Минцифра
Оренбургской области
digital.orb.ru

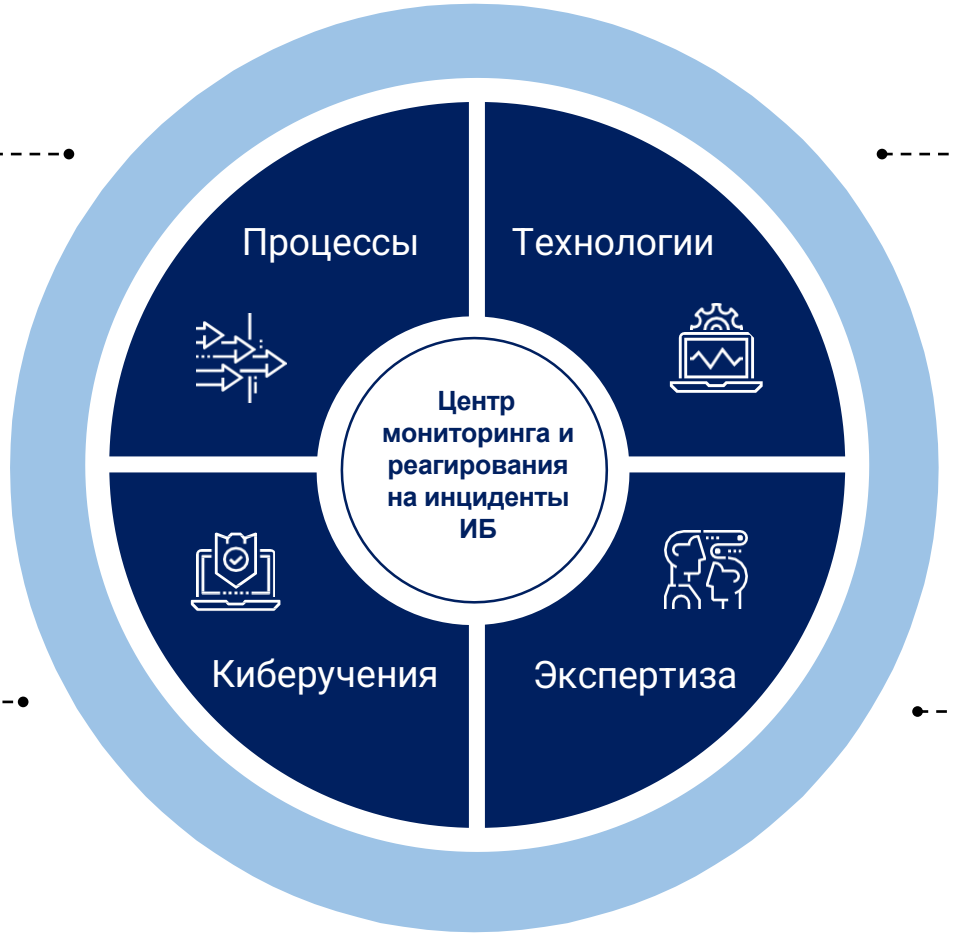
СТРАТЕГИЯ РЕЗУЛЬТАТИВНОЙ КИБЕРБЕЗОПАСНОСТИ МИНИСТЕРСТВА ЦИФРОВОГО РАЗВИТИЯ И СВЯЗИ ОРЕНБУРГСКОЙ ОБЛАСТИ

Оренбургская область
2025 год

АКТУАЛЬНОЕ СОСТОЯНИЕ ЦЕНТРА МОНИТОРИНГА И РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРЕНБУРСГКОЙ ОБЛАСТИ

Центр мониторинга и реагирования на инциденты информационной безопасности Правительства Оренбургской области сформирован в 2020 году и функционирует в качестве обособленной функциональной единицы, созданной на базе отдела кибербезопасности ГКУ «Центр информационных технологий Оренбургской области»

Работа команды выстроена на основе «Механизма непрерывного улучшения»,что позволяет максимально быстро, гибко и эффективно реагировать на любые возникающие угрозы ИБ



МЦР, ГКУ ЦИТ закуплены, установлены и настроены различные системы защиты и средства мониторинга от ведущих компаний – лидеров рынка по защите информации, включающие необходимый набор для построения комплексной защиты инфраструктуры

Проверка полноты и качества построения ЦПК и невозможности реализации недопустимых событий

Специалисты, обладающие необходимыми знаниями и опытом и постоянно повышающие квалификацию на киберучениях; возможность привлечения экспертной поддержки

ЗАЩИЩАЕМЫЕ РЕСУРСЫ ПРАВИТЕЛЬСТВА ОРЕНБУРГСКОЙ ОБЛАСТИ

ЦЕНТР ОБРАБОТКИ ДАННЫХ ПРАВИТЕЛЬСТВА ОРЕНБУРГСКОЙ ОБЛАСТИ

ОБЩЕЕ КОЛИЧЕСТВО СТОЕК **14**

ОБЩЕЕ КОЛИЧЕСТВО СЕРВЕРОВ **67**

ОБЩЕЕ КОЛИЧЕСТВО ВИРТУАЛЬНЫХ МАШИН **872**

~1 млн.
ПОЛЬЗОВАТЕЛЕЙ

2
ОБЪЕКТЫ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

25
ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

6 000
АВТОМАТИЗИРОВАННЫХ РАБОЧИХ МЕСТ ПРАВИТЕЛЬСТВА ОРЕНБУРСГКОЙ ОБЛАСТИ

ФУНКЦИОНАЛЬНАЯ СХЕМА ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ В ЦОД ПРАВИТЕЛЬСТВА ОРЕНБУРГСКОЙ ОБЛАСТИ

Центр мониторинга и реагирования на инциденты информационной безопасности Оренбургской области - это группа специалистов, которые непрерывно осуществляют контроль за сообщениями, поступающими от средств защиты

SIEM
класс программных продуктов, предназначенных для сбора и анализа информации о событиях безопасности

- Платформа киберразведки
- Средства антивирусной защиты
- СКЗИ для создания защищенных сетей
- Межсетевой экран

- Система обнаружения вторжений
- Система мониторинга ИТ-инфраструктуры
- Средства фильтрации трафика прикладного уровня

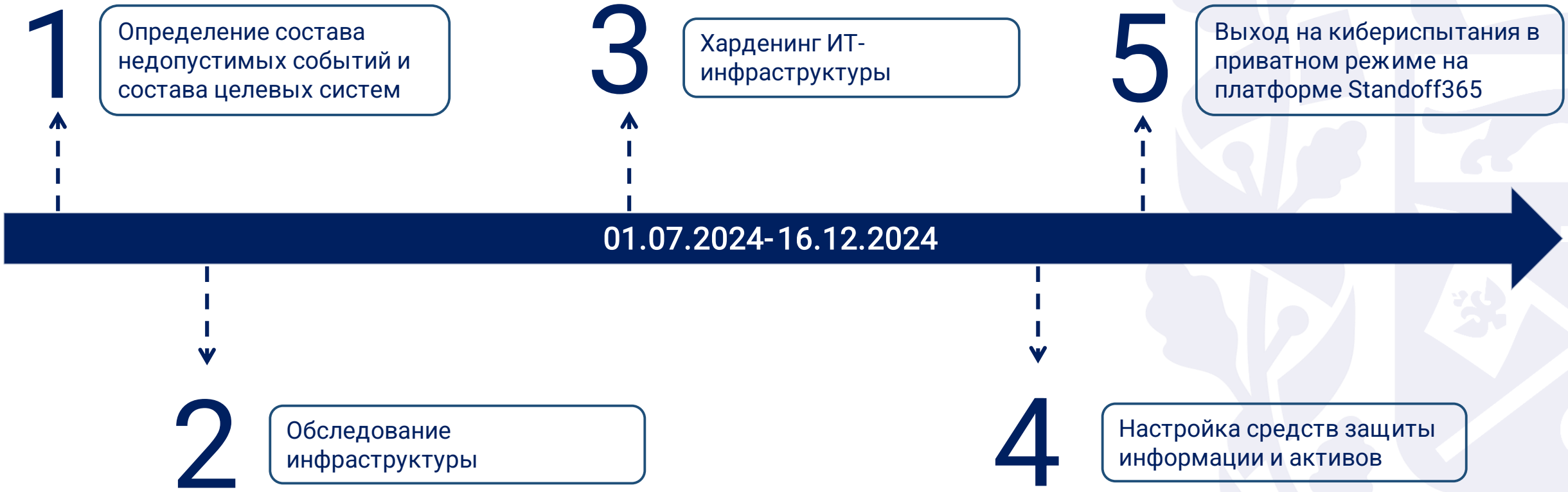
- Аттестация
- Система комплексного мониторинга ИБ

Государственные информационные системы/информационные системы

ЗАДАЧИ

- ✓ Выработать подход к обеспечению киберзащиты, который позволит оптимально распределять усилия внутри команды и предотвращать наступление недопустимых событий
- ✓ Донастроить процессы для кибербезопасности, на которых в дальнейшем можно будет развивать безопасность других информационных систем и сервисов Оренбургской области
- ✓ Для выбранных систем донастроить систему защиты, которая позволит увидеть действия хакеров на самых ранних этапах и отреагировать до наступления недопустимого события
- ✓ Сделать кибербезопасность измеримой и убедиться в выстроенной защите от недопустимого события на кибериспытаниях. Превратить кибериспытания в неотъемлемый элемент стратегии кибербезопасности региона

ПРОЕКТ СОСТОЯЛ ИЗ ЭТАПОВ:



1 ЭТАП

Определение состава недопустимых событий и состава целевых систем

Минцифры Оренбургской области составило перечень недопустимых событий исходя из критичности государственных информационных систем
Перечень целевых систем, рассматриваемых в рамках согласованных недопустимых событий был ограничен для оптимизации сроков проекта

Проект нацелен на две государственные информационные системы:

- ГИС «Единый личный кабинет Оренбургской области»
- ГИС «Единая централизованная система управления финансово-хозяйственной деятельности Оренбургской области»

Целевая система (ЦС) — Целевая система (ЦС) – объект инфраструктуры, при атаке на который может произойти недопустимое для организации событие. Эти системы являются конечной целью злоумышленника при реализации недопустимого события

В качестве ЦС признаны:

- платформа виртуализации на которой работают сервера ГИС
- балансировщик, через который пользователи подключаются к web-серверам ГИС
- сетевое оборудование, через которое проходит весь трафик

2 ЭТАП

Обследование инфраструктуры

- обследование целевых систем
- составление карты сети и получение всех конфигураций оборудования
- определение ключевых систем и их подсети
- сканирование сети, определение в них ключевых активов;
- определение состава используемых средств защиты и ключевых элементов ИТ-инфраструктуры
- разработка скрипта для сбора информации с инфраструктурных систем и сервисов
- проведение анализа защищенности как внутреннего так и внешнего и экспресс-анализ защищенности сетевого периметра

Ключевая система – это объект в информационной инфраструктуре, несанкционированный доступ к которому или воздействие на который необходимы нарушителю, чтобы развить атаку на целевую систему, или такая система, взлом которой существенно упростит сценарий атаки или повысит ее эффективность

3 ЭТАП

Харденинг ит-инфраструктуры

По итогам обследования приоритизированных целевых и ключевых систем определены задачи для харденинга ИТ-инфраструктуры и перечня активов систем, которые необходимо поставить на мониторинг

~350 задач по харденингу

Харденинг нацелен:

- платформа виртуализации на которой работают сервера ГИС
- балансировщик, через который пользователи подключаются к web-серверам ГИС
- сетевое оборудование, через которое проходит весь трафик
- средства защиты информации

Hardening — это процесс настройки системы для повышения её безопасности путём уменьшения уязвимостей. Он включает в себя ряд мероприятий, направленных на минимизацию потенциальных рисков и атак, которым может подвергнуться система

4 ЭТАП

Настройка средств защиты и активов

- на платформе управления событиями информационной безопасности организован мониторинг для целевых и ключевых систем, в которых ранее отсутствовал контроль за активами
- проведена настройка, снижающие количество ложноположительных срабатываний
- проведен аудит активов целевых и ключевых систем на наличие трендовых уязвимостей на платформе автоматизации процессов информационной безопасности
- проведен аудит используемых веб-приложений и настроек системы защиты приложений от несанкционированного доступ
- определены точки съема трафика для системы поведенческого анализа сетевого трафика для обнаружения скрытых кибератак
- проведен аудит источников для системы многопоточной проверки файловых ресурсов, подключена почтовая система

СОБЫТИЯ

2500EPS → 9000EPS

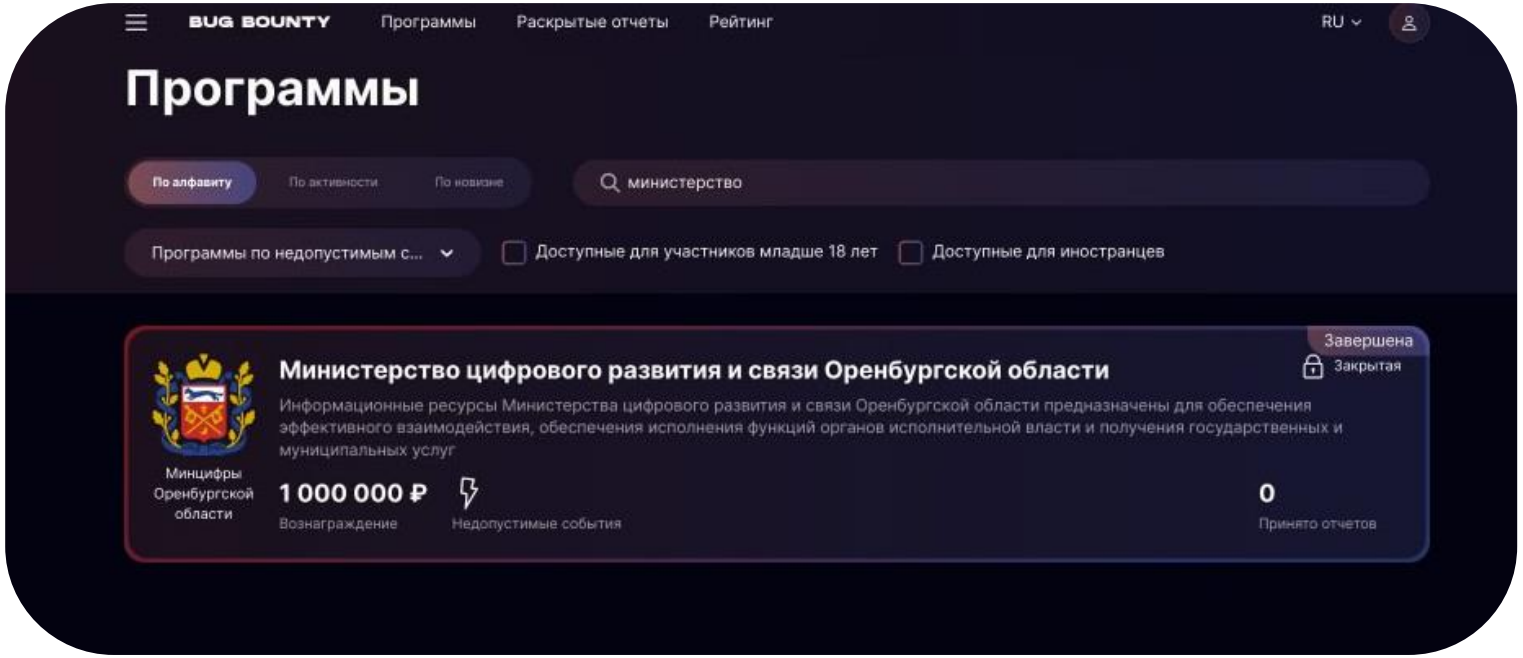
АКТИВЫ

450 → 636

Количество активов по потоку событий - 2690

5 ЭТАП

Выход на кибериспытания в приватном режиме на платформе standoff365



2,5 месяца

Срок проведения кибериспытаний

1 млн руб.

Вознаграждение

0

Количество отчетов о реализации недопустимых событий на платформе BugBounty Standoff365

Динамика показателей работы центра мониторинга и реагирования на инциденты информационной безопасности

ПОКАЗАТЕЛЬ	2022 год	2023 год	2024 год
Отработанные события информационной безопасности	48 млн	93 млн	~1млрд
Количество ГИС	22	25	25
Количество ИС (не являются ГИС)	-	-	8
Количество инцидентов ИБ	19	12	30
Количество рабочих мест структуры Правительства, о которых информация поступает в SOC	4 000	5 000	6 000
Охват подключенных элементов ГИС	92%	95%	100%
Количество внешних аудитов ГИС	-	-	7
Публичные программы выявления уязвимостей в программных сервисах информационных систем и информационных ресурсах Оренбургской области с привлечением специалистов за вознаграждение (Bug Bounty)	-	-	1

Минцифра
Оренбургской области
digital.orb.ru

СПАСИБО ЗА ВНИМАНИЕ!