Министерство по развитию
информационных технологий
и коммуникаций Республики Узбекистан

Центр информационной безопасности
и содействия в обеспечении
общественного порядка

СТРАТЕГИЯ ДЕЙСТВИЙ
2017-2021

О деятельности Центра информационной безопасности и содействия в обеспечении общественного порядка Министерства по развитию информационных технологий и коммуникаций Республики Узбекистан

Начальник департамента безопасности сетей телекоммуникаций и кибербезопасности Центра информационной безопасности и содействия в обеспечении общественного порядка

Гафуров Шарифжон Рахимович

ЦЕНТР ИНФОРМАЦИОННОЙ И ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ

ВВЕДЕНИЕ

Согласно Стратегии действий по пяти приоритетным направлениям Республики Узбекистан, одним из приоритетных задач является совершенствование системы обеспечения информационной безопасности и защиты информации, своевременное и адекватное противодействие угрозам в информационной сфере.

Центр информационной безопасности и содействия в обеспечении общественного порядка совершенствует все вопросы, касающиеся развития сферы обеспечения информационной безопасности.

ЦЕНТР ИНФОРМАЦИОННОЙ И ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ

ИСТОРИЯ ЦЕНТРА

Центр был создан в 2013 году под названием «Центр обеспечения информационной безопасности» при Министерстве по развитию информационных технологий и коммуникаций Республики Узбекистан.

CENTER OF INFORMATION SECURITY

ЦЕНТР ИНФОРМАЦИОННОЙ И ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ

ИСТОРИЯ ЦЕНТРА

С 2017 года был преобразован в Центр информационной безопасности и содействия в обеспечении общественного порядка Министерства по развитию информационных технологий и коммуникаций Республики Узбекистан.

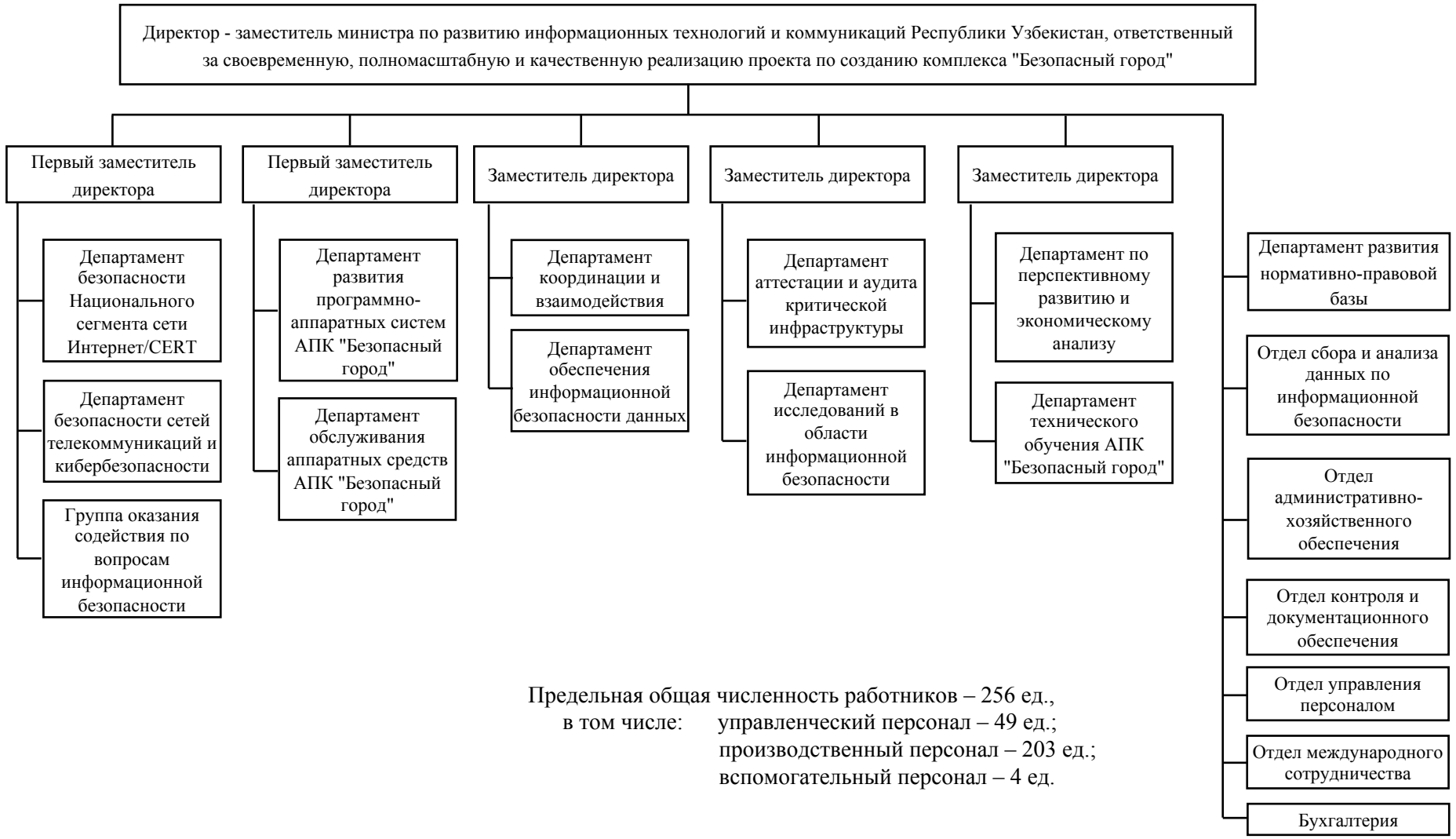
ЦЕНТР ИНФОРМАЦИОННОЙ И ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ

ЗАДАЧИ ЦЕНТРА

- Сбор, анализ и накопление данных о современных угрозах информационной безопасности;
- Проведение аттестации объектов информатизации;
- Координация деятельности государственных органов и иных организаций;
- Своевременное оповещение национальных пользователей Интернета;
- Создание аппаратно – программного комплекса «Безопасный город»;
- Выработка концепции по созданию АПК «Безопасный город»;
- Формирование единой дежурно – диспетчерской службы.

ЦЕНТР ИНФОРМАЦИОННОЙ И ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ

Структура Центра информационной безопасности и содействия в обеспечении общественного порядка



Предельная общая численность работников – 256 ед.,
в том числе: управленческий персонал – 49 ед.;
производственный персонал – 203 ед.;
вспомогательный персонал – 4 ед.

ЦЕНТР ИНФОРМАЦИОННОЙ И ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ

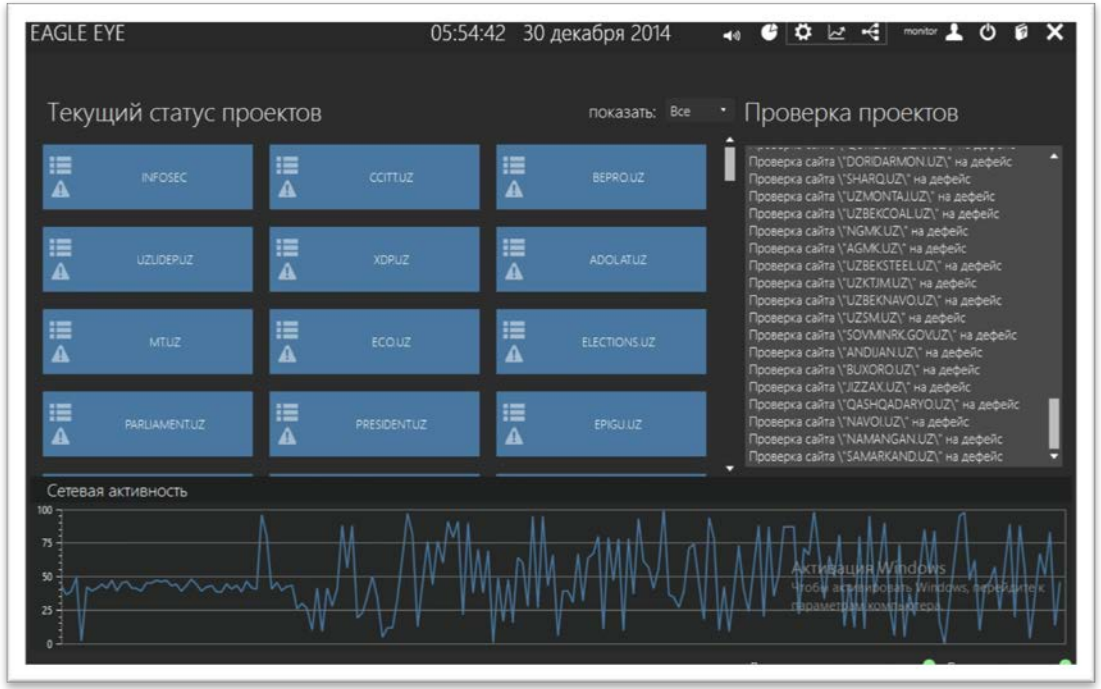
Роль группы CERT

- Мониторинг событий ИБ;
- Оповещение и предупреждение;
- Анализ и обработка инцидентов;
- Реакция на инциденты:
  - *Определение цели и вектора атаки;*
  - *Уменьшение последствий;*
- Координация реагирования на инциденты.

ЦЕНТР ИНФОРМАЦИОННОЙ И ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ

ПРОЕКТЫ ЦЕНТРА

2014 году разработана и внедрена в эксплуатацию «Система оповещения и предотвращения проникновения к сайтам сети Интернет».



Главной целью Системы является оперативное выявление и реагирование на попытки несанкционированного доступа к веб-сайтам государственных органов.

ЦЕНТР ИНФОРМАЦИОННОЙ И ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ

ПРОЕКТЫ ЦЕНТРА

В декабре 2015 года Центром запущен 2 этап «Системы обнаружения инцидентов на информационных ресурсах доменной зоны .UZ».

ЦЕНТР ИНФОРМАЦИОННОЙ И ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ

ПРОЕКТЫ ЦЕНТРА

В 2017 году Центром также реализованы проекты, а именно:

- Система мониторинга комплексов информационных систем и базы данных системы «Электронное правительство» на предмет требований информационной безопасности (система мониторинга КИС и БД);
- Информационная система по мониторингу событий информационной безопасности в межведомственной сети передачи данных электронное правительство (система мониторинга МСПД);
- Система автоматического оповещения владельцев серверов по выявленным уязвимостям в установленном программном обеспечении (система оповещения).

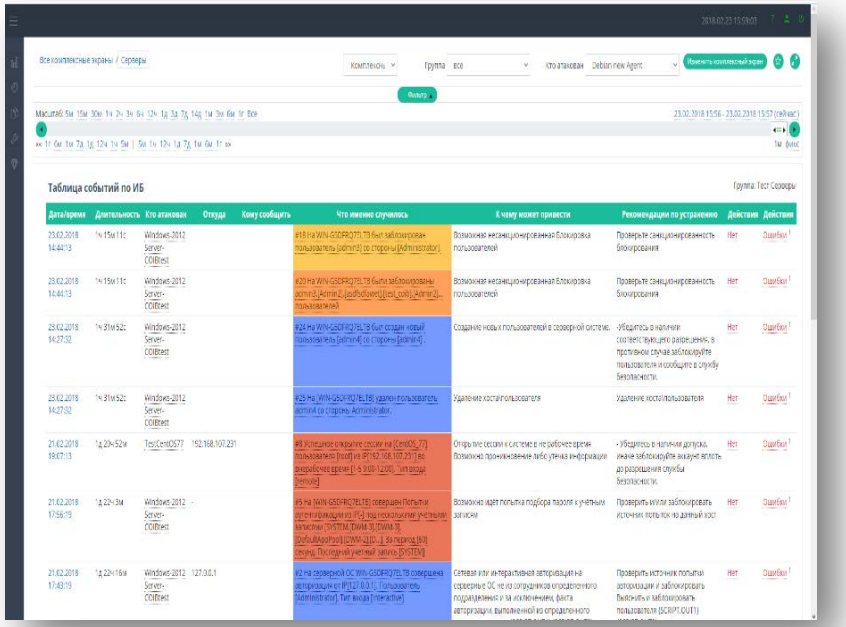
ЦЕНТР ИНФОРМАЦИОННОЙ И ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ

ПРОЕКТЫ ЦЕНТРА

Система мониторинга КИС и БД предназначена для мониторинга событий информационной безопасности в комплексов информационных систем и баз данных «Электронного правительство».

Основные задачи системы:

- сбор, обработка и анализ событий безопасности, поступающих в систему из множества источников;
- обнаружение в режиме реального времени атак и нарушений критериев и политик безопасности;
- формирование отчетных документов.



ЦЕНТР ИНФОРМАЦИОННОЙ И ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ

ПРОЕКТЫ ЦЕНТРА

Система мониторинга МСПД предназначена для мониторинга событий информационной безопасности в межведомственном сети передачи данных электронного правительства.

Основные задачи системы:

-централизованный сбор и обработку событий ИБ в режиме реального времени;

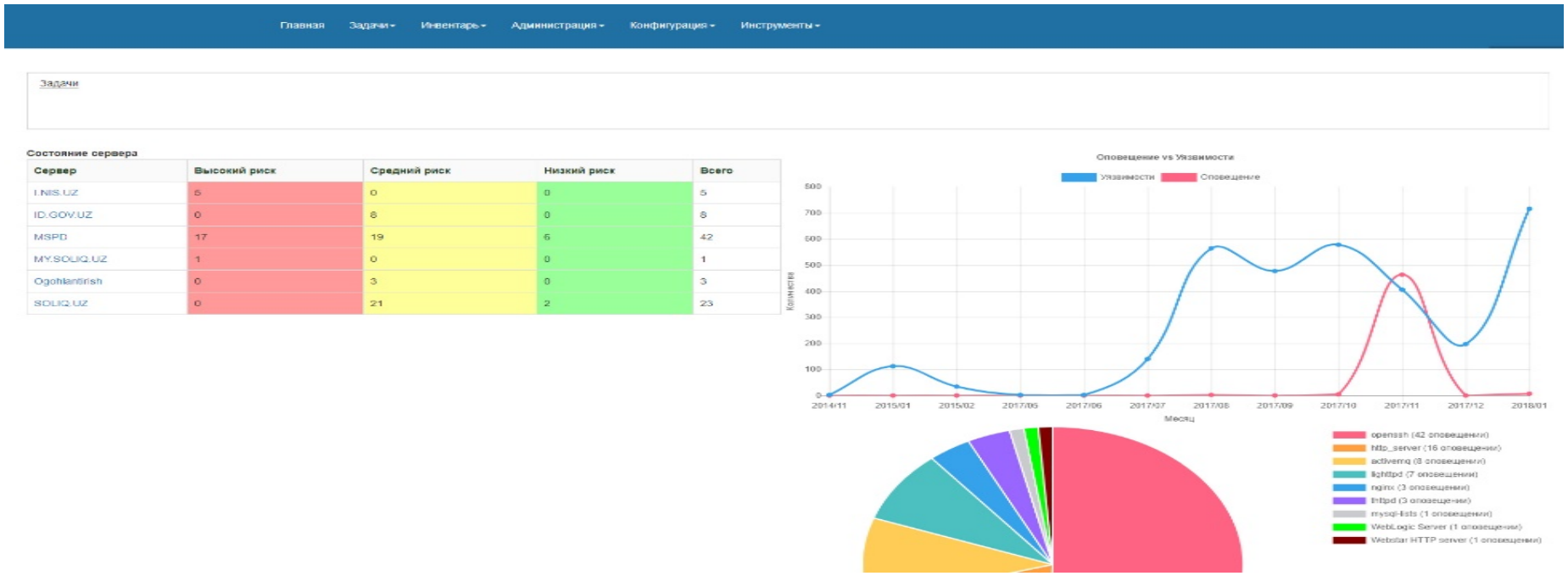
-долговременное хранение событий и инцидентов Иб для формирования доказательной базы;

-своевременное выявление инцидентов ИБ.

ЦЕНТР ИНФОРМАЦИОННОЙ И ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ

ПРОЕКТЫ ЦЕНТРА

Системы оповещения предназначена для создания централизованного перемещения, хранения и накопления данных, необходимых для автоматического определения на предмет наличия уязвимостей в программном обеспечении, установленном на серверах, а также автоматическое сопоставление их с базами данных уязвимостей публикуемых официальными источниками и оповещение владельцев серверов.



Сервер	Высокий риск	Средний риск	Низкий риск	Всего
I.NIS.UZ	5	0	0	5
ID.GOV.UZ	0	8	0	8
MSPD	17	19	6	42
MY.SOLIQ.UZ	1	0	0	1
Ogohlantirish	0	3	0	3
SOLIQ.UZ	0	21	2	23

ЦЕНТР ИНФОРМАЦИОННОЙ И ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ

МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО

KISA
Korea Internet & Security Agency

KZ-CERT

CN CERT/CC
国家互联网应急中心

SingCERT
Singapore Computer Emergency Response Team

JPCERT CC®
Japan Computer Emergency Response Team
Coordination Center
JPCERT コーディネーションセンター

HKCERT

certin
enhancing cyber security in India

ЦЕНТР ИНФОРМАЦИОННОЙ И ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ

ОЖИДАЕМЫЙ РЕЗУЛЬТАТ ДЕЯТЕЛЬНОСТИ ЦЕНТРА

- Формирование единой системы информационной безопасности государственных информационных ресурсов и баз данных в рамках системы «Электронное правительство»;
- Координация действий операторов, провайдеров и других субъектов национального сегмента сети Интернет по вопросам предотвращения правонарушений в области использования компьютерных и информационных технологий;
- Введение системы аттестации объектов информатизации в рамках внедрения системы «Электронное правительство» в соответствии с действующим законодательством;
- Создание единого аппаратно – программного комплекса «Безопасный город» для организации полноценной системы обеспечения общественной безопасности и правопорядка.

БЛАГОДАРЮ ЗА ВНИМАНИЕ!

Центр информационной безопасности и содействие в обеспечении общественного порядка Министерства по развитию информационных технологий и коммуникаций Республики Узбекистан

Республика Узбекистан, г.Ташкент 100115, ул.Кирк киз, 10А
Телефон: (99871) 277 97 78
Факс: (99871) 277 70 66
www.infosec.uz | www.uzcert.uz | www.pki.uz