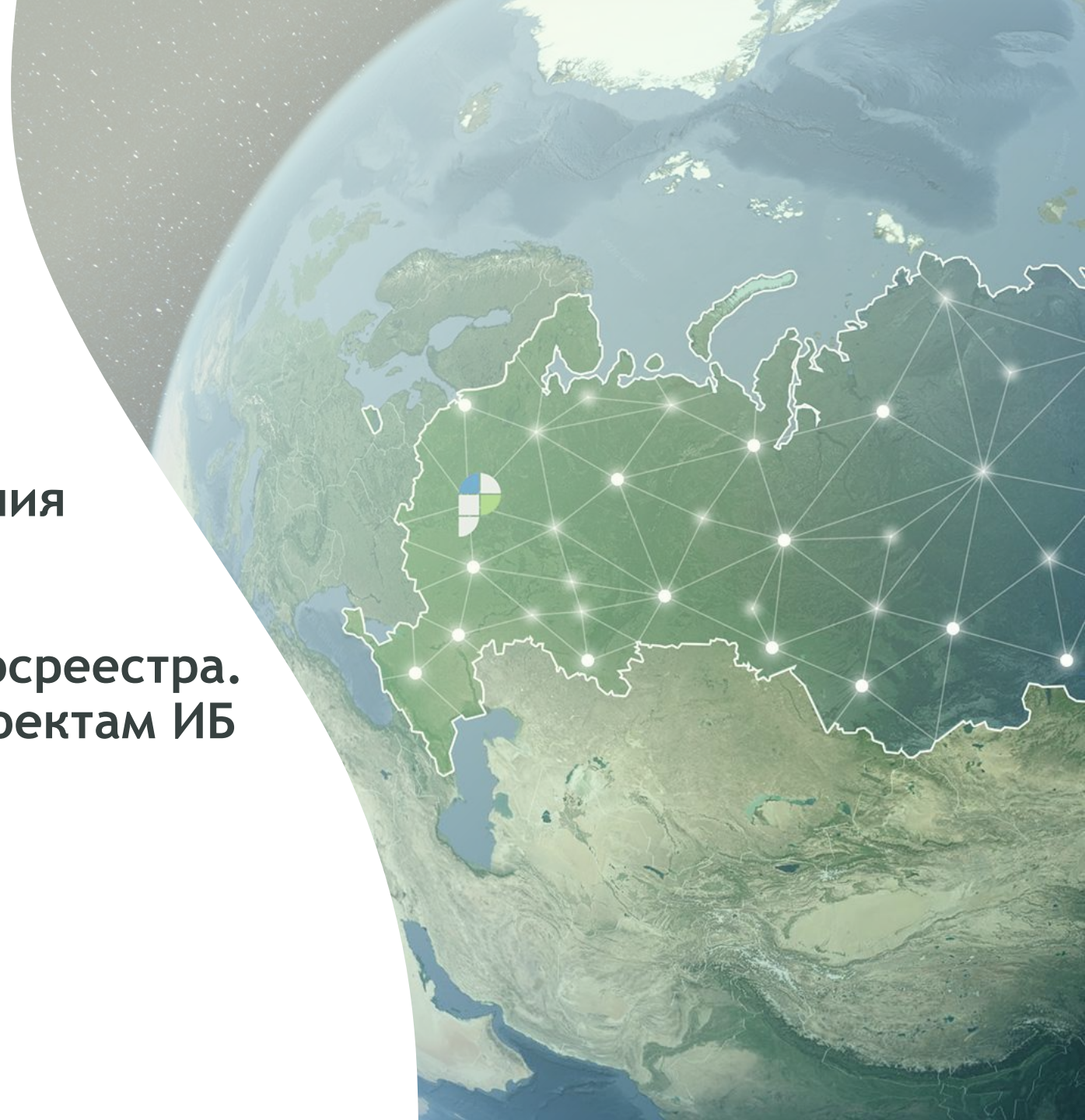




Создание комплексной системы обеспечения информационной безопасности инфраструктуры Росреестра. Статус работ по проектам ИБ

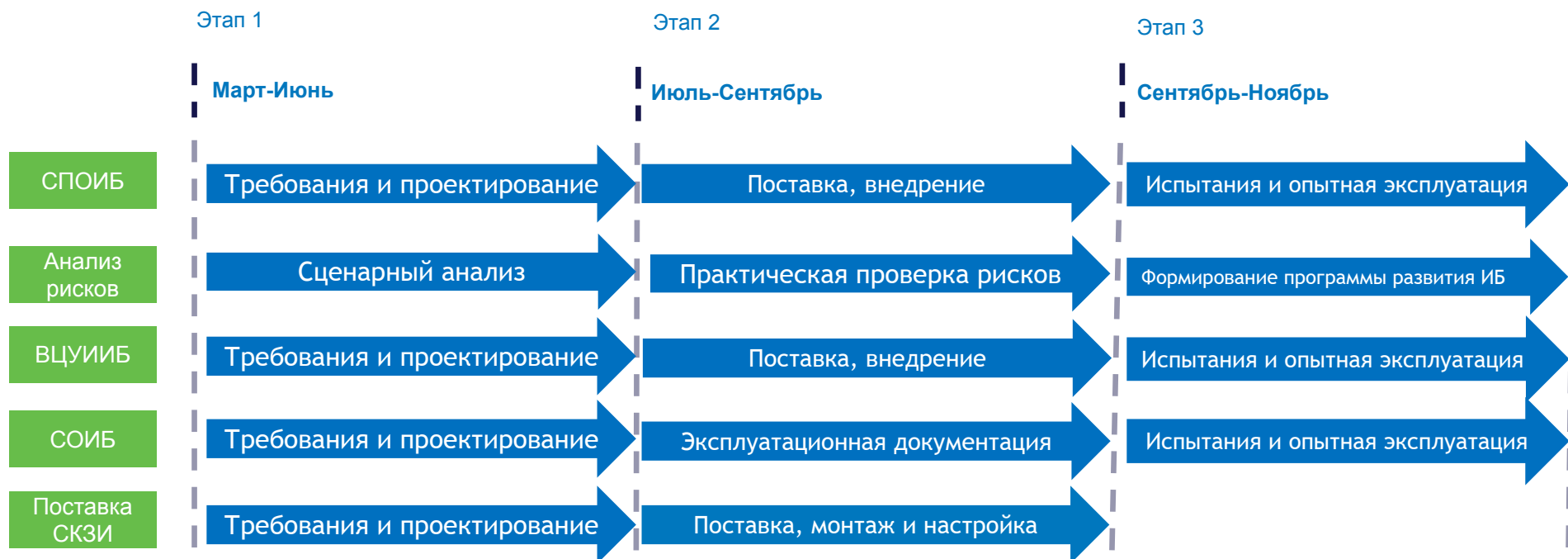
ДЕКАБРЬ 2021 г.



Программа проектов
ГК 0005-10-21 от 12.03.2021 с учётом
ДС№1, 2, 3

- **СПОИБ** – система повышения осведомленности пользователей
- **ВЦУИИБ** - Ведомственный центр управления инцидентами информационной безопасности
- **СОИБ** – система обеспечения информационной безопасности
- **Поставка СКЗИ для ПКЗ** (Подсистемы криптографической защиты)
- **Риски** - Сценарный анализ недопустимых событий

ЭТАПЫ ГК





СПОИБ

01

Работы



- ▶ Проектирование СПОИБ
- ▶ Внедрение и предварительные испытания

- ▶ Система создана на базе программного обеспечения российского вендора Антифиш

Отчеты

19 октября



677 писем доставлено

168 сотрудников открыли письма

153 сотрудника уязвимы - открыли вложение или перешли по ссылке

112 сотрудников ввели данные в фишинговую форму

21 компьютер имеют критические уязвимости и могут быть взломаны

РЕЗУЛЬТАТЫ

- ▶ Разработаны:
 - ▶ ЧТЗ
 - ▶ ПЗ к ТП
 - ▶ Эксплуатационная документация
 - ▶ Процессная модель повышения осведомленности сотрудников Росреестра в сфере информационной безопасности
- ▶ Система внедрена, проведены предварительные испытания (с небольшими замечаниями), проведена опытная эксплуатация.
- ▶ Проведено 4 фишинговых рассылки.



Стартовая страница

Количество инцидентов

1 066

Количество активов

7 459

Средний поток событий

10 195

Распределение среднего потока событий

последние 24 часа



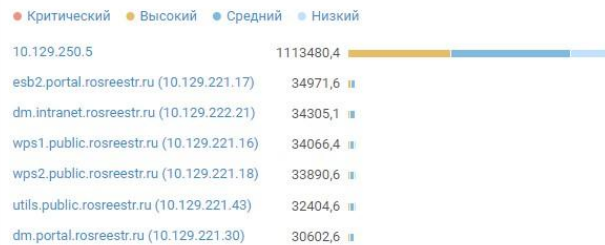
Проверки по чек-листу

09:39



Топ-10 уязвимых активов

последние 7 дней



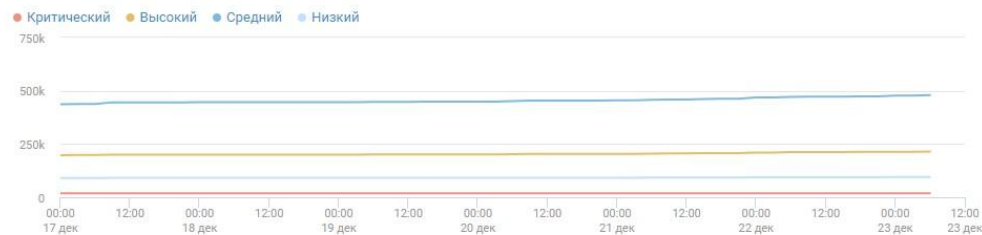
Инциденты по категории

последние 7 дней



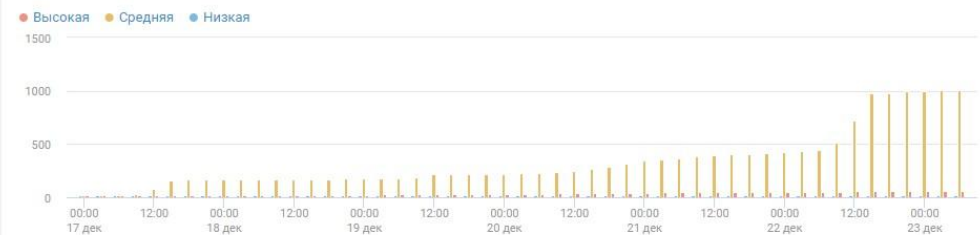
Уязвимости по уровню

последние 7 дней



Инциденты по уровню опасности

последние 7 дней





СОИБ

03

Работы



- ▶ Проектирование СОИБ
- ▶ Пилотирование СЗИ

- ▶ Выбор технических решений произведён с учетом состава программных и технических средств защиты, используемых у Заказчика.

Антивирус – Касперский
Защита от НСД – SecretNet
Защита виртуальных сред – vGate
Межсетевой экран - UserGate

РЕЗУЛЬТАТЫ

- ▶ Разработаны:
 - ▶ ЧТЗ на СОИБ
 - ▶ ПЗ к ТП
 - ▶ Эксплуатационная документация
- ▶ Проведены предварительные испытания KES, SNS, vGate, **Usergate/CheckPoint** на пилотных площадках

По результатам предварительных испытаний рассматривается смена технического решения в части межсетевого экранирования



Поставка СКЗИ для ПКЗ Росреестра

04

Работы



- ▶ Проектирование ПКЗ на базе СКЗИ Континент
- ▶ Поставка СКЗИ Континент на объекты УРР и филиалов ФКП

РЕЗУЛЬТАТЫ

- ▶ Разработаны:
 - ▶ ЧТЗ
 - ▶ ПЗ к техническому проекту
- ▶ Проведена поставка СКЗИ на объекты, ведется документальное закрытие



- ▶ Кол-во СКЗИ по ГК избыточно. 919 единиц оборудования Тип 2 (IPC-10) не требуется согласно проектному решению
- ▶ Адреса поставки оборудования в ГК не актуальны (площадки переехали, закрылись, открылись новые)

- ▶ Заключены ДС№2 и №3 к ГК на исключение 357 ед. избыточного оборудования, актуализацию адресов поставки
- ▶ Проведена приемка по фактически выполненному объему, без поставки и приемки оставшегося избыточного объема в 573 ед.
- ▶ После приемки, ГК расторгнут в отношении 573 ед.



СЦЕНАРНЫЙ АНАЛИЗ НЕДОПУСТИМЫХ СОБЫТИЙ

05

Работы



- Формирование карты недопустимых событий



- Верификация возможности реализации недопустимых событий

РЕЗУЛЬТАТЫ

- ▶ Разработаны:
 - ▶ Матрица недопустимых событий и ущерба
 - ▶ Комплект карточек сценариев реализации недопустимых событий
- ▶ Проведен практический семинар по недопустимым событиями
- ▶ Проведена верификация рисков (возможности реализации недопустимых событий), подготовлен отчет



Реализованные в 2022г. мероприятия не вошедшие (исключенные ГК 0005)

06

Работы



- Аттестация ИС Росреестра



- Поставка Антивирусного ПО



- Поставка ПО и ТС для подключения к системам АП и МО

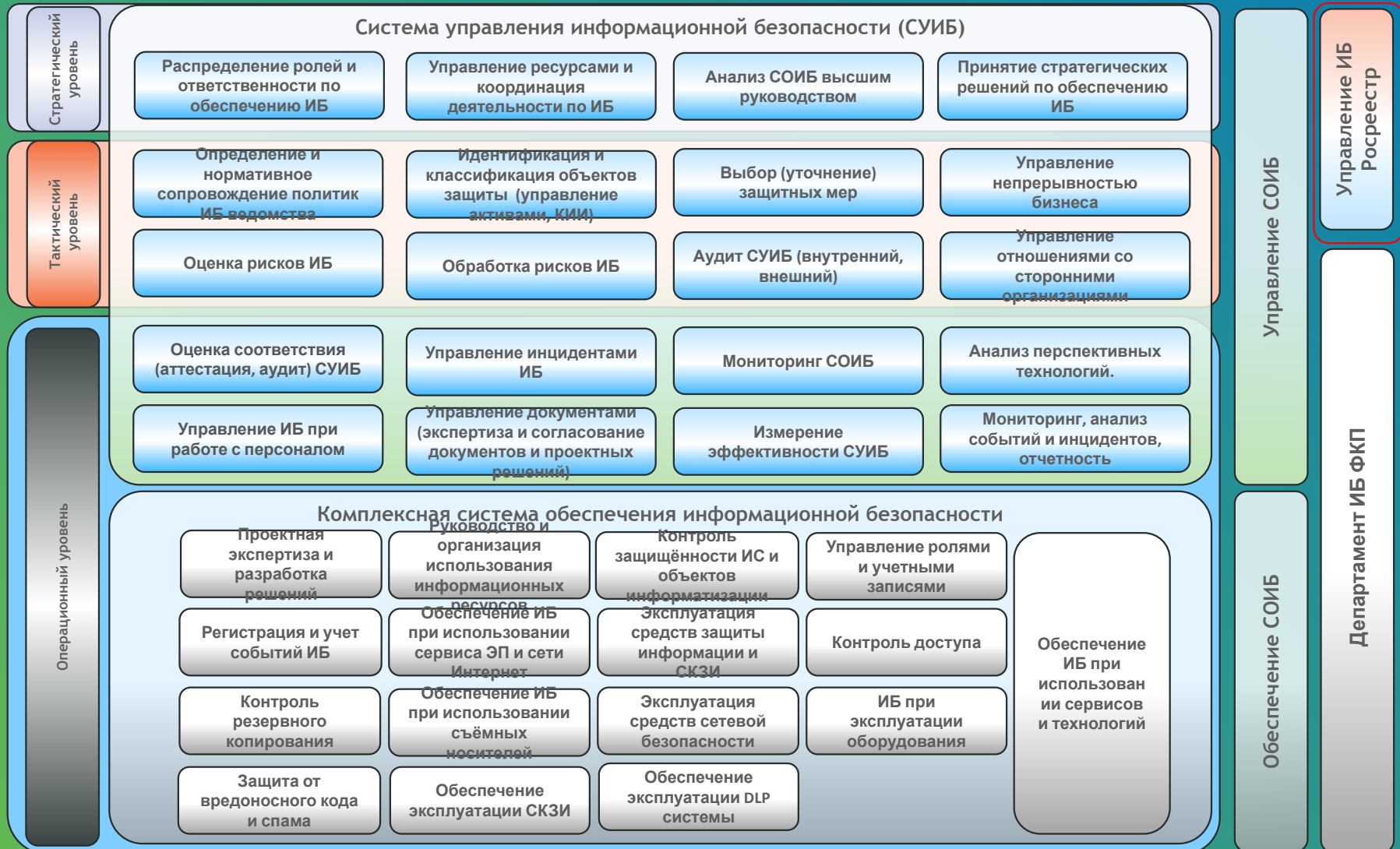
РЕЗУЛЬТАТЫ

- Развернута СЗИ сетевой инфраструктуры, аттестованы на настоящий момент 29 из 37 ИС
- 5 систем аттестовываются в рамках создания ИС
- Остальные системы выводятся из эксплуатации
- Поставлено АВ ПО
- Развернуты и аттестованы 2 АРМ взаимодействия

№ п/п	Наименование ИС	Наличие аттестации	Сроки
1	Автоматизированная информационная система «Мониторинг движения государственных услуг» (ИС «МЭГУ») *	+	РК.0003-10-10 от 30.10.2019
2	Автоматизированная информационная система «Рестор свердловских организаций» (ИС «Рестор СДО») *	+	РК.0003-10-10 от 30.10.2019
3	Программное обеспечение «Автоматизированная информационная система ведения реестра кадастровых номеров» (ИС «РН») *	+	РК.0003-10-10 от 30.10.2019
4	Автоматизированная информационная система хранения фонда данных государственной кадастровой оценки (ИС «ФД ГКО») *	+	РК.0003-10-10 от 30.10.2019
5	Автоматизированная система «Гискадастр» *	+	РК.0003-10-10 от 30.10.2019
6	Программа для ЗМ «Система автоматизированной публикации карт в сеть Интернет» (ИС «ПКО») *	+	РК.0003-10-10 от 30.10.2019
7	Информационная система «Официальный сайт Росреестра» (ИС ОСР) *	+	РК.0003-10-21 от 24.11.2021
8	Федеральная государственная информационная система ведения Единого государственного реестра недвижимости (ФГИС ЕГРН) *	+	РК.0003-10-10 от 31.10.2019
9	Программное обеспечение для ЗМ «Федеральная информационная система по предоставлению сведений участникам рынка РФ на территории Дальневосточного федерального округа» (ИС ИДВ) *	+	РК.0003-10-10 от 31.10.2019
10	Программное обеспечение системы информационной безопасности Федеральной службы государственной регистрации, кадастра и картографии (ФМ ИБ Росреестра) *	+	РК.0003-10-10 от 28.10.2019
11	Общая онлайн-инфраструктура Федеральной службы государственной регистрации, кадастра и картографии (ОС ИР) *	+	РК.0003-10-21 от 24.11.2021
12	Федеральная база данных Регистра (ФБД Регистра) *	+	РК.0003-10-21 от 24.11.2021
13	Платформа сбора и анализа данных о состоянии и движении основных средств учредительной Федеральной службы государственной регистрации, кадастра и картографии (ПСА) *	+	РК.0003-10-21 от 24.11.2021
14	Программа для мониторинга вычислительных мощностей «Автоматизированная информационная система управления парком» (ИС УП) *	+	РК.0003-10-21 от 24.11.2021
15	Программный комплекс сбора данных об информационных ресурсах ГИС и ЕГРН на уровне территориальных органов (ПМ) *	+	РК.0003-10-21 от 24.11.2021
16	Программный комплекс «Федеральный информационный реестр» (ФИР) *	+	РК.0003-10-21 от 24.11.2021
17	Программа для ЗМ «Автоматизированная информационная система комплексной оценки профессиональной деятельности гражданских служащих» *	+	РК.0003-10-21 от 24.11.2021
18	Информационная система управления архивом реестровых дел и иных учетных документов (ИС АРМ) *	+	РК.0003-10-21 от 24.11.2021
19	Программное обеспечение Система по обеспечению целостности трамплинов и параметризованной доставки сообщений на основе FTP-канала с авторитетными государственными реестрами, включая Росреестр, Федеральную базу данных и Систему автоматизированной и параметризованной доставки сообщений регионального уровня регистрации (СМД ИД Р) *	+	РК.0003-10-21 от 24.11.2021
20	Автоматизированная информационно-поставочная система Государственного каталога географических названий (ГКГН) *	+	РК.0003-10-21 от 24.11.2021
21	Автоматизированная информационная система «Юсуд» *	-	Регистрационные аттестаты ОСИРР в рамках РК.0003
22	Программный комплекс Информационная система ведения Единого государственного реестра прав на недвижимое имущество и сделок с ним (ЕГР ИС ЕГРН) *	-	Регистрационные аттестаты ОСИРР в рамках РК.0003
23	Автоматизированная информационная система государственного кадастра недвижимости (ИС ГКО) *	-	Регистрационные аттестаты ОСИРР в рамках РК.0003
24	Платформа «Фонд данных ЕГРН» цифровой инфраструктуры *	-	Система в процессе создания. Аттестат Росреестра
25	Программный комплекс приема сведений документов (ПКСД) *	+	РК.0003-10-21 от 24.11.2021
26	Автоматизированная система электронного документооборота (СЭД) *	+	РК.0003-10-21 от 24.11.2021
27	Единая система регистрации и обработки сведений (ЕКСОД) *	+	РК.0003-10-21 от 24.11.2021
28	Единая система управления персоналом государственной информационной Регистрации (ИС УПС) *	+	РК.0003-10-21 от 24.11.2021
29	Автоматизированная информационная система «Лицензирование геодезической и картографической деятельности» (ИС «Лицензирование геодезической и картографической деятельности») *	-	РК.0003-10-21 от 24.11.2021
31	Автоматизированная информационная система аттестации кадастровых номеров (ИС АКО) *	-	П.0448 от 30.09.2021 в стадии аттестации
32	Программа для ЗМ «Система предоставления сведений о ходе приема заявления» (СЗС) *	-	П.0448 от 30.09.2021 в стадии аттестации
33	Программное обеспечение программный комплекс автоматизированной информационной системы взаимодействия с заявителями (ПО АСЗ) *	-	П.0448 от 30.09.2021 в стадии аттестации
34	Государственная информационная система ведения единой интегрированной картографической основы (ИС ЕКО) *	-	Аттестат ФГИС «Центр геодезии, картографии и ИС»
35	Государственная информационная система «Федеральный портал пространственных данных» (ИС ФПД) *	-	Аттестат ФГИС «Центр геодезии, картографии и ИС»
36	Сайт «Информационный реестр» о лицах и недвижимости (ИР) *	-	Система в процессе создания. Аттестат Росреестра
37	Информационная система ведения Федерального фонда пространственных данных (ИС ФФД) *	-	Система в процессе создания. Аттестат ФГИС «Центр геодезии, картографии и ИС»



Карта процессов информационной безопасности





Карта процессов информационной безопасности (проект)

Регламентация УИБ РР	Планирование УИБ ФКП РР	Выполнение УИБ ФКП РР	Контроль УИБ РР	Управляющее воздействие УИБ РР
Формирование требований и методическое сопровождение разработки и актуализации нормативной базы и политик информационной безопасности ведомственного уровня	Формирование планов реализации	Разработка и адаптация локальной нормативной базы и политик информационной безопасности	Контроль реализации требований корпоративного уровня в ЛНА организаций и подразделений ведомства	Согласование подключения к ИС, обработки информации ограниченного доступа.
Нормативно-методическое сопровождение выполнения работ подразделениям ИБ подразделений и организаций ведомства (в т.ч. в вопросах лицензирования, разработки нормативов оказания услуг в области ИБ, маршрутных карт, регламентов взаимодействия)	Формирование планов реализации	Выполнение работ по направлению ИБ	Контроль выполнения работ подразделениям ИБ (в т.ч. в вопросах лицензирования, разработки нормативов оказания услуг в области ИБ, маршрутных карт, регламентов взаимодействия)	Согласование подключения к централизованным ИС, обработки информации ограниченного доступа.
Создание АСЗИ, ИС				
Эксплуатация АСЗИ				
Проектная деятельность				
АСУТП и КИИ				
Международная деятельность				
ВЦУИИБ и ведомственный центр ГосСОПКА				
Прочие функции				



Развитие ИБ **2022**

1. Тираж СОИБ, СПОИБ, ВЦУИИБ
2. Проектирование и внедрение ядер новых систем:
 - DLP системы;
 - системы контроля действий привилегированных пользователей;
 - системы централизованного управления учетными данными и правами доступа;
 - системы защиты от целенаправленных атак;
 - аттестации государственных информационных систем.
3. Внедрение процессной модели;
4. Формирование сервисов ИБ для всего периметра ведомства.



РОСРЕЕСТР

Федеральная служба
государственной регистрации,
кадастра и картографии

ВЦУИИБ. ФУНКЦИОНАЛЬНАЯ СТРУКТУРА

Подсистема контроля защищенности и соответствия стандартам

Подсистема мониторинга событий информационной безопасности

Подсистема анализа сетевого трафика, выявления и расследования инцидентов

Подсистема управления инцидентами и взаимодействия с ГосСОПКА

Подсистема защиты веб-приложений от несанкционированного доступа



Подсистема защиты информации ВЦУИИБ

*на базе типовых средств СОИБ

НАЗНАЧЕНИЕ

- ▶ Обеспечивает невозможность реализации недопустимых событий
- ▶ Осуществляет противодействие компьютерным атакам
- ▶ Определяет то, как функционируют меры и средства СОИБ

ПИЛОТНАЯ ЗОНА (2021 ГОД)

- ▶ 10 объектов (Москва, МО, Орел)
- ▶ 5 000 узлов
- ▶ 10 Гбит/с мониторинг трафика
- ▶ 3 недопустимых события

ИЕРАРХИЧНАЯ СТРУКТУРА КСОИБ РОСРЕЕСТРА

