Возможные роли центров ГосСОПКА в обеспечении безопасности критической информационной инфраструктуры

Анатолий Грачев
(НКЦКИ)

Восприятие роли Центра ГосСОПКА: Информационный хаб

- Приём сообщений
- Переадресация запросов
- Накопление информации
- Наблюдение за событиями
- Подготовка отчетов и уведомлений
- Учет инцидентов
- Информирование об угрозах
- Связь с ГосСОПКА

ГОССОПКА

Роль: Помощник архитектора системы обеспечения информационной безопасности

- Знание конфигураций и настроек защищаемых объектов и средств защиты информации – основа эффективного мониторинга и реагирования
- Профилирование защищаемых систем и средств по результатам анализа инцидентов – необходимый и постоянный процесс
- Методическое сопровождение и внедрение успешного практического опыта (best practice) – значимая функция в системе управления конфигурациями объекта и обеспечении защищенности

Роль: Инспектор
зоны ответственности центра ГосСОПКА

- Формирование и поддержание в актуальном состоянии сведений о зоне ответственности центра ГосСОПКА
- Передача в НКЦКИ сведений о зоне ответственности центра, своевременное информирование об изменениях в жизненном цикле активов/сервисов/систем
- Обогащение сведений об ИТ-активах дополнительным контекстом

Роль: Исследователь
защищенности инфраструктуры субъекта КИИ

- Проведение мероприятий по выявлению уязвимостей и проблемных конфигураций в ИТ-активах
- Моделирование угроз безопасности информации, адаптация существующей модели угроз
- Выработка компенсирующих мер защиты информации и участие в устранении уязвимостей и рисков информационной безопасности
- Анализ результатов устранения компьютерных инцидентов, корректировка мер по недопущению повторения инцидента

ГОССОПКА

Роль: Координатор
сил и средств обнаружения, предупреждения и ликвидации последствий компьютерных атак

- Обеспечение деятельности по приему, обработке, учету и хранению запросов и уведомлений о компьютерных инцидентах
- Управление задачами сил реагирования на компьютерный инцидент или угрозу, оптимизация процессов реагирования
- Контроль использования средств обнаружения и реагирования на компьютерные инциденты
- Установление причин возникновения компьютерного инцидента
- Анализ последствий компьютерного инцидента: масштабов вредоносного воздействия и причиненного ущерба

ГОССОПКА

Роль: Дежурный оператор средств обнаружения атак и реагирования на компьютерные инциденты

- Мониторинг событий о компьютерных атаках и выявление возможного инцидента
- Анализ сведений об инциденте и его регистрация
- Принятие решения о реагировании на компьютерный инцидент
- Реагирование на инциденты и ликвидация их последствий
- Взаимодействие с уполномоченными лицами и Национальным координационным центром по компьютерным инцидентам
- Эксплуатация средств защиты информации при нейтрализации атаки
- Подготовка отчетных материалов

ГОССОПКА

Роль: Разведчик
актуальных угроз безопасности информации

- Сбор и анализ информационно-аналитических материалов об актуальных угрозах
- Поддержка локальной базы данных угроз и уязвимостей
- Организация работы с дополнительными источниками информации об угрозах по подписке
- Обогащение информации об ИТ-активах сведениями об уязвимостях
- Проактивный поиск угроз, выявление в «ручном режиме» фактов компрометации систем
- Информационно-аналитическая функция

ГОССОПКА

Роль: Проводник
в культуру информационной безопасности

- Разработка программ обучения и повышения осведомленности операторов и пользователей систем
- Управление обучением, проверка знаний
- Имитация действий злоумышленников, выявление наименее осведомленных пользователей и «проблемных» зон

ГОССОПКА

ГОССОПКА

Обнаружение. Предупреждение. Ликвидация.