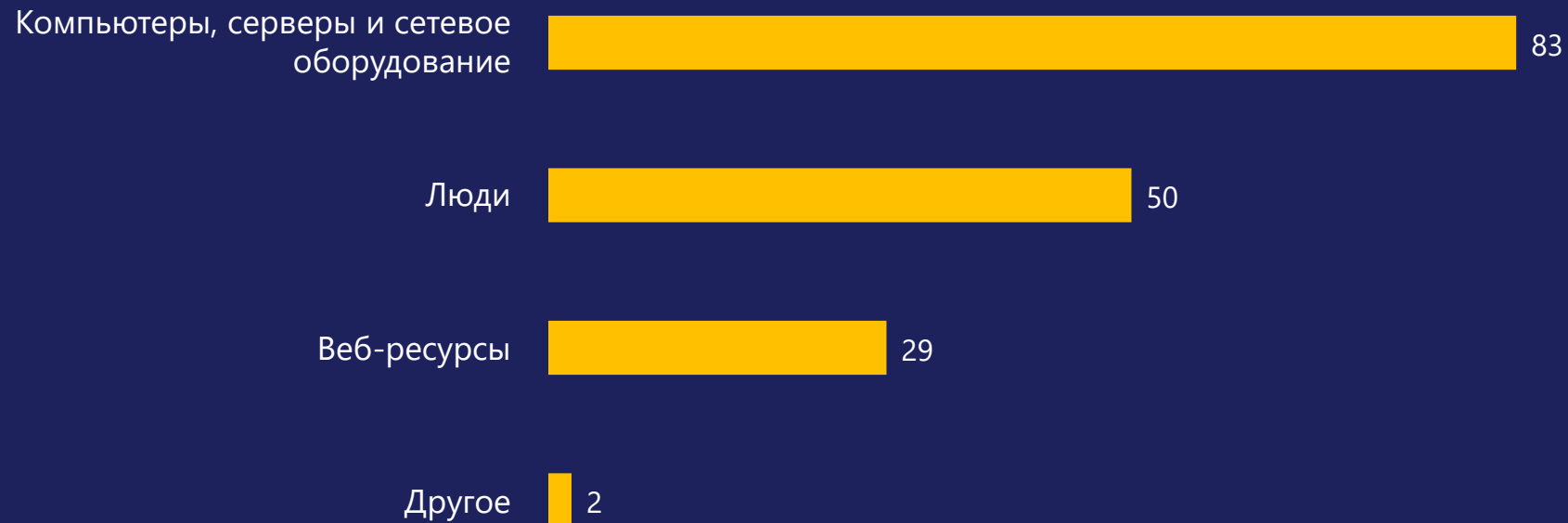


Категории жертв среди организаций

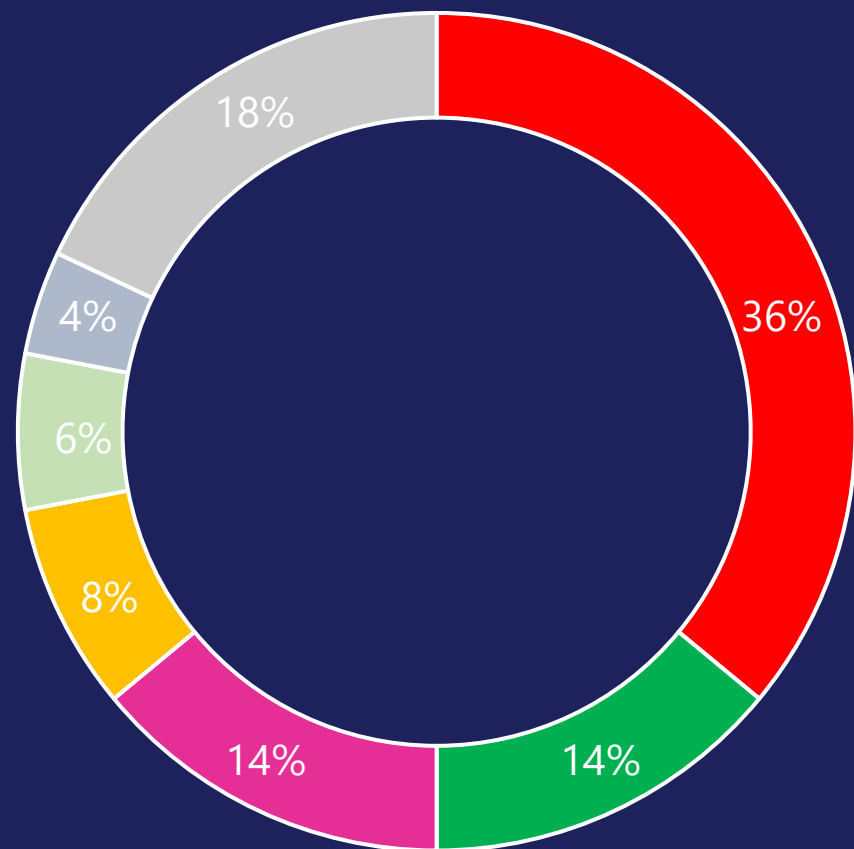
- Госучреждения
- Медицинские учреждения
- Наука и образование
- Финансовые организации
- Промышленность
- IT-компании
- Телекоммуникации
- Транспорт
- Торговля
- Другие
- Без привязки к отрасли

НАПРАВЛЕНИЯ АТАК

Объекты атак (доля атак)



ПОСЛЕДСТВИЯ АТАК



Какие данные утекают?

- Персональные данные
- Коммерческая тайна
- Учетные данные
- Медицинская информация
- Переписка
- Данные платежных карт
- Другая информация

РЕЗЮМЕ

Актуальный

тренд атак – веб-ресурсы
госучреждений

Люди

основная причина
инцидентов

Основная

цель – конфиденциальная
информация (ПДн, коммерческая
тайна, логины/пароли,
медицинская информация)

Главные

последствия – утечки
данных и нарушение
основной деятельности

Новые «фишки»

атаки на разработчиков ПО, SEO, QR

7000+

новых уязвимостей в 1 квартале 2023 года

ПОСТОЯННЫЕ ПРОБЛЕМЫ



МЕРЫ ПО ЗАЩИТЕ
ИНФОРМАЦИИ



ПОСТОЯННЫЕ
ИЗМЕНЕНИЯ



ФИНАНСЫ

ФСТЭК О КИИ

ПРОЦЕДУРУ ПЕРЕКАТЕГОРИРОВАНИЯ НЕОБХОДИМО ПРОЙТИ ВСЕМ СУБЪЕКТАМ КИИ

С АВГУСТА 2022 ГОДА

к мониторингу мер по защите информации в кии подключились государственные органы, в сферах деятельности которых субъекты кии осуществляют свою работу

18 ВЫЕЗДОВ

осуществил в 2022 году ФСТЭК России

БОЛЕЕ 70 ВЫЕЗДОВ

в 2023 году

С 21 МАРТА 2023 ГОДА

органы власти получили право разрабатывать и утверждать перечни типовых объектов КИИ в соответствующих сферах

> 700 ОРГАНИЗАЦИЙ

в различных сферах деятельности была дана оценка принимаемым мерам

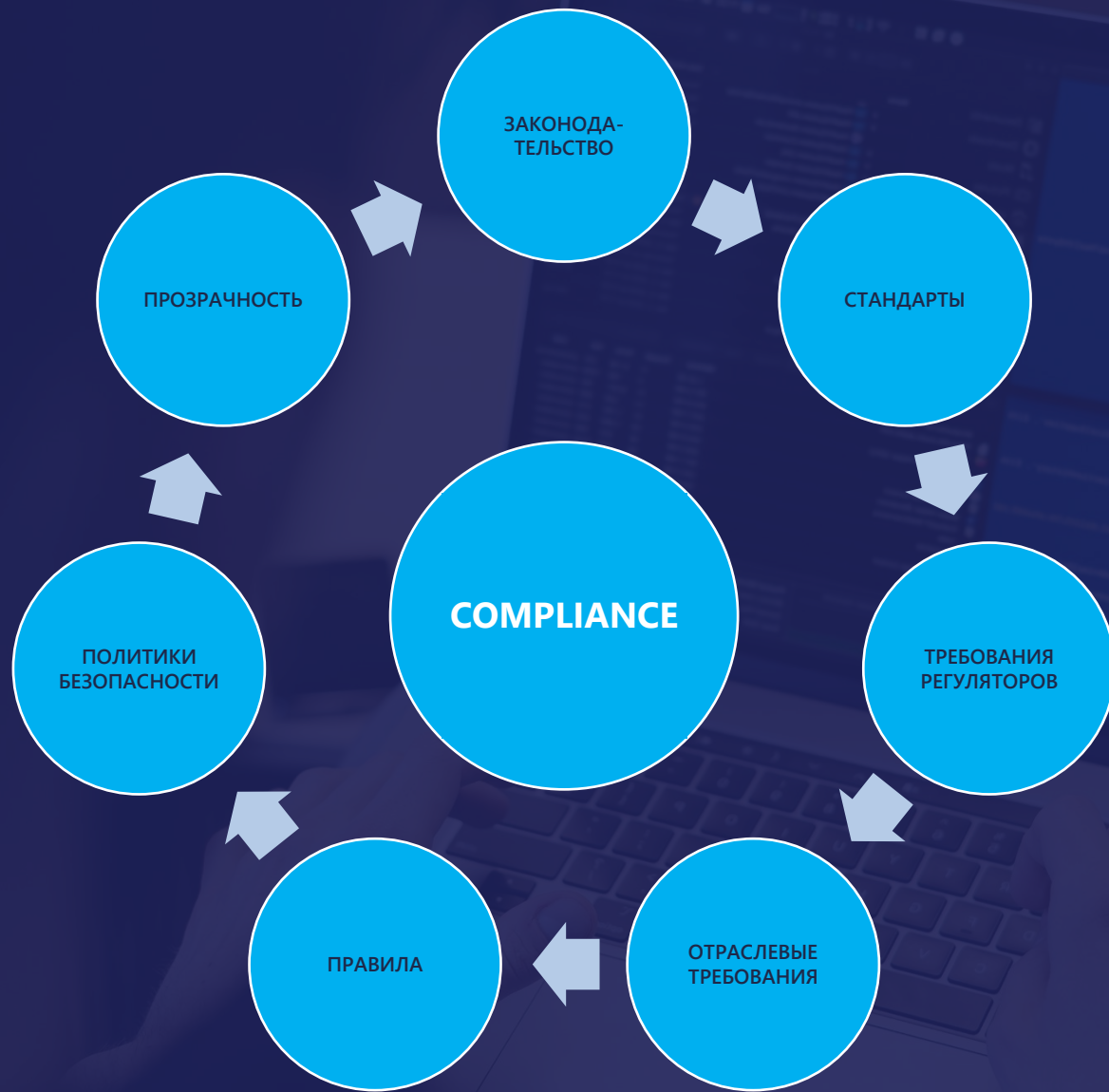
КИИ



ПЕРЕЧЕНЬ ТИПОВЫХ ОТРАСЛЕВЫХ ОБЪЕКТОВ
КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ,
ФУНКЦИОНИРУЮЩИХ В СФЕРЕ ЭНЕРГЕТИКИ



ПЕРЕЧЕНЬ ТИПОВЫХ ОТРАСЛЕВЫХ ОБЪЕКТОВ
КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ,
ФУНКЦИОНИРУЮЩИХ В СФЕРЕ ТРАНСПОРТА

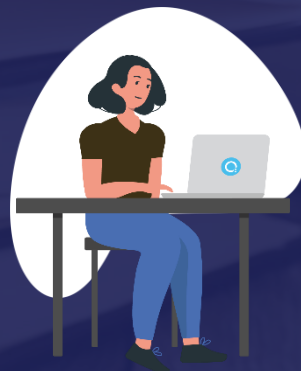




Учет информационных ресурсов (ИС/ГИС/ИСПДН) в регионе или сложных организационных структурах

Помогает не только учесть ИС, но и получить информацию о системах с подведомственных учреждений

- Автоматизация процесса сбора информации об ИС/ГИС и иных типов информационных систем
- Публикация сведений реестра ИС/ГИС на публичной части
- Формирование ИТ-ландшафта на основе сведений реестра



Внесение сведений

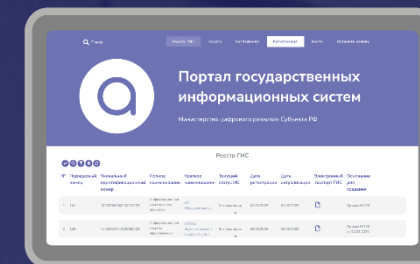


Формирование и отправка заявки



В случае соответствия – регистрация ИС, формирование электронного паспорта

В случае несоответствия – отправка мотивированного отказа.



Использование в организационных структурах



Автоматизация организационных мер по защите персональных данных, объектов критической информационной инфраструктуры и информации, обрабатываемой в государственных информационных системах

- Автоматическая разработка и актуализация комплекта документов по обработке и защите информации
- Формирование технической документации для построения системы защиты информации
- Мониторинг изменений и контроль защищенности информационных ресурсов



**Использование как «для себя»,
так и в организационных структурах**



Автоматизация процессов подключения пользователей к информационным системам и дальнейшего контроля выполнения ими предъявляемых требований

Помогает сформировать требования по подключению к ИС и транслировать их пользователям

- Регламентация доступа пользователей
- Автоматизация контроля подключения пользователей к информационным системам
- Снижение риска доступа нелегальных пользователей, а также доступа с незащищенных АРМ



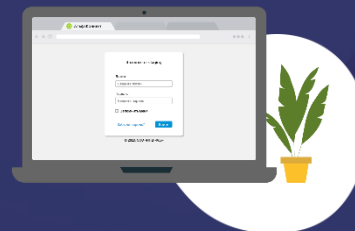
Оператор:

- Оцифровывает регламент подключения в графическом конструкторе
- Формирует требования паспортов АРМ
- Размещает услуги по подключению на портале



Заявитель:

- Регистрируется на портале
- Заполняет данные по выбранной услуге
- Подписывает сгенерированную заявку электронной подписью



Оператор:

- Рассматривает заявку на подключение
- Проверяет выполнение требований по подключению
- Принимает решение об одобрении либо отклонении заявки

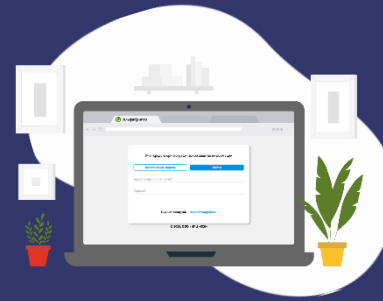
Использование в организационных структурах



Автоматизация выполнения требований законодательства по учету и выдаче СКЗИ

Причем как для организаций, занимающихся распространением СКЗИ, так и для внутреннего учета криптосредств

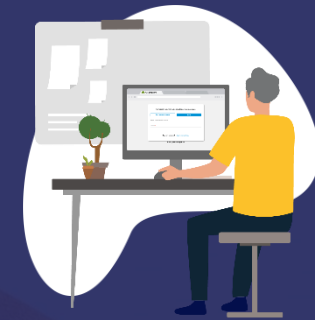
- Автоматизация процессов учета и выдачи СКЗИ
- Существенное снижение нагрузки на сотрудников
- Выполнение требований ФСБ России
- Создание единого портала по работе с криптосредствами



Создается портал предоставления услуг, связанных с СКЗИ



Заполнение заявки по заранее настроенному бизнес-процессу
Формирование всей необходимой информации для выдачи СКЗИ
Формирование всей необходимой сопроводительной документации



Электронная очередь

QR-код для быстрого и оперативного открытия заявки в системе

Автоматическая фиксация СКЗИ в личных кабинетах: в журналах учета (как на стороне лицензиата, так и пользователя), в лицевых счетах пользователей

**Использование как «для себя»,
так и в организационных структурах**



альфа|док

- Автоматическая разработка и актуализация комплекта документов по обработке и защите информации
- Формирование технической документации для построения системы защиты информации
- Мониторинг изменений и контроль защищенности информационных ресурсов

альфа|крипто

- Автоматизация процессов учета и выдачи СКЗИ
- Существенное снижение нагрузки на сотрудников
- Выполнение требований ФСБ России
- Создание единого портала по работе с криптосредствами

альфа|коннект

- Регламентация доступа пользователей
- Автоматизация контроля подключения пользователей к информационным системам
- Снижение риска доступа нелегальных пользователей, а также доступа с незащищенных АРМ

альфа|реестр

- Автоматизация процесса сбора информации об ИС/ГИС и иных типов информационных систем
- Публикация сведений реестра ИС/ГИС на публичной части
- Формирование ИТ-ландшафта на основе сведений реестра ГИС

Единая точка входа
во все приложения

Возможность интеграции
благодаря поддержке
открытых протоколов

Отсутствие необходимости
установки дополнительного ПО



Управление учётными
данными и доступом
к информационным системам

Доверие к результатам
идентификации
и аутентификации

Двухфакторная аутентификация

СООТВЕТСТВИЕ ТРЕБОВАНИЯМ

№17

ПРИКАЗ
ФСТЭК РОССИИ
от 11.02.2013

№21

ПРИКАЗ
ФСТЭК РОССИИ
от 18.02.2013

№31

ПРИКАЗ
ФСТЭК РОССИИ
от 14.03.2014

№239

ПРИКАЗ
ФСТЭК РОССИИ
от 25.12.2017



S O C
R A T

SECURITY
OPERATION
CENTER
RUSSIAN
ANALYTICS
TEAM

Мониторинг инцидентов ИБ
в режиме 24/7

Индивидуальный подход к потребностям компании

Вариативность при подключении
к Центру мониторинга

Доступность по цене

ПРОЕКТЫ В СФЕРЕ РЕГИОНАЛЬНОГО ЗДРАВООХРАНЕНИЯ

- Республика Бурятия **11**
- Республика Хакасия **1**
- Красноярский край **116**
- Ставропольский край **1**
- Архангельская область **63**
- Брянская область **61**
- Владимирская область **82**
- Вологодская область **31**
- Орловская область **1**
- Сахалинская область **48**
- Ульяновская область **1**
- Город Севастополь **19**
- Ямало-Ненецкий автономный округ **29**



ОСТАЛИСЬ ВОПРОСЫ?

info@npc-ksb.ru

8 800 500 52 33

ПРОТЕСТИРУЙТЕ БЕСПЛАТНО

НА ALFA-DOC.RU

ЗАКАЖИТЕ ПИЛОТНЫЙ ПРОЕКТ

НА ВАШИХ МОЩНОСТЯХ



<https://t.me/alfaecosystem>