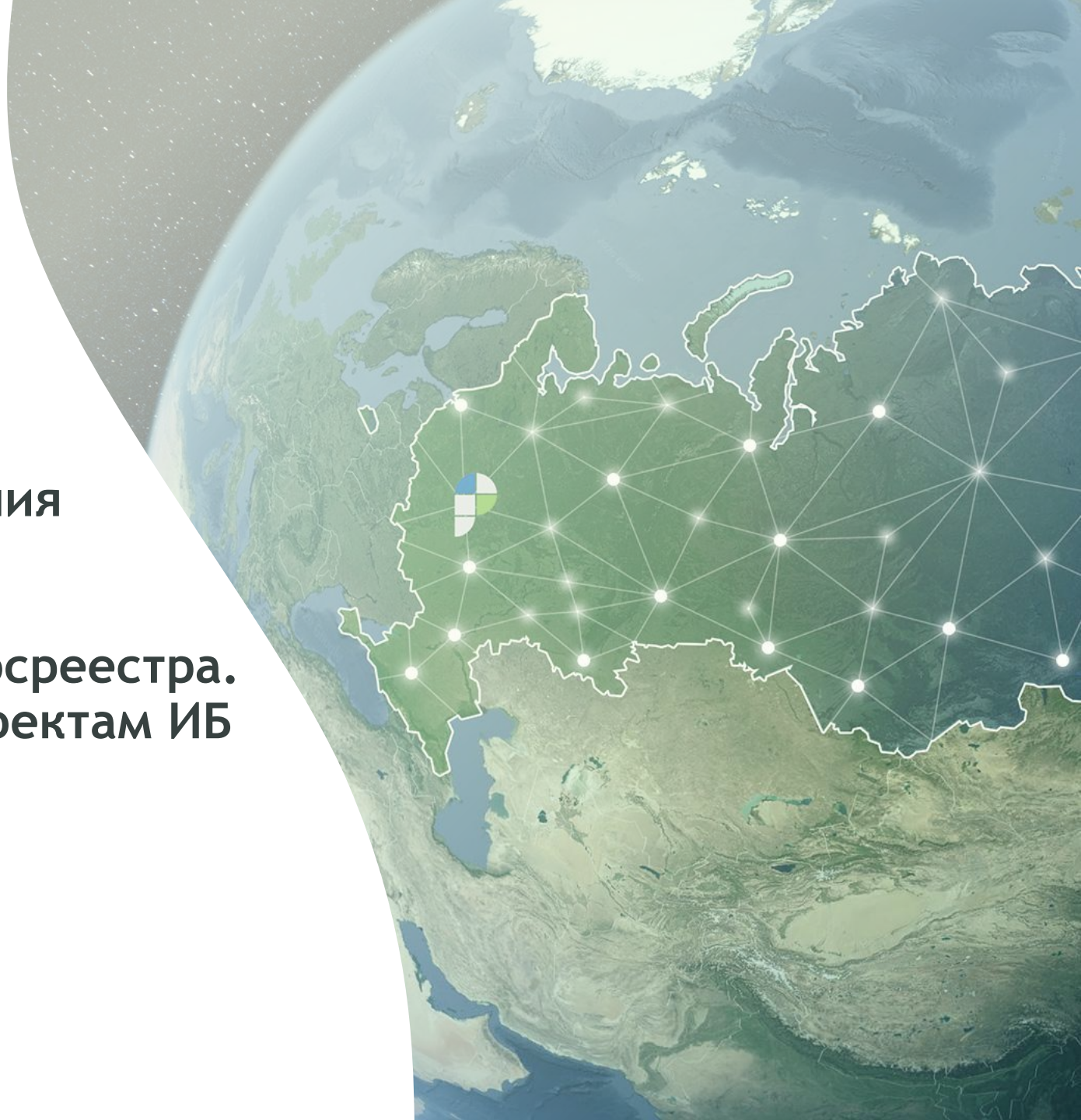
РОСРЕЕСТР
Федеральная служба
государственной регистрации,
кадастра и картографии



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

ДЕКАБРЬ 2021 г.

РОСРЕЕСТР

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

РОСРЕЕСТР

ЭТАПЫ ГК

РОСРЕЕСТР

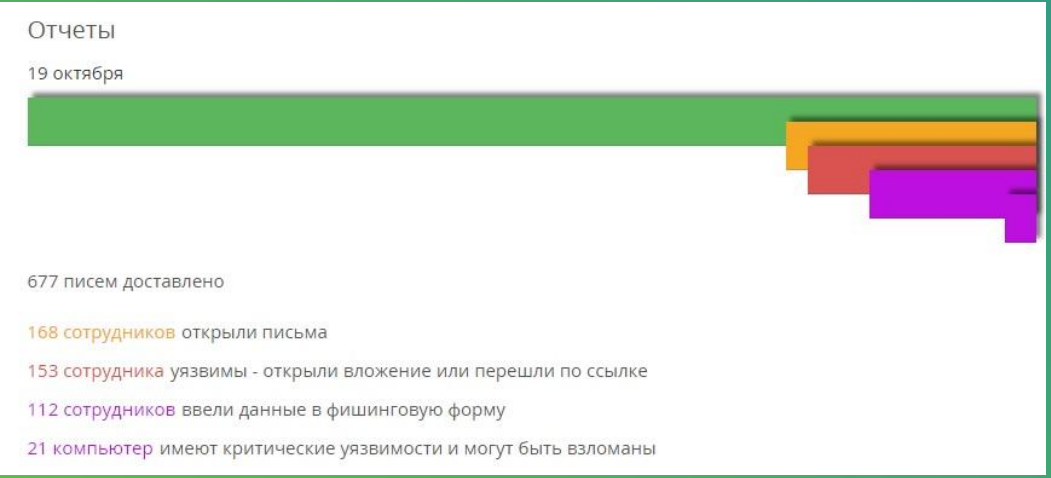
СПОИБ

01

Работы

- Проектирование СПОИБ
- Внедрение и предварительные испытания

- Система создана на базе программного обеспечения российского вендора Антифиш



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.

РОСРЕЕСТР

ВЦУИИБ

02

Работы

- Проектирование
- Внедрение и предварительные испытания

- Система спроектирована на базе продуктов российского вендора «Позитивные технологии» на пилотных площадках

РЕЗУЛЬТАТЫ

- Разработаны:
  - ЧТЗ
  - ПЗ к ТП
  - Эксплуатационная документация

- Система внедрена на пилотных площадках (ЦА Чистые пруды, ЦОД Варшавский), проведены предварительные испытания, переведена в опытную эксплуатацию

Перечень инцидентов с 24.11.2021 9:31:22 по 25.11.2021 9:31:22

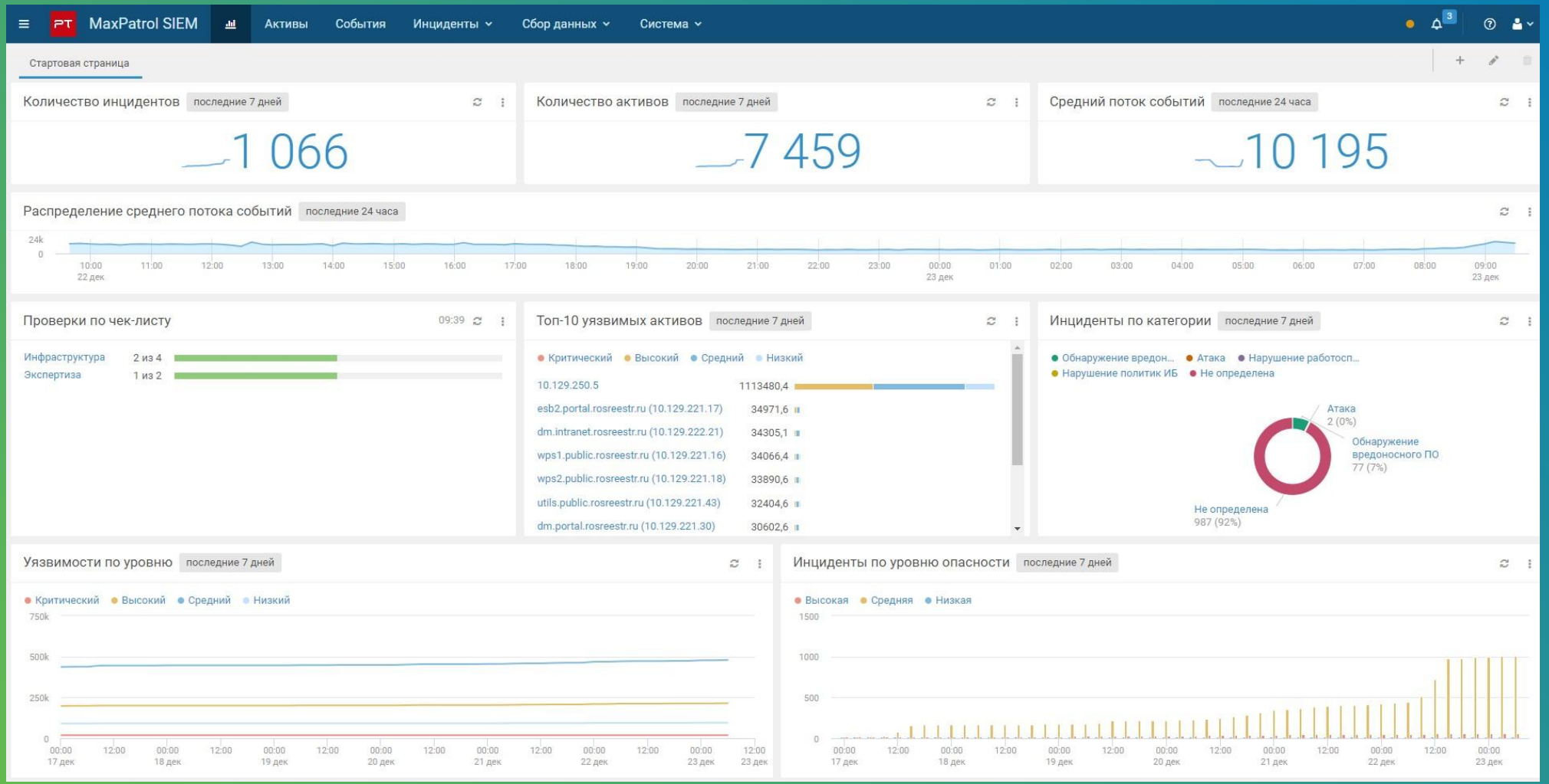
Группы: ВЦ-ГЦА РР

Фильтр: status != "Closed" AND category = "Undefined", созданные с 24 ноября 2021 г. 9:31 по 25 ноября 2021 г. 9:31

Номер п/п	Дата и время регистрации	Статус на дату окончания отчетного периода	Категория	Приоритет	Содержание инцидента	Атакующий адрес
INC-11570	24.11.2021 9:32	Новый	Сетевая атака	Высокий	Обнаружена сетевая атака '' с узла 10.128.8.37 на узле cp-ws33334.ca.rosreestr.local	10.128.8.37
INC-11571	24.11.2021 9:42	Новый	Сетевая атака	Высокий	Обнаружена сетевая атака '' с узла 10.128.8.37 на узле vp-ws311-4.ca.rosreestr.local	10.128.8.37
INC-11572	24.11.2021 10:06	Новый	Сетевая атака	Высокий	Обнаружена сетевая атака '' с узла 10.128.8.37 на узле cp-ws3540.ca.rosreestr.local	10.128.8.37
INC-11573	24.11.2021 9:50	Новый	Сетевая атака	Высокий	Обнаружена сетевая атака '' с узла 10.128.8.37 на узле vp-ws311-0.ca.rosreestr.local	10.128.8.37
INC-11574	24.11.2021 9:58	Новый	Сетевая атака	Высокий	Обнаружена сетевая атака '' с узла 10.128.8.37 на узле cp-ws33339.ca.rosreestr.local	10.128.8.37
INC-11580	24.11.2021 10:35	Новый	Сетевая атака	Высокий	Обнаружена сетевая атака '' с узла 10.128.8.37 на узле cp-ws333025.ca.rosreestr.local	10.128.8.37
INC-11581	24.11.2021 10:51	Новый	Сетевая атака	Высокий	Обнаружена сетевая атака '' с узла 10.128.8.37 на узле vp-ws380.ca.rosreestr.local	10.128.8.37
INC-11585	24.11.2021 12:37	Новый	Сетевая атака	Высокий	Обнаружена сетевая атака '' с узла 10.128.8.37 на узле cp-ws333025.ca.rosreestr.local	10.128.8.37
INC-11587	24.11.2021 12:54	Новый	Сетевая атака	Высокий	Обнаружена сетевая атака '' с узла 10.128.8.37 на узле vp-ws380.ca.rosreestr.local	10.128.8.37
INC-11597	24.11.2021 15:21	Новый	Сетевая атака	Высокий	Обнаружена сетевая атака '' с узла 10.128.8.37 на узле cp-ws333025.ca.rosreestr.local	10.128.8.37
INC-11598	24.11.2021 15:37	Новый	Сетевая атака	Высокий	Обнаружена сетевая атака '' с узла 10.128.8.37 на узле vp-ws380.ca.rosreestr.local	10.128.8.37
INC-11600	24.11.2021 16:09	Новый	Сетевая атака	Высокий	Обнаружена сетевая атака '' с узла 10.128.60.203 на узле rub-ws2219.ca.rosreestr.local	10.128.60.203
INC-11602	24.11.2021 16:13	Новый	Сетевая атака	Высокий	Обнаружена сетевая атака '' с узла 10.128.8.37 на узле cp-ws333025.ca.rosreestr.local	10.128.8.37
INC-11603	24.11.2021 16:15	Новый	Сетевая атака	Высокий	Обнаружена сетевая атака '' с узла 10.128.60.203 на узле cp-ws33334.ca.rosreestr.local	10.128.60.203
INC-11604	24.11.2021 16:23	Новый	Сетевая атака	Высокий	Обнаружена сетевая атака '' с узла 10.128.60.203 на узле vp-ws311-4.ca.rosreestr.local	10.128.60.203
INC-11605	24.11.2021 16:48	Новый	Сетевая атака	Высокий	Обнаружена сетевая атака '' с узла 10.128.60.203 на узле cp-ws3540.ca.rosreestr.local	10.128.60.203
INC-11606	24.11.2021 16:33	Новый	Сетевая атака	Высокий	Обнаружена сетевая атака '' с узла 10.128.60.203 на узле vp-ws311-0.ca.rosreestr.local	10.128.60.203
INC-11607	24.11.2021 16:33	Новый	Сетевая атака	Высокий	Обнаружена сетевая атака '' с узла 10.128.8.37 на узле vp-ws380.ca.rosreestr.local	10.128.8.37
INC-11608	24.11.2021 16:39	Новый	Сетевая атака	Высокий	Обнаружена сетевая атака '' с узла 10.128.8.37 на узле rub-ws2219.ca.rosreestr.local	10.128.8.37
INC-11609	24.11.2021 16:46	Новый	Сетевая атака	Высокий	Обнаружена сетевая атака '' с узла 10.128.8.37 на узле cp-ws33334.ca.rosreestr.local	10.128.8.37
INC-11610	24.11.2021 16:54	Новый	Сетевая атака	Высокий	Обнаружена сетевая атака '' с узла 10.128.8.37 на узле vp-ws311-4.ca.rosreestr.local	10.128.8.37
INC-11611	24.11.2021 17:03	Новый	Сетевая атака	Высокий	Обнаружена сетевая атака '' с узла 10.128.8.37 на узле vp-ws311-0.ca.rosreestr.local	10.128.8.37
INC-11612	24.11.2021 17:21	Новый	Сетевая атака	Высокий	Обнаружена сетевая атака '' с узла 10.128.8.37 на узле cp-ws3540.ca.rosreestr.local	10.128.8.37
INC-11613	24.11.2021 17:34	Новый	Сетевая атака	Высокий	Обнаружена сетевая атака '' с узла 10.128.8.37 на узле vp-ws380.ca.rosreestr.local	10.128.8.37
INC-11614	24.11.2021 18:11	Новый	Сетевая атака	Высокий	Обнаружена сетевая атака '' с узла 10.128.8.37 на узле cp-ws333025.ca.rosreestr.local	10.128.8.37
INC-11617	25.11.2021 2:04	Новый	Сетевая атака	Высокий	Обнаружена сетевая атака '' с узла 10.128.64.194 на узле vp-ws312-4.ca.rosreestr.local	10.128.64.194
INC-11618	25.11.2021 2:16	Новый	Сетевая атака	Высокий	Обнаружена сетевая атака '' с узла 10.128.64.194 на узле vp-ws306-0-0.ca.rosreestr.local	10.128.64.194
INC-11619	25.11.2021 2:18	Новый	Сетевая атака	Высокий	Обнаружена сетевая атака '' с узла 10.128.64.194 на узле vp-ws208-1.ca.rosreestr.local	10.128.64.194
INC-11620	25.11.2021 2:19	Новый	Сетевая атака	Высокий	Обнаружена сетевая атака '' с узла 10.128.64.194 на узле vp-ws412-0.ca.rosreestr.local	10.128.64.194
INC-11621	25.11.2021 2:19	Новый	Сетевая атака	Высокий	Обнаружена сетевая атака '' с узла 10.128.64.194 на узле vp-ws329-0-1.ca.rosreestr.local	10.128.64.194
INC-11622	25.11.2021 5:42	Новый	Сетевая атака	Высокий	Обнаружена сетевая атака '' с узла 10.128.64.194 на узле vp-ws412-0.ca.rosreestr.local	10.128.64.194
INC-11623	25.11.2021 5:52	Новый	Сетевая атака	Высокий	Обнаружена сетевая атака '' с узла 10.128.64.194 на узле ws312-4.ca.rosreestr.local	10.128.64.194
INC-11624	25.11.2021 5:57	Новый	Сетевая атака	Высокий	Обнаружена сетевая атака '' с узла 10.128.64.194 на узле vp-ws208-1.ca.rosreestr.local	10.128.64.194
INC-11625	25.11.2021 5:59	Новый	Сетевая атака	Высокий	Обнаружена сетевая атака '' с узла 10.128.64.194 на узле vp-ws329-0-1.ca.rosreestr.local	10.128.64.194
INC-11626	25.11.2021 6:48	Новый	Сетевая атака	Высокий	Обнаружена сетевая атака '' с узла 10.128.64.194 на узле vp-ws306-0-0.ca.rosreestr.local	10.128.64.194
INC-11629	25.11.2021 8:53	Новый	Сетевая атака	Высокий	Обнаружена сетевая атака '' с узла 10.128.64.194 на узле vp-ws312-4.ca.rosreestr.local	10.128.64.194
INC-11630	25.11.2021 8:55	Новый	Сетевая атака	Высокий	Обнаружена сетевая атака '' с узла 10.128.64.194 на узле vp-ws124-1.ca.rosreestr.local	10.128.64.194
INC-11631	25.11.2021 8:56	Новый	Сетевая атака	Высокий	Обнаружена сетевая атака '' с узла 10.128.64.194 на узле vp-ws318-0.ca.rosreestr.local	10.128.64.194
INC-11632	25.11.2021 8:56	Новый	Сетевая атака	Высокий	Обнаружена сетевая атака '' с узла 10.128.64.194 на узле vp-ws204-1.ca.rosreestr.local	10.128.64.194
INC-11633	25.11.2021 9:01	Новый	Сетевая атака	Высокий	Обнаружена сетевая атака '' с узла 10.128.64.194 на узле vp-ws306-0-0.ca.rosreestr.local	10.128.64.194
INC-11634	25.11.2021 9:02	Новый	Сетевая атака	Высокий	Обнаружена сетевая атака '' с узла 10.128.64.194 на узле vp-ws208-1.ca.rosreestr.local	10.128.64.194
INC-11635	25.11.2021 9:04	Новый	Сетевая атака	Высокий	Обнаружена сетевая атака '' с узла 10.128.64.194 на узле vp-ws329-0-1.ca.rosreestr.local	10.128.64.194
INC-11636	25.11.2021 9:06	Новый	Сетевая атака	Высокий	Обнаружена сетевая атака '' с узла 10.128.8.14 на узле cp-ws333025.ca.rosreestr.local	10.128.64.194
INC-11637	25.11.2021 9:24	Новый	Сетевая атака	Высокий	Обнаружена сетевая атака '' с узла 10.128.64.194 на узле vp-ws406-1.ca.rosreestr.local	10.128.64.194
INC-11638	25.11.2021 9:25	Новый	Сетевая атака	Высокий	Обнаружена сетевая атака '' с узла 10.128.64.194 на узле vp-ws242-ca.rosreestr.local	10.128.64.194
INC-11639	25.11.2021 9:27	Новый	Сетевая атака	Высокий	Обнаружена сетевая атака '' с узла 10.128.8.14 на узле rub-ws219.ca.rosreestr.local	10.128.8.14

РОСРЕЕСТР

ВЦУИИБ



РОСРЕЕСТР

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

РОСРЕЕСТР

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.

РОСРЕЕСТР

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

РОСРЕЕСТР

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

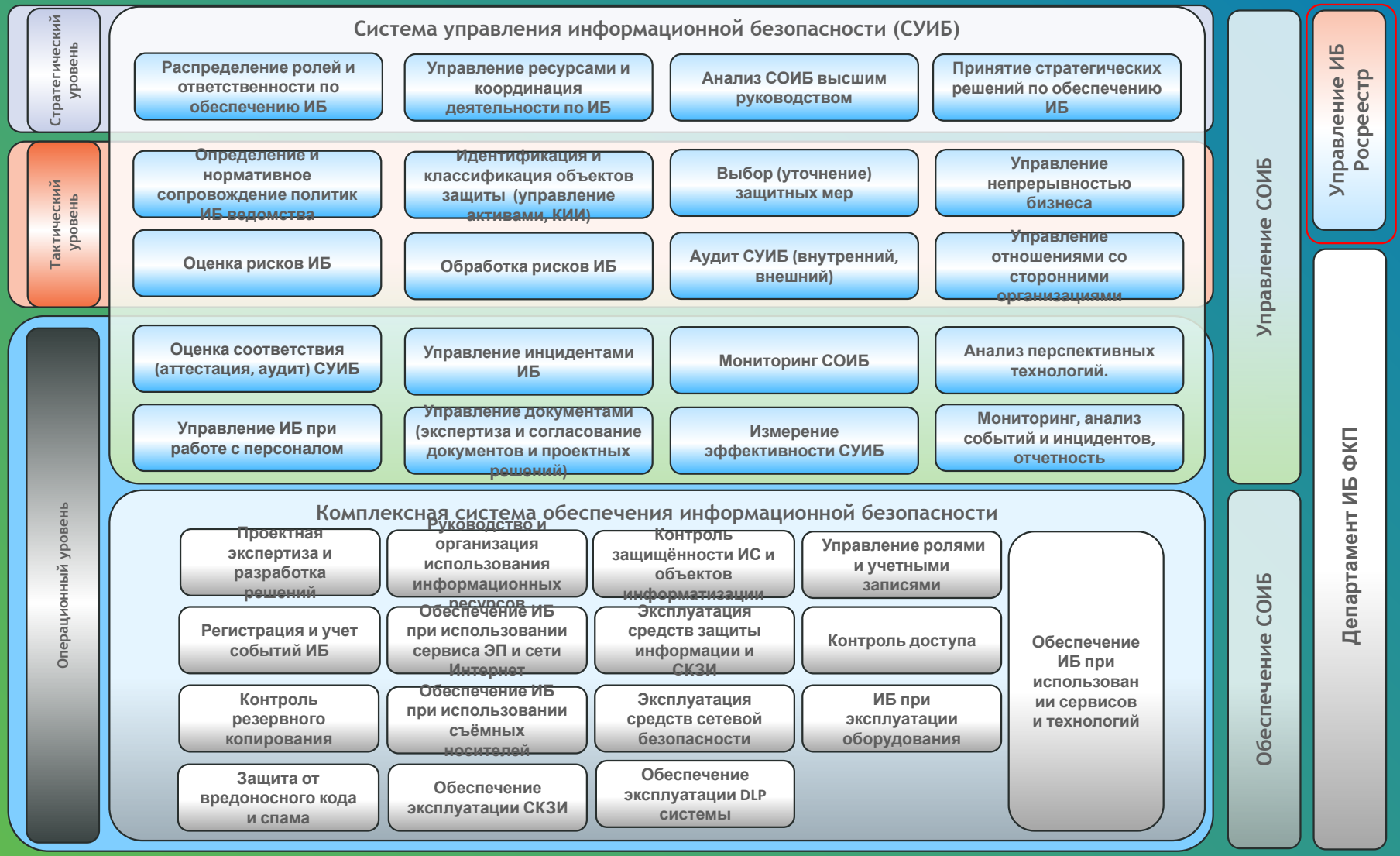
РЕЗУЛЬТАТЫ

- 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 аттестата	Основание
1	Автоматизированная информационная система «Мониторинг оказания государственных услуг» (АИС «МОГУ»)	+	ГК 0072-10-19 от 30.10.2019
2	Автоматизированная информационная система «Реестр саморегулируемых организаций» (АИС «Реестр СРО»)	+	ГК 0072-10-19 от 30.10.2019
3	Программное обеспечение «Автоматизированная информационная система ведения реестра кадастровых инженеров» (АИС «РКИ»)	+	ГК 0072-10-19 от 30.10.2019
4	Автоматизированная информационная система ведения фонда данных государственной кадастровой оценки (АИС «ФД ГКО»)	+	ГК 0072-10-19 от 30.10.2019
5	Автоматизированная система «Госземнадзор»	+	ГК 0072-10-19 от 30.10.2019
6	Программа для ЭВМ «Система автоматизированной публикации карт в сети Интернет» (АС «ПКИ»)	+	ГК 0072-10-19 от 30.10.2019
7	Информационная система «Официальный сайт Росреестра» (ИС ОСР)	+	ГК 0053-10-21 от 24.11.2021
8	Федеральная государственная информационная система ведения Единого государственного реестра недвижимости (ФГИС ЕГРН)	+	ГК 0083-10-19 от 31.10.2019
9	Программное обеспечение для ЭВМ «Федеральная информационная система по предоставлению земельных участков гражданам РФ на территории Дальневосточного федерального округа» (ФИС НДВ)	+	ГК 0075-10-19 от 31.10.2019
10	Программно-аппаратный комплекс информационной безопасности Федеральной службы государственной регистрации, кадастра и картографии (ПАК ИБ Росреестра)	+	ГК 0082-10-19 от 28.10.2019
11	Общая сетевая инфраструктура Федеральной службы государственной регистрации, кадастра и картографии (ОСИФР)	+	ГК 0053-10-21 от 24.11.2021
12	Федеральная база знаний Росреестра (ФБЗ Росреестра)	+	ГК 0053-10-21 от 24.11.2021
13	Подсистема сбора и анализа данных о состоянии и движении основных средств учреждений Федеральной службы государственной регистрации, кадастра и картографии (ОС)	+	ГК 0053-10-21 от 24.11.2021
14	Программа для электронных вычислительных машин «Автоматизированная информационная система управления персоналом» (АИС УП)	+	ГК 0053-10-21 от 24.11.2021
15	Программный комплекс сбора данных из информационных ресурсов ГИН и ЕГРП на уровне территориальных органов (ТИР)	+	ГК 0053-10-21 от 24.11.2021
16	Программный комплекс Федеральный информационный ресурс (ФИР)	+	ГК 0053-10-21 от 24.11.2021
17	Программа для ЭВМ «Автоматизированная информационная система комплексной оценки профессиональной служебной деятельности гражданских служащих»	+	ГК 0053-10-21 от 24.11.2021
18	Информационная система управления архивом реестровых дел и книг учета документов (ИС Архив)	+	ГК 0053-10-21 от 24.11.2021
19	Программное обеспечение - Система по обеспечению интеграции приложений и гарантированной доставки сообщений на основе IP-сети с интернет-порталом государственных услуг, оказываемых Росреестром в электронном виде и Система интеграции приложений и гарантированной доставки сообщений регионального модуля диспетчеризации (СУДС ЦД Р)	+	ГК 0053-10-21 от 24.11.2021
20	Автоматизированная информационно-поисковая система Государственного каталога географических названий (ГКГН)	+	ГК 0053-10-21 от 24.11.2021
21	Автоматизированная информационная система «Юстиция»	-	Распространение аттестата ОСИФР в рамках ГК 0053
22	Программный комплекс Информационная система ведения Единого государственного реестра прав на недвижимое имущество и сделок с ним (ПК ИС ЕГРП)	-	Распространение аттестата ОСИФР в рамках ГК 0053
23	Автоматизированная информационная система государственного кадастра недвижимости (АИС ГКН)	-	Распространение аттестата ОСИФР в рамках ГК 0053
24	Подсистема «Витрина данных ЕГРН» цифровой платформы		Система в процессе создания. Аттестует Росреестр
25	Программный комплекс приема-выдачи документов (ПКПВД)	+	ГК 0053-10-21 от 24.11.2021
26	Автоматизированная система электронного документооборота (СЭД)	+	ГК 0053-10-21 от 24.11.2021
27	Единая система регистрации и обработки обращений (ЕСРОО)	+	ГК 0053-10-21 от 24.11.2021
28	Единая система управления нормативно-справочной информацией Росреестра (ЕС УНСИ)	+	ГК 0053-10-21 от 24.11.2021
29	Автоматизированная информационная система «Лицензирование геодезической и картографической деятельности» (АИС «Лицензирование геодезической и картографической деятельности»)	+	ГК 0053-10-21 от 24.11.2021
31	Автоматизированная информационная система аттестации кадастровых инженеров (АИС АКИ)		П/0448 от 30.09.2021 о выводе из эксплуатации
32	Программа для ЭВМ "Система предоставления сведений о ходе приема заявителей" (СПС)		П/0449 от 30.09.2021 о выводе из эксплуатации
33	Программное обеспечение - программный комплекс автоматизированной информационно-справочной системы взаимодействия с заявителями (ПО АСВЗ)		П/0450 от 30.09.2021 о выводе из эксплуатации
34	Государственная информационная система ведения единой электронной картографической основы (ГИС ЕЭКО)		Аттестует ФГБУ "Центр геодезии, картографии и ИПД"
35	Государственная информационная система Федеральный портал пространственных данных (ГИС ФППД)		Аттестует ФГБУ "Центр геодезии, картографии и ИПД"
36	Единый информационный ресурс о земле и недвижимости (ЕИР)		Система в процессе создания. Аттестует Росреестр
37	Информационная система ведения федерального фонда пространственных данных (ИС ФФПД)		Система в процессе создания. Аттестует ФГБУ "Центр геодезии, картографии и ИПД"

РОСРЕЕСТР

Карта процессов информационной безопасности



РОСРЕЕСТР

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				

РОСРЕЕСТР

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 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

РОСРЕЕСТР

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

РОСРЕЕСТР

ИЕРАРХИЧНАЯ СТРУКТУРА КСОИБ РОСРЕЕСТРА