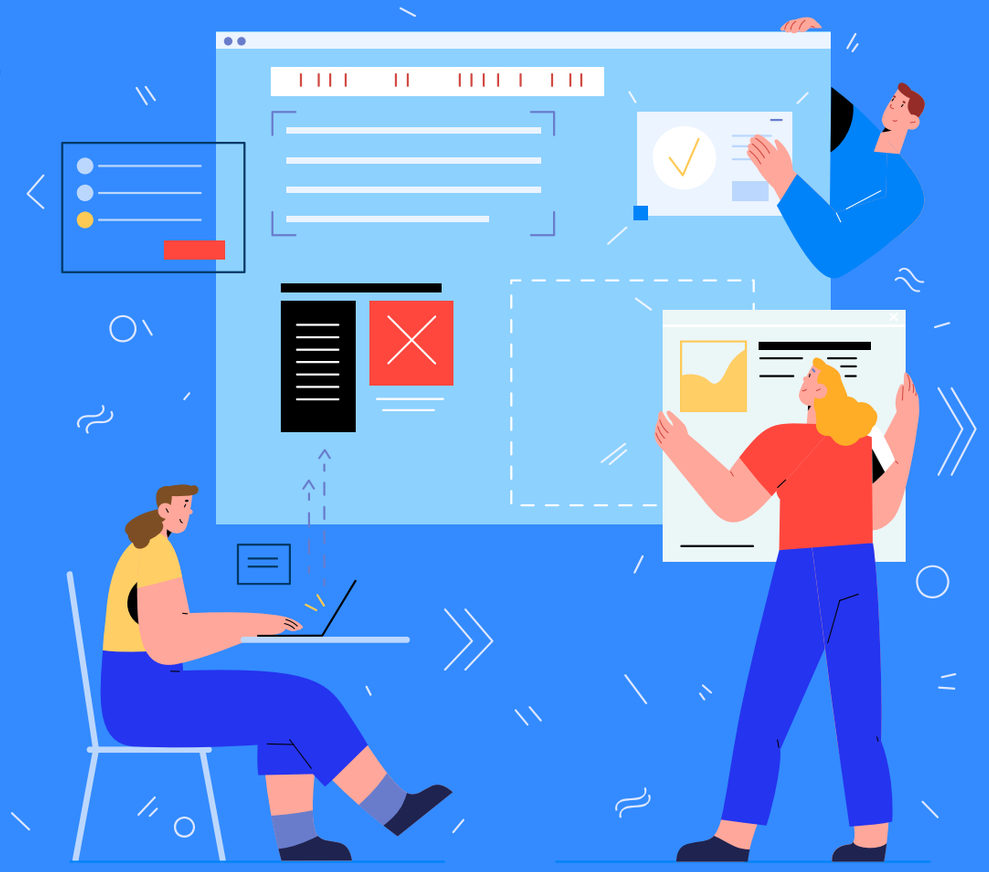
ДИТ

Что должен включать в себя план реагирования на инциденты ИБ на промышленном предприятии?

Управление информационной безопасности



В.В. Комаров

2021

ДИТ

Методическая база

Приказ ФСБ России от 19.06.2019 № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры РФ»

Рекомендации ФСТЭК России по подготовке планов мероприятий, реализуемых субъектами критической информационной инфраструктуры РФ при установлении в отношении принадлежащих им объектов критической информационной инфраструктуры уровней опасности проведения целевых компьютерных атак

Методические рекомендации НКЦКИ по установлению причин и ликвидации последствий компьютерных инцидентов

Проекты национальных стандартов ГОСТ Р:

«Управление инцидентами, связанными с безопасностью информации. Руководство по планированию и подготовке к реагированию на инциденты»

«Управление инцидентами, связанными с безопасностью информации. Руководство по реагированию на инциденты в сфере информационных и компьютерных технологий»

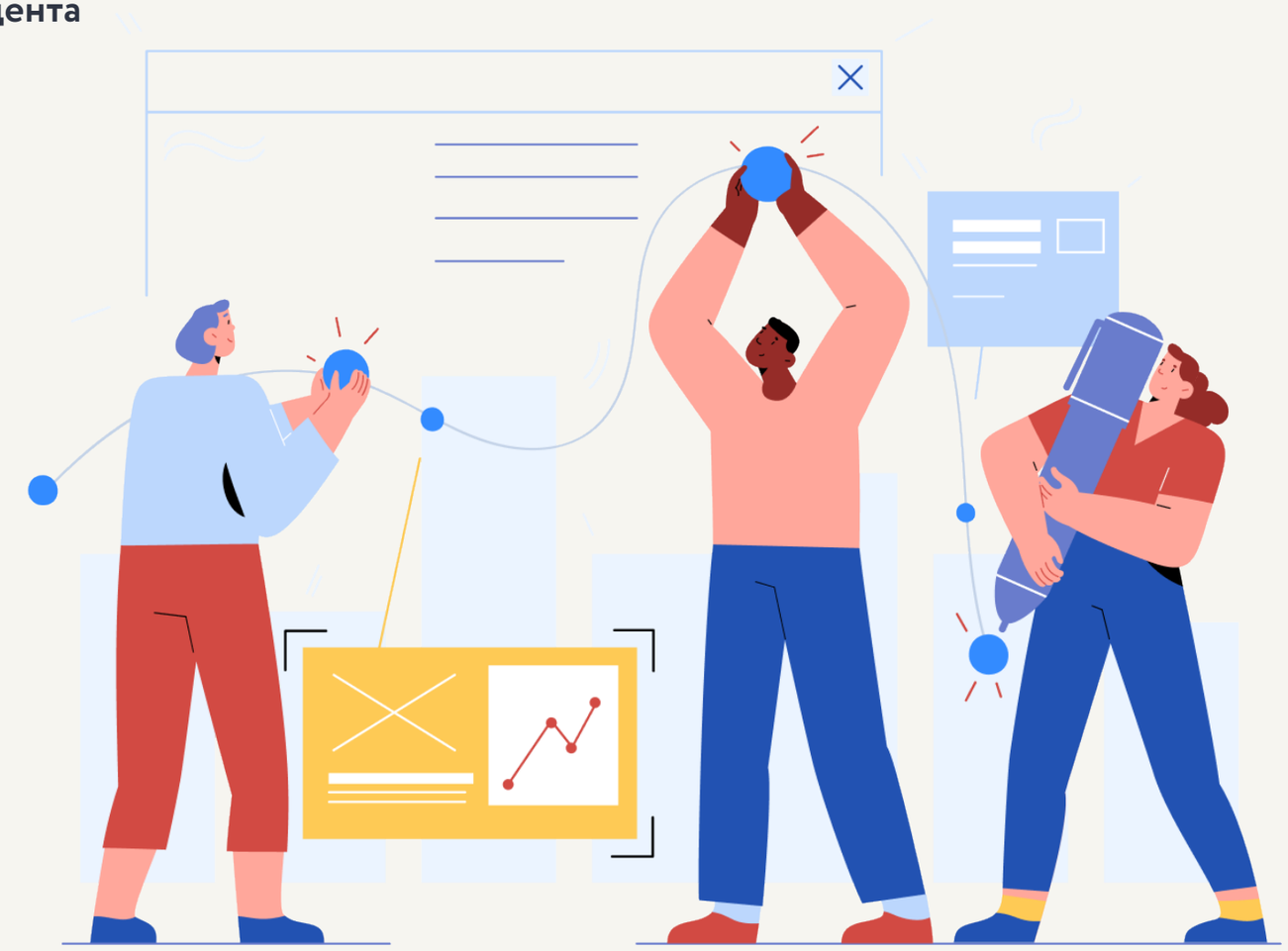
«Управление инцидентами, связанными с безопасностью информации. Принципы менеджмента инцидентов»

Методические рекомендации НКЦКИ по разработке плана реагирования на компьютерные инциденты

ДИТ

Этапы плана реагирования

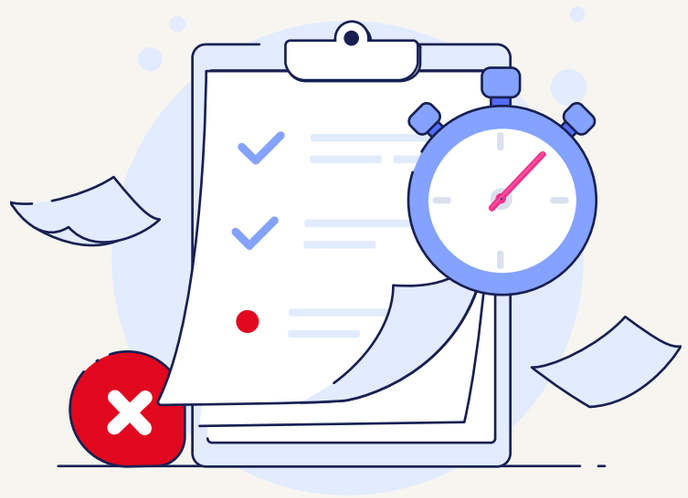
1. Выявление (обнаружение) компьютерного инцидента
2. Информирование внутри предприятия
3. Реагирование на компьютерный инцидент
4. Регистрация компьютерного инцидента и взаимодействие с НКЦКИ
5. Сбор и подготовка информации о компьютерном инциденте
6. Обучение задействованного персонала предприятия и подрядчиков
7. Контроль и управление процессами



ДИТ

Эффективность плана реагирования обеспечивают действия:

- Определяем источники информации о компьютерном инциденте и регламентируем работу с этой информацией
- Устанавливаем каналы коммуникации и формат обмена информацией о компьютерном инциденте
- Назначаем и обучаем работников, задействованных в процессах реагирования на компьютерные инциденты
- Поддерживаем процессы в актуальном состоянии (перевод на удаленную работу, изменения в кадровом составе, смена поставщиков и т.д.)
- Фиксируем выполнение всех обязательных требований законодательства
- Проводим тренировки по реагированию на компьютерные инциденты и корректировку плановых действий



ДИТ

Проблемы при разработке плана реагирования

- **Расчет времени выполнения этапов планов реагирования на компьютерные инциденты**
- **Взаимодействие с поставщиками услуг по эксплуатации и обеспечению функционирования предприятия**
- **Отсутствие персонала с навыками ИТ и защиты информации**
- **Недостаточность каналов связи и отсутствие их резервирования**
- **Недостоверная контактная информация задействованных работников**

Сложность организации тренировок:

- **Согласование с эксплуатирующими подразделениями;**
- **Большая длительность тренировки;**
- **Структура управления силами предприятия при аварийных ситуациях;**
- **Сильная загруженность персонала основными задачами по восстановлению объекта информатизации при компьютерном инциденте**

Эти проблемы приводят к упрощенным планам по реагированию случая компьютерного инцидента (не учитывается комплексный характер нарушения работы предприятия)

ДИТ

Всегда на связи!

mos.ru/dit

vk.com/ditmos

twitter.com/ditmos

facebook.com/ditmos

ok.ru/ditmos