ДИТ

Культура кибербезопасности субъекта КИИ

Валерий Комаров, начальник отдела обеспечения осведомленности, ДИТ Москвы

Киберкультура? А зачем?

ДИТ

Предотвратить дешевле, чем устранять последствия!

- Профилактика причин возникновения компьютерного инцидента
- Реагирование на компьютерные инциденты в ходе эксплуатации ЗОКИИ
- Обеспечение действий в нештатных ситуациях в ходе эксплуатации ЗОКИИ
- Ликвидация последствий компьютерных атак
- Минимизация последствий компьютерных инцидентов

Способы формирования культуры безопасного обеспечения функционирования и эксплуатации значимого объекта КИИ

- Обучение обучения персонала ЗОКИИ
- Информирование персонала об угрозах безопасности информации, о правилах безопасной эксплуатации значимого объекта
- Доведение до персонала требований по обеспечению безопасности значимых объектов, а также положений организационно-распорядительных документов по безопасности значимых объектов в части, их касающейся; обучение персонала правилам эксплуатации отдельных средств защиты информации, включая проведение практических занятий с персоналом
- Субъект КИИ не реже одного раза в год организует и проводит тренировки по отработке мероприятий плана
- Контроль осведомленности персонала об угрозах безопасности информации и уровня знаний персонала по вопросам обеспечения безопасности критической информационной инфраструктуры

А что с подрядными и сторонними организациями?

Представители организаций, привлекаемых субъектом критической информационной инфраструктуры для эксплуатации, обеспечения функционирования значимых объектов критической информационной инфраструктуры и (или) для обеспечения их безопасности, должны быть ознакомлены с организационно-распорядительными документами по безопасности значимых объектов

Киберкультура важна на всех стадиях жизненного цикла ЗОКИИ

Обеспечение безопасности при создании (модернизации) должно предусматривать

- Категорирование до утверждения ТЗ на создание ЗОКИИ
- Пересмотр категории значимости при модернизации
- Согласование с ФСТЭК подключение ЗОКИИ к сети электросвязи общего пользования
- Уведомление ФСТЭК России об изменении сведений о результатах категорирования при модернизации, в том числе и в случаях без изменения категории значимости

Обеспечение безопасности при выводе из эксплуатации должно предусматривать

- Архивирование информации, содержащейся в значимом объекте
- Уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации
- Уничтожение или архивирование данных об архитектуре и конфигурации значимого объекта
- Архивирование или уничтожение эксплуатационной документации на значимый объект и его подсистему безопасности и организационно-распорядительных документов по безопасности значимого объекта

Компьютерный инцидент на ЗОКИИ — нарушение функционирования, повлекшее тяжкие последствия для страны!

- План мероприятий по обеспечению безопасности
- План антитеррор
- План по обеспечению пожарной безопасности
- План мероприятий по реагированию на компьютерные инциденты ЗОКИИ
- План мероприятий по обеспечению промышленной безопасности
- План эвакуации
- План мероприятий по действиям в нештатной ситуации
- План мероприятий по локализации аварий и последствий

Вы реально готовы устранять компьютерный инцидент в условиях пожара или в очаге химического поражения?

Планы реагирования учитывают вывод резервных систем на ремонт?

- План вывода в ремонт

ДИТ

Всегда на связи!

mos.ru/dit