РЕГИОНАЛЬНЫЙ ЦЕНТР КИБЕРБЕЗОПАСНОСТИ

ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СВЯЗИ САМАРСКОЙ ОБЛАСТИ

Ведомственный центр ГосСОПКА Сложности построения и возможности развития

АКИМОВ МАКСИМ ОЛЕГОВИЧ

Начальник управления информационной безопасности ГКУ СО «РЦУП»

+7 846 200 09 32
+7 987 436 06 34
m.akimov@rcu.samregion.ru

ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СВЯЗИ САМАРСКОЙ ОБЛАСТИ

ЦЕНТР ОБНАРУЖЕНИЯ, ПРЕДУПРЕЖДЕНИЯ И ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ КОМПЬЮТЕРНЫХ АТАК НА ИНФОРМАЦИОННЫЕ СИСТЕМЫ И РЕСУРСЫ САМАРСКОЙ ОБЛАСТИ

РЕГИОНАЛЬНЫЙ ЦЕНТР КИБЕРБЕЗОПАСНОСТИ

Центр создан в 2015 году постановлением Правительства Самарской области от 20.11.2015 № 745

ГОССОПКА

Осуществлено подключение к ГосСОПКА в рамках пилотного взаимодействия

НКЦКИ

Заключено соглашение от 28.08.2019 между НКЦКИ и Правительством Самарской области о взаимодействии в области обнаружения, предупреждения и ликвидации последствий компьютерных атак

Взаимодействие с УФСБ по Самарской области в рамках оперативной деятельности

Подписаны соглашения о взаимодействии:

БАНК РОССИИ ФИНЦЕРТ

Ростелеком Солар

ГКУ «ЦИТ» г.Оренбург

ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
И СВЯЗИ САМАРСКОЙ ОБЛАСТИ

ОБЩАЯ СТРУКТУРА КОМАНДЫ ЦЕНТРА

13 чел.

общая численность команды

Руководитель центра - 3 линия:

- Главный аналитик (анализ информации от 1 и 2 линии; выявление, анализ и прогнозирование угроз)
- Методолог (нормативно-правовое и методическое сопровождение)

Специалисты 2 линии:

- Специалист по оценке защищенности (pentesting)
- Специалист по администрированию систем защиты (operations)
- Аналитик (расследование кибератак)

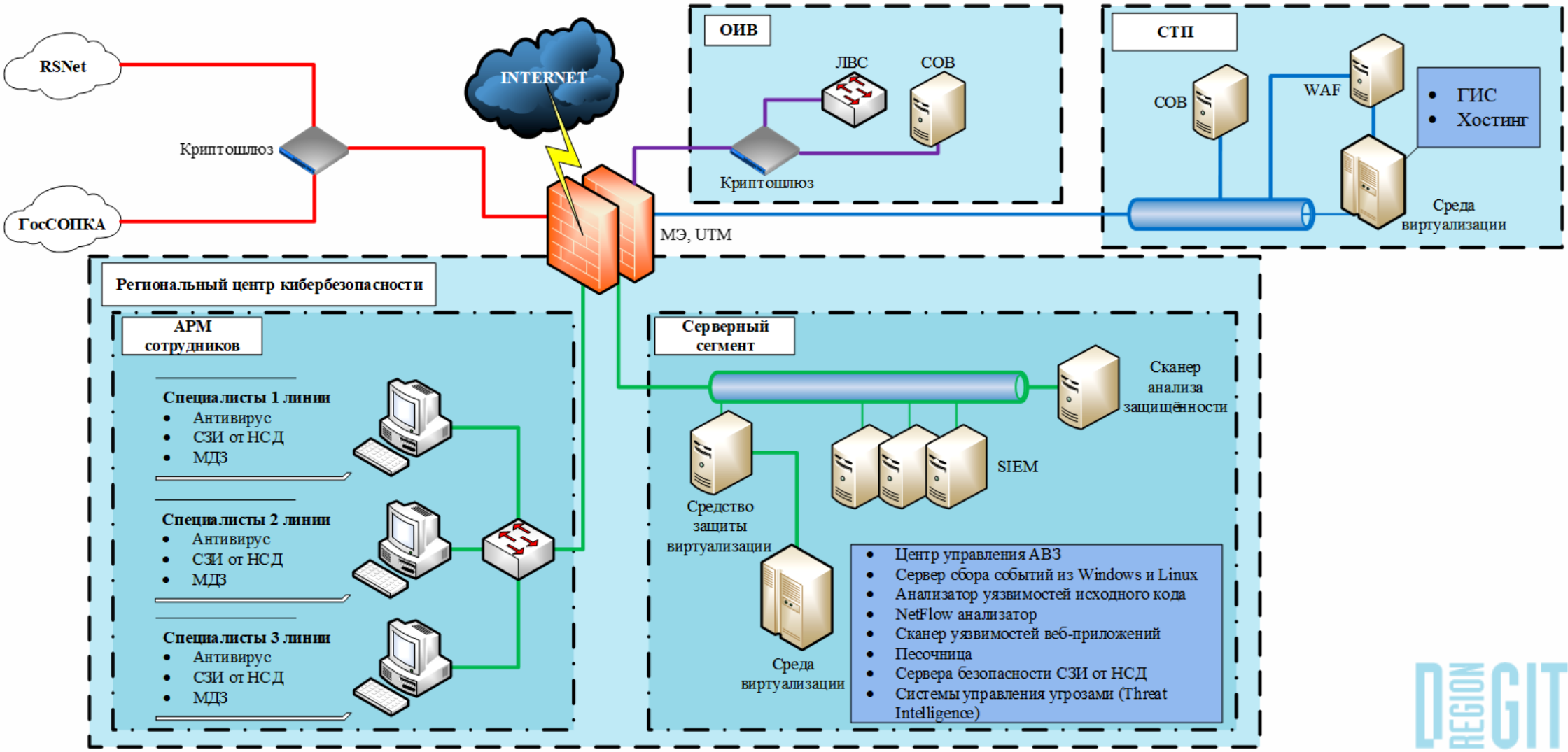
Специалисты 1 линии (режим работы 24x7):

- Главный инженер по мониторингу инцидентов
- Ведущий инженер по мониторингу инцидентов

DIGITAL REGION

ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
И СВЯЗИ САМАРСКОЙ ОБЛАСТИ

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ЦЕНТРА



REGION DIGITAL

ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
И СВЯЗИ САМАРСКОЙ ОБЛАСТИ

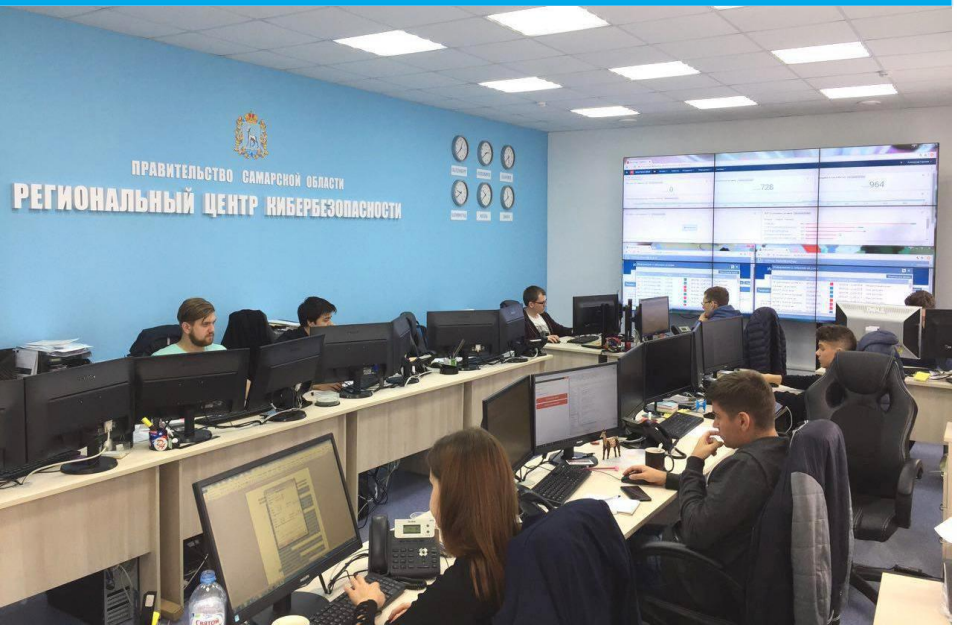
ОСНОВНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ЦЕНТРА

- Средства (системы) контроля (анализа) защищенности информационных систем:
  - Сетевой сканер
  - Сканер веб-приложений
  - Анализатор исходного кода
- Замкнутая среда предварительного выполнения программ («песочница»)
- Средства управления информацией об угрозах безопасности информации (Threat Intelligence)
- Средства управления событиями и инцидентами информационной безопасности (SIEM)
- Системы обнаружения и предотвращения вторжений (IDS, IPS)
- Средства защиты каналов передачи данных (СКЗИ)
- Универсальный шлюз безопасности (UTM)
- Средства антивирусной защиты
- СЗИ от НСД

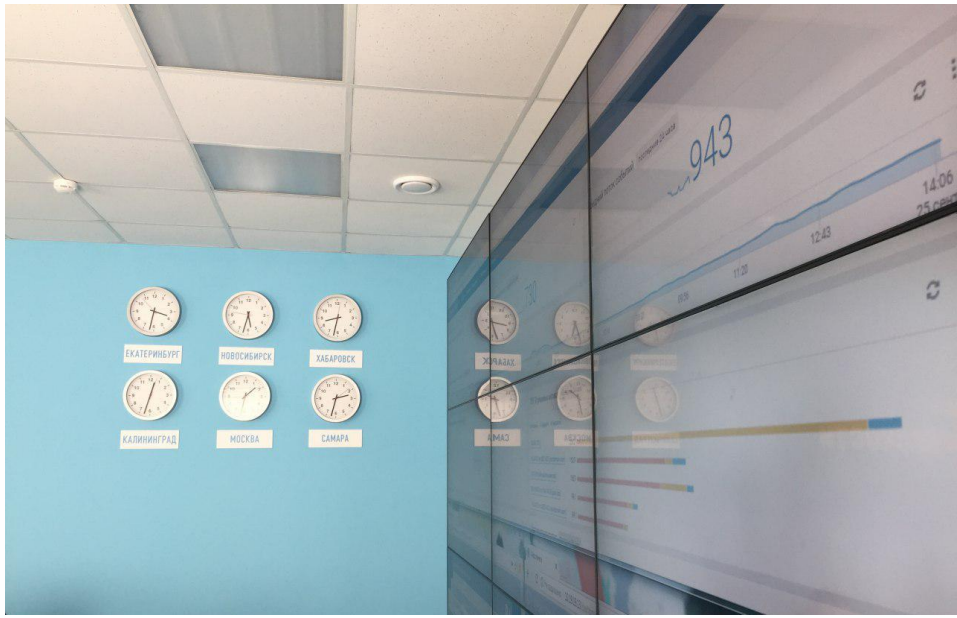
REGION DIGITAL

ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
И СВЯЗИ САМАРСКОЙ ОБЛАСТИ

РЕЗУЛЬТАТЫ РАБОТЫ ЦЕНТРА ЗА 2018 ГОД



РЕГИОНАЛЬНЫЙ ЦЕНТР КИБЕРБЕЗОПАСНОСТИ



Отработано в 2018 году

400
Тысяч событий ИБ высокого уровня критичности

>5
Миллионов событий информационной безопасности

Отработано в период ЧМ-2018

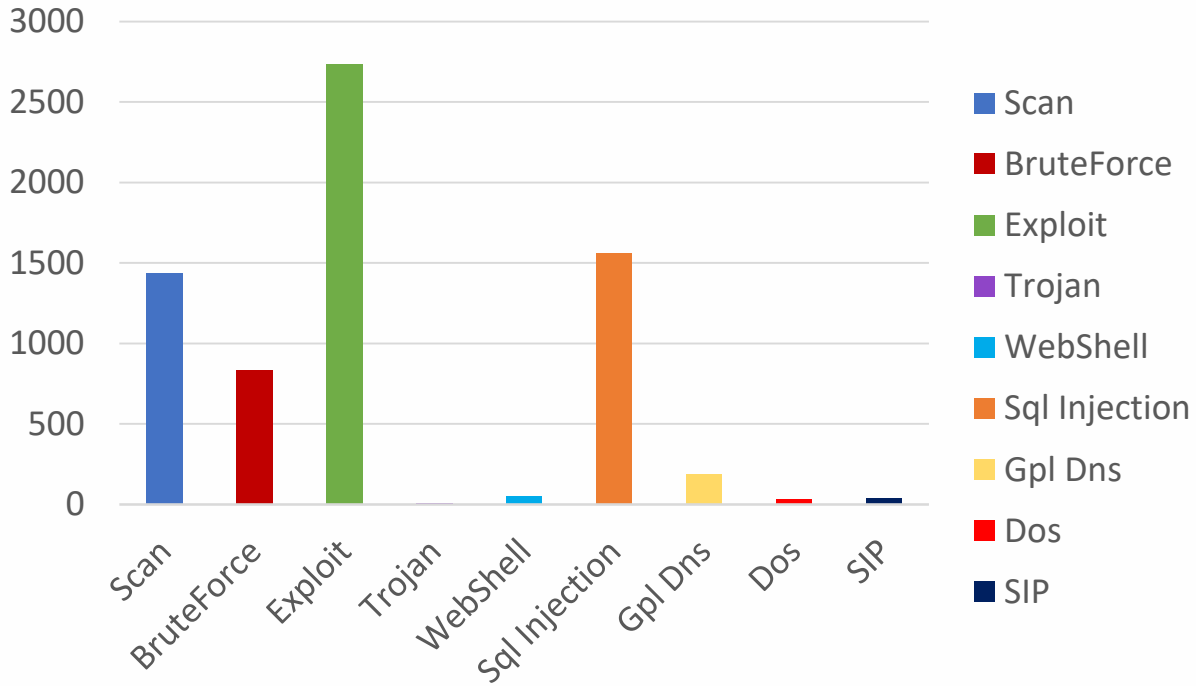
72
Инцидентов информационной безопасности

>3
Миллионов событий информационной безопасности

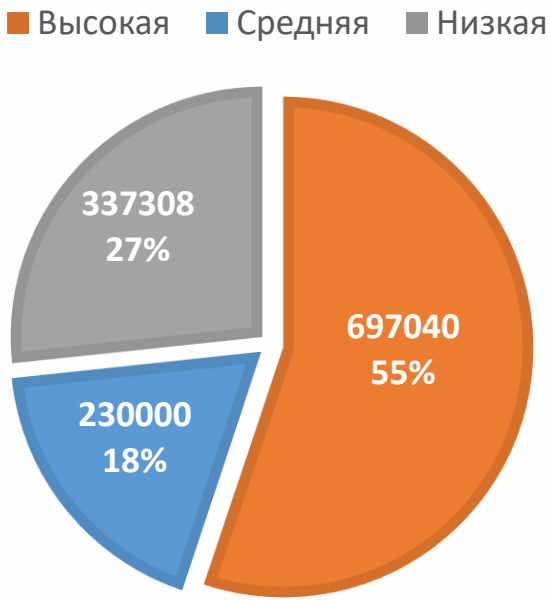
ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
И СВЯЗИ САМАРСКОЙ ОБЛАСТИ

РЕЗУЛЬТАТЫ РАБОТЫ ЦЕНТРА ЗА 2019 ГОД

СТАТИСТИКА ПО ЗАКРЫТЫМ ИНЦИДЕНТАМ



СОБЫТИЯ ПО УРОВНЮ КРИТИЧНОСТИ



Всего закрыто ~ 7 000 инцидентов ИБ

Заблокировано более 13 000 IP-адресов

REGION DIGITAL

ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
И СВЯЗИ САМАРСКОЙ ОБЛАСТИ

СТАТИСТИКА УЯЗВИМОСТЕЙ WEB-ПРИЛОЖЕНИЙ

1234

Высокий уровень критичности уязвимости

High Severity Vulnerabilities

22603

Средний уровень критичности уязвимости

Medium Severity Vulnerabilities

8039

Низкий уровень критичности уязвимости

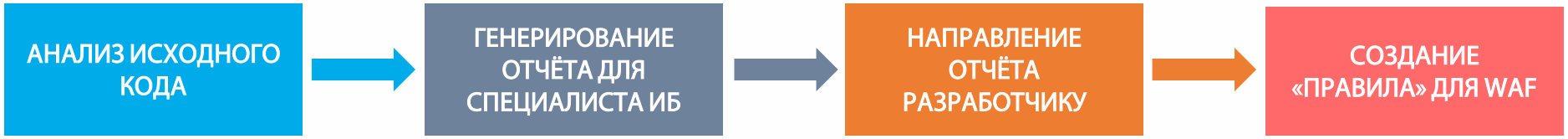
Low Severity Vulnerabilities

За текущий год просканировано более 235 web-приложений (сайты, порталы) на угрозы ИБ

DIGITAL REGION

ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
И СВЯЗИ САМАРСКОЙ ОБЛАСТИ

АНАЛИЗ УЯЗВИМОСТЕЙ ИСХОДНОГО КОДА



Пример найденной уязвимости:

Код:

```
77 // todo ДИЧАЙЩИЙ КАСТЫЛЬ ПРАВИТЬ !!!
78 export const getAccessToken = (username, password) => dispatch => {
79   axios({
80     method: "post",
81     url: "/oauth/token",

82     auth: { username: "my-trusted-client", password: "secret" },

83     headers: {
84       "Content-type": "application/x-www-form-urlencoded; charset=utf-8"
85     },
86     params: {
```

REGION DIGITAL

ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СВЯЗИ САМАРСКОЙ ОБЛАСТИ

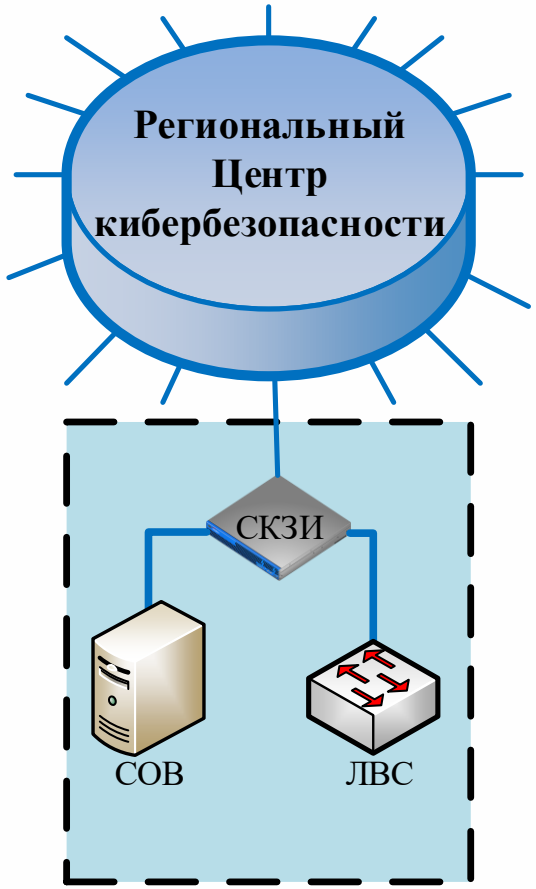
ПЛАНЫ РАЗВИТИЯ, РАСШИРЕНИЕ КРУГА ЗАДАЧ

- Сканирование исходного кода на наличие уязвимостей
- Подключение ИС к WAF в разрыв
- Размещение ресурсов ОИВ (ГИС, ИСПДн, серверные мощности) в ЦОД Центра
- Централизованное управление средствами защиты ОИВ, операторов ГИС
- Размещение IDS в ОИВ, подключение к мониторингу ИБ
- Введение единой политики информационной безопасности в Правительстве Самарской области во главе с центром компетенции – Региональным Центром Кибербезопасности
- Закрепление специалиста ИБ Центра за ОИВ
- Проведение контроля выполнения требований ИБ на ресурсах в зоне ответственности Правительства Самарской области
- Коммерческая деятельность

REGION DIGITAL

ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
И СВЯЗИ САМАРСКОЙ ОБЛАСТИ

СХЕМА ПОДКЛЮЧЕНИЯ К ЦЕНТРУ

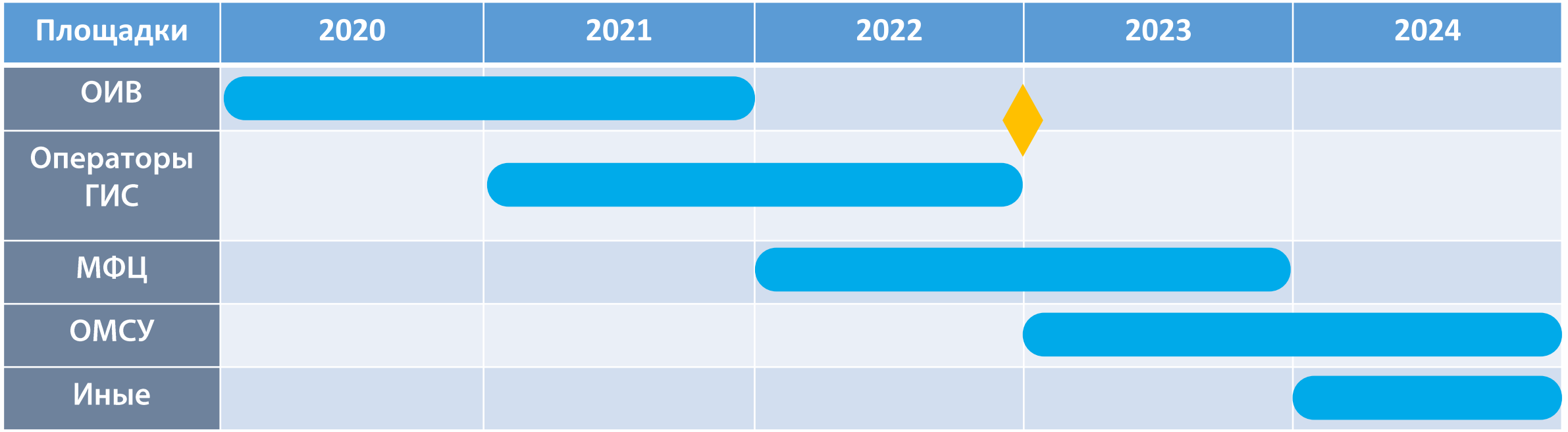


- Заключение соглашения
- Утверждение схемы подключения
- Определение ресурсов и объектов защиты
- Определение степени критичности
- Категорирование объектов (при необходимости)
- Определение сроков реагирования (SLA)
- Разграничение зоны ответственности

REGION DIGITAL

ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
И СВЯЗИ САМАРСКОЙ ОБЛАСТИ

ПЛАН ПОДКЛЮЧЕНИЯ К ЦЕНТРУ



REGION DIGITAL

ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
И СВЯЗИ САМАРСКОЙ ОБЛАСТИ

ПРОБЛЕМАТИКА

- **Кейс № 1.** Кадры
- **Кейс № 2.** Средства защиты информации
- **Кейс № 3.** Финансирование
- **Кейс № 4.** Нормативно-правовое регулирование

REGION DIGITAL

ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
И СВЯЗИ САМАРСКОЙ ОБЛАСТИ

ШТАТНАЯ ЧИСЛЕННОСТЬ

- Фактически постоянно работающий состав Центра составляет **7** единиц
- По рекомендации опытных специалистов SOC - состав центра должен быть не менее **27** единиц*
- Для мониторинга ИБ большей части ресурсов Правительства Самарской области требуется не менее **34** специалистов 1, 2 и 3 линий

*https://www.anti-malware.ru/practice/methods/optimal-gossopka-team-line-up

REGION DIGITAL

ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
И СВЯЗИ САМАРСКОЙ ОБЛАСТИ

ПОДГОТОВКА КАДРОВ. ОБРАЗОВАНИЕ

- Слабая подготовка кадров в ВУЗ
- В учебных программах не предусмотрены, либо слабо раскрыты курсы по темам:
  - SOC
  - ГосСОПКА
  - КИИ
  - Защита АСУ ТП
- Навыки проведения различных видов сетевых атак отсутствуют
- Абстрактные знания без практического применения
- Программы быстро устаревают
- Курсы повышения квалификации не согласованы со ФСТЭК, ФСБ
- Специалисты-самоучки
- Бакалавры-магистры

REGION DIGITAL

ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
И СВЯЗИ САМАРСКОЙ ОБЛАСТИ

ТРЕБОВАНИЯ К ДОЛЖНОСТНЫМ ЛИЦАМ ЦЕНТРА ГОССОПКА

СТАЖ

Требования НКЦКИ к Ведомственному центру

- Руководитель Центра – не менее **5 лет**
- Специалисты 3 линии – не менее **5 лет**
- Специалисты 2 линии – не менее **3 лет**
- Специалисты 1 линии – не менее **3 лет** в области ИБ, либо профильное образование ИБ

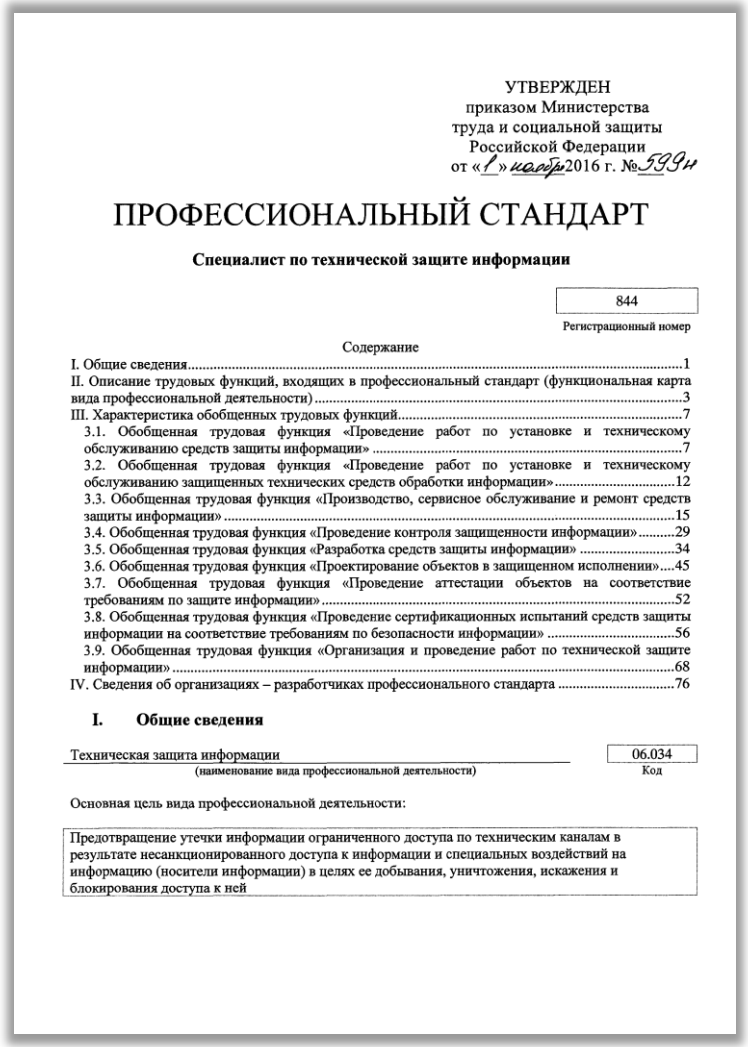
Требования ПП № 79 для лицензии по мониторингу

- Руководитель – не менее **5 лет**
- Инженер – не менее **3 лет** – 2 единицы

REGION DIGITAL

ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
И СВЯЗИ САМАРСКОЙ ОБЛАСТИ

ПРОФСТАНДАРТЫ



УТВЕРЖДЕН
приказом Министерства
труда и социальной защиты
Российской Федерации
от «1» марта 2016 г. №599н

ПРОФЕССИОНАЛЬНЫЙ СТАНДАРТ

Специалист по технической защите информации

844
Регистрационный номер

Содержание

I. Общие сведения

Техническая защита информации — 06.034
(наименование вида профессиональной деятельности) — Код

Основная цель вида профессиональной деятельности:

Предотвращение утечки информации ограниченного доступа по техническим каналам в результате несанкционированного доступа к информации и специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней

Обязательны к применению с 1 января 2020 года в госучреждениях!

- **06.030** Специалист по защите информации в телекоммуникационных системах и сетях
- **06.031** Специалист по автоматизации информационно-аналитической деятельности в сфере безопасности
- **06.032** Специалист по безопасности компьютерных систем и сетей
- **06.033** Специалист по защите информации автоматизированных систем
- **06.034** Специалист по технической защите информации

Статья 5.27 КоАП РФ. Штрафы за нарушение:
1 000 – 5 000 руб. – должностные лица
30 000 – 50 000 руб. – юридические лица

REGION DIGITAL

ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
И СВЯЗИ САМАРСКОЙ ОБЛАСТИ

ЗАРАБОТНАЯ ПЛАТА

Аналитик по информационной безопасности

з/п не указана

Требуемый опыт работы: 5 лет
Полная занятость

Чем предстоит заниматься:

Разработка отчетов (подробных технических - для специалистов службы ИБ, и кратких аналитических – для руководства) по результатам работы:

- Тестирование на проникновение
- Анализ защищенности веб- и мобильных приложений
- Анализ исходного кода приложения
- Анализ уязвимости сети

Требование к кандидату:

- Высшее профессиональное образование (по направлению «Информационная безопасность»)
- Знание современных угроз ИБ и уязвимостей веб-приложений
- Знание технологий и средств защиты информации (MDM, SIEM, 2FA, EDR, AV, IDP, TDS/APT, Network security, Vulnerability Management)
- Опыт проведения расследований ИБ
- Опыт написания sql-запросов, скриптов
- Опыт программирования на популярных языках
- Грамотная письменная и устная речь
- Знание английского языка
- Наличие сертификатов в области ИБ
- И т.д…..

REGION DIGITAL

ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
И СВЯЗИ САМАРСКОЙ ОБЛАСТИ

ЗАРАБОТНАЯ ПЛАТА

Оклады (тарифная ставка):

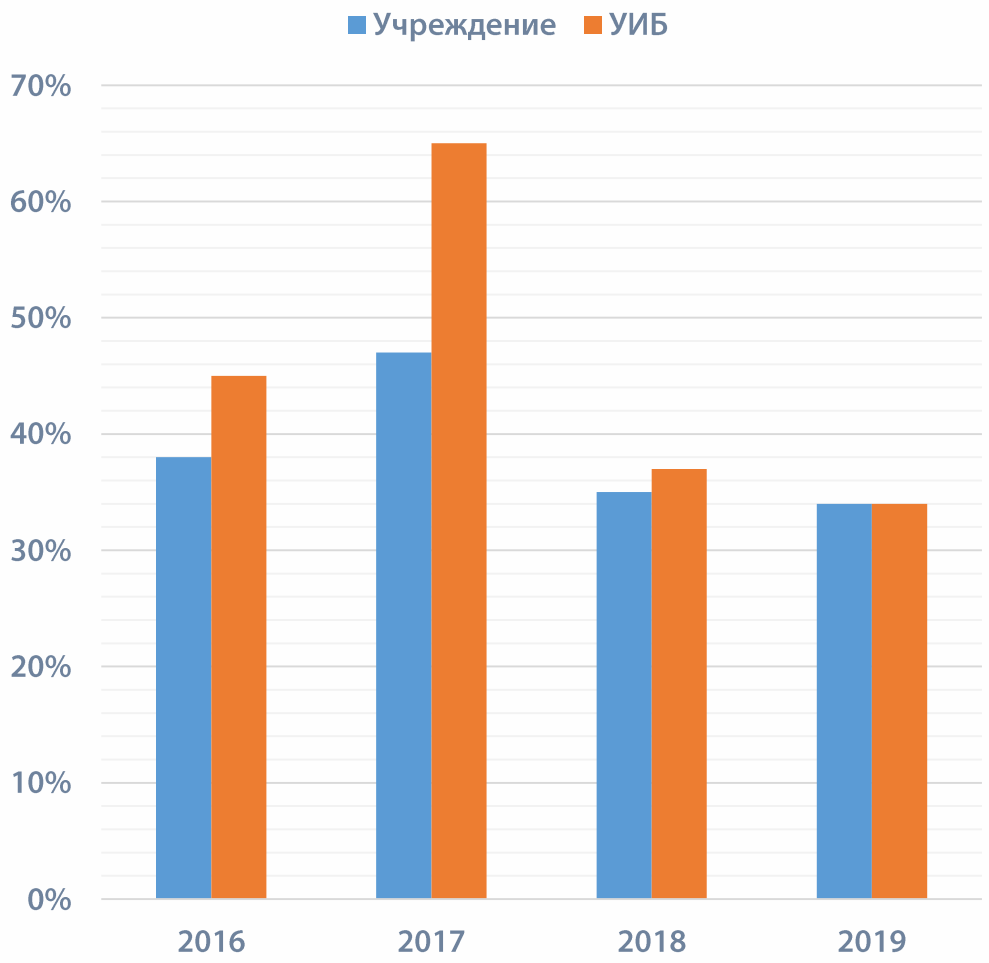
- Начальник управления информационной безопасности:
  19 934
- Руководитель группы мониторинга и анализа защищенности информационных систем:
  18 693
- Главный инженер по защите информации:
  15 283
- Ведущий инженер по защите информации:
  13 439
- Инженер по защите информации 1 категории:
  11 620

Низкий уровень заработной платы –
является угрозой информационной безопасности!

DIGITAL REGION

ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
И СВЯЗИ САМАРСКОЙ ОБЛАСТИ

ТЕКУЧЕСТЬ КАДРОВ



Текучесть по Учреждению:

- 2016 - 38%
- 2017 - 47%
- 2018 - 35%
- 2019 - 34%

Текучесть по Управлению информационной безопасности:

- 2016 - 45%
- 2017 - 65%
- 2018 - 37%
- 2019 - 34%

DIGITAL REGION

ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
И СВЯЗИ САМАРСКОЙ ОБЛАСТИ

СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ. СЛОЖНОСТЬ НАСТРОЙКИ, ЭКСПЛУАТАЦИИ

- Система сбора и корреляции событий информационной безопасности (SIEM)
- Анализатор уязвимостей исходного кода
- Межсетевой экран уровня приложений (WAF)

- Платформа реагирования на инциденты (Incident Response Platform)
- Средства управления информацией об угрозах безопасности информации (Threat Intelligence)
- Защите конечных точек от сложных угроз (EPP, EDR)

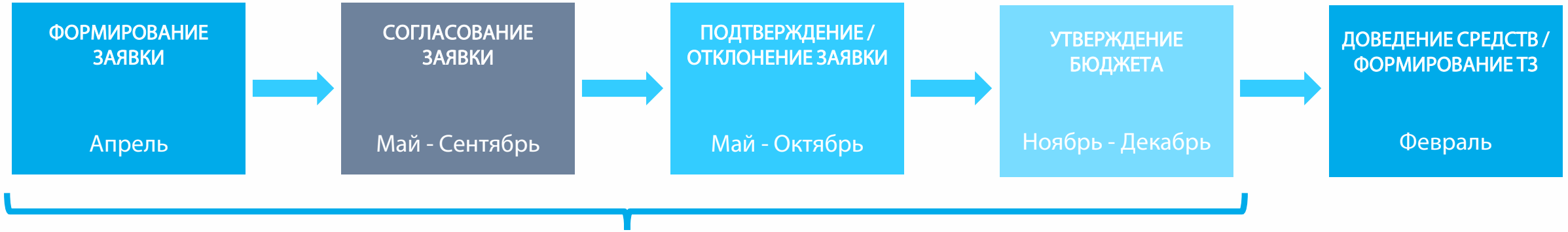
- Контроль изменения конфигураций сетевой инфраструктуры
- Антивирусная защита уровня виртуальной среды (гипервизора)
- Система защиты баз данных / Система аудита и блокировки сетевого доступа к базам данных
- DLP ^_^

REGION DIGITAL

ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СВЯЗИ САМАРСКОЙ ОБЛАСТИ

ФИНАНСИРОВАНИЕ

- Долгий процесс выделения средств и формирования закупки
- Риск увеличение стоимости закупки
- Непонимание со стороны Минфина
- Появление новых потребностей

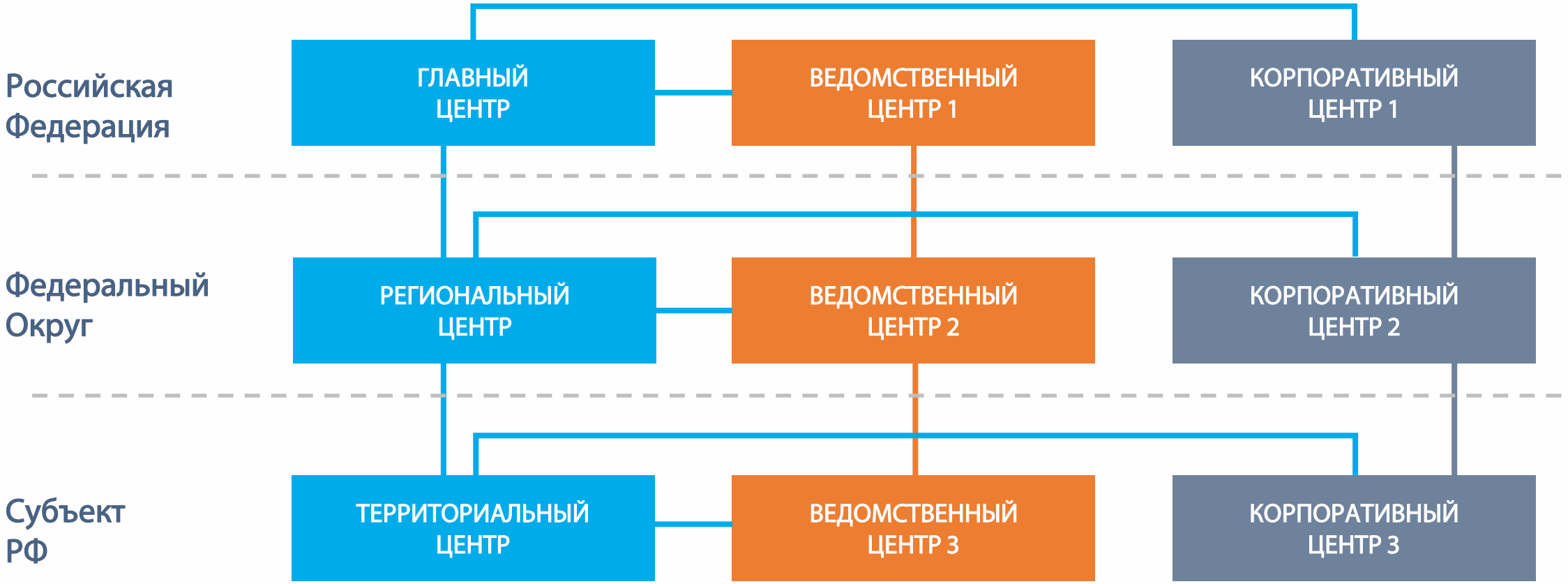


9 МЕСЯЦЕВ

DIGITAL REGION

ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
И СВЯЗИ САМАРСКОЙ ОБЛАСТИ

ВЕДОМСТВЕННЫЙ ЦЕНТР КАК ЧАСТЬ ГОССОПКА



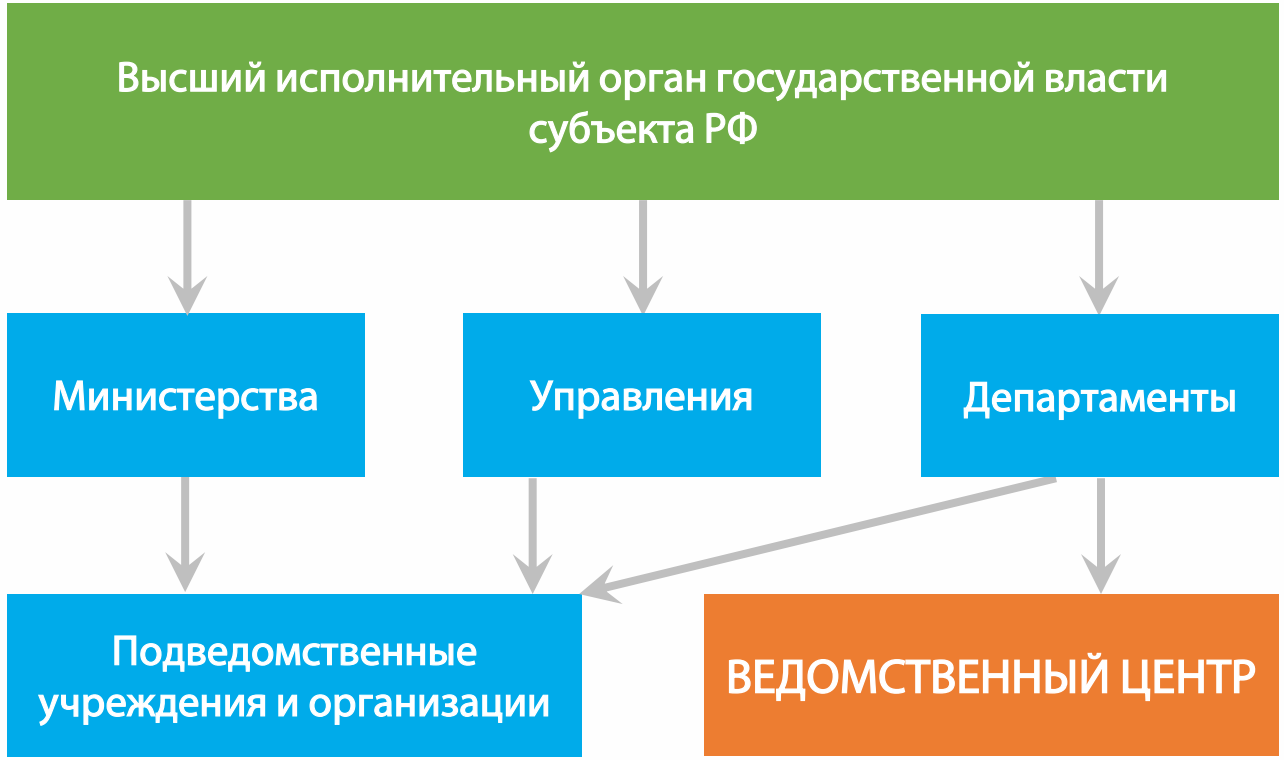
DIGITAL REGION

ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
И СВЯЗИ САМАРСКОЙ ОБЛАСТИ

ВЕДОМСТВЕННЫЙ ЦЕНТР В СТРУКТУРЕ СУБЪЕКТА РФ

Законодательный (представительный) орган государственной власти субъекта РФ

Органы местного самоуправления муниципальных образований субъекта



DIGITAL REGION

ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
И СВЯЗИ САМАРСКОЙ ОБЛАСТИ

НПА. ПОЛНОМОЧИЯ ЦЕНТРА. ОТВЕТСТВЕННОСТЬ СОТРУДНИКОВ

Необходима разработка на федеральном, а затем на региональном уровне нормативных правовых актов устанавливающих :

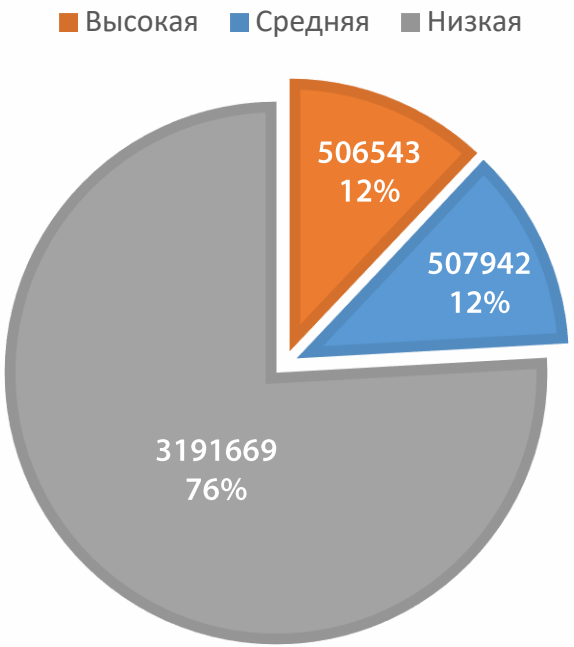
- статус Ведомственного центра
- права Ведомственного центра в сфере ИБ
- обязанности органов и организаций выполнять требования Ведомственного центра

DIGITAL REGION

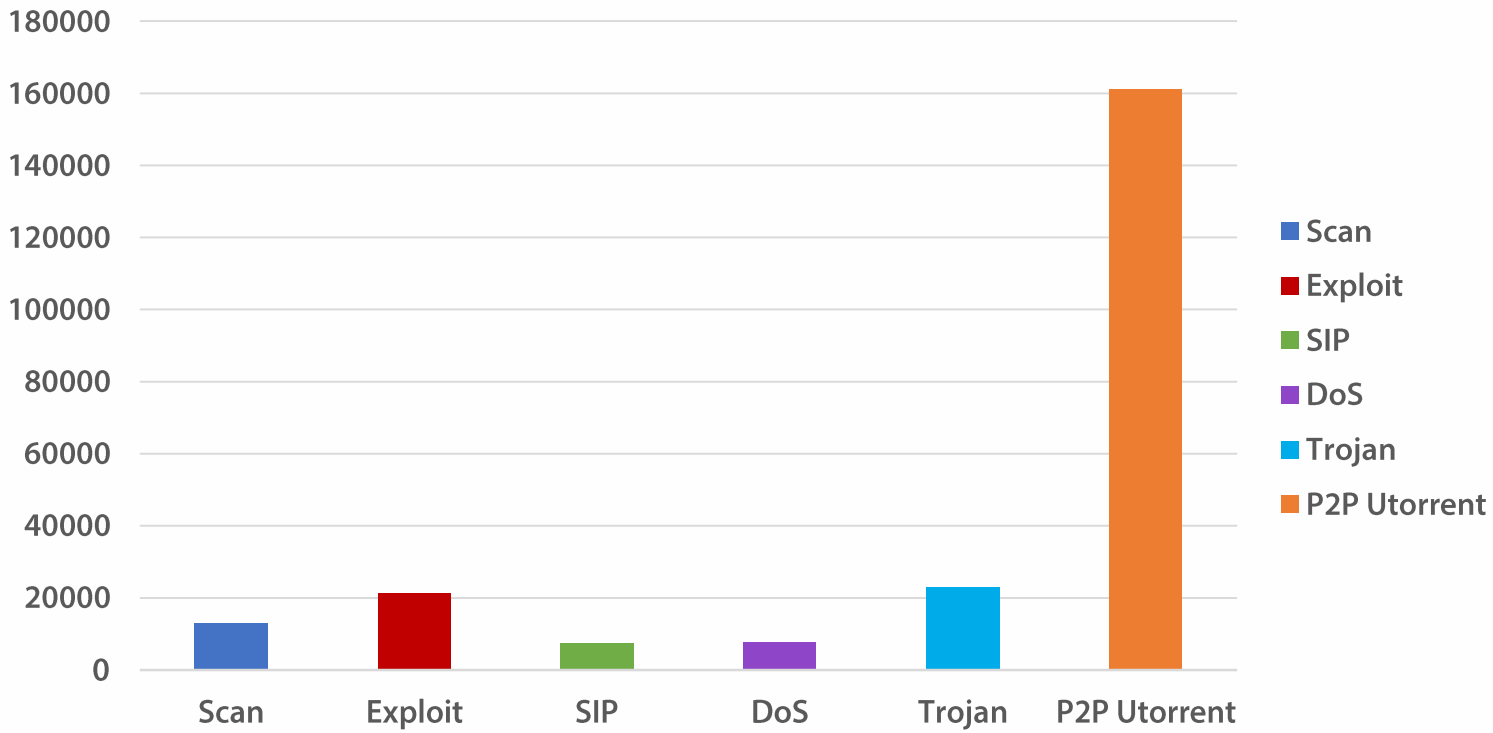
ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
И СВЯЗИ САМАРСКОЙ ОБЛАСТИ

ПРИМЕРЫ

СОБЫТИЯ ПО УРОВНЮ КРИТИЧНОСТИ



ИНЦИДЕНТЫ ПО ТИПАМ УЯЗВИМОСТЕЙ



REGION DIGITAL

ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
И СВЯЗИ САМАРСКОЙ ОБЛАСТИ

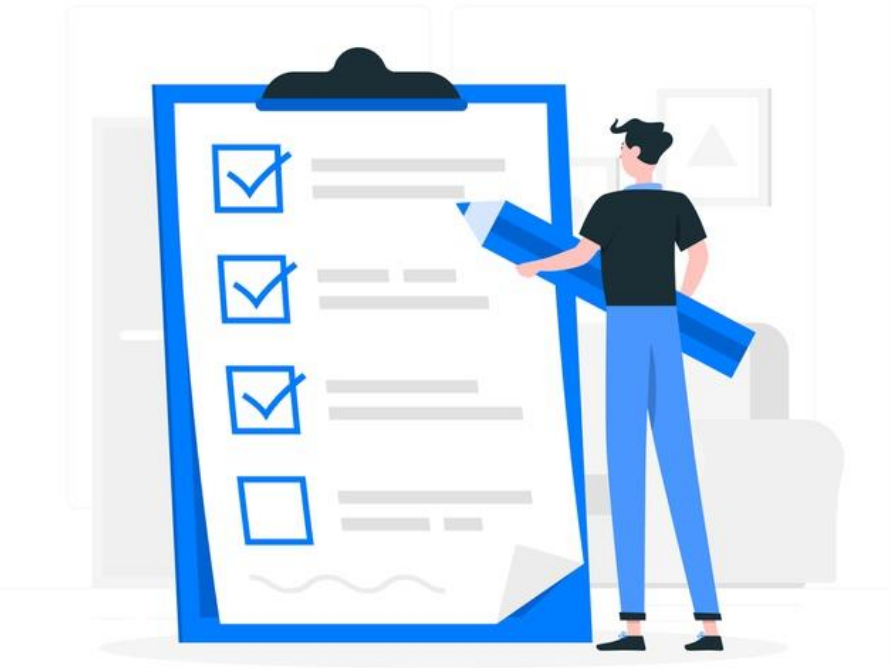
АУТСОРСИНГ? +/-
РЕШЕНИЕ ВСЕХ ПРОБЛЕМ?

- Ответственность на операторе ГИС, субъекте КИИ.
  Административная (ст. 13.12.1, 19.7.15 КоАП)
  Уголовная (ст.272, 274, 274.1 УК РФ)
  NEW
- Контроль качество оказания услуг.
  Как проверить качество мониторинга?
- Скорость реакции специалиста ИБ Заказчика на информацию, рекомендации центра мониторинга Исполнителя
- Предоставление доступа к ресурсам Правительства
- Зависимость от Исполнителя
- Отсутствует рост собственных активов
- Банковская гарантия, страховка?
- Роль в ГосСОПКА?
- Финансирование

REGION DIGITAL

ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
И СВЯЗИ САМАРСКОЙ ОБЛАСТИ

ТАК ЧТО В ИТОГЕ?



Процесс построения Ведомственного центра сложный и многогранный. Требуется:

- Огромное количество людских ресурсов
- Необходимый уровень квалификации и компетенция специалистов
- Непрерывное финансирование в необходимом объёме
- Наделение полномочий, определение зоны ответственности
- Централизованный подход к администрированию СЗИ
- Стандартизация и регламентация процессов
- И т.д. и т.п

REGION DIGITAL

Спасибо за внимание!

АКИМОВ МАКСИМ ОЛЕГОВИЧ

Начальник управления информационной безопасности ГКУ СО «РЦУП»

+7 846 200 09 32
+7 987 436 06 34
m.akimov@rcu.samregion.ru