Безопасность объектов КИИ

Анализ методик по разработке планов реагирования на инциденты ИБ объектов КИИ

Гаращенко Дмитрий Владимирович

НКЦКИ

- **Национальный координационный центр по компьютерным инцидентам**

  - План реагирования на компьютерные инциденты и принятие мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов КИИ РФ (далее – План реагирования)

ФСТЭК РФ

- **Федеральная служба по техническому и экспортному контролю Российской Федерации**

- План мероприятий, реализуемый субъектами КИИ РФ при установлении в отношении принадлежащих им объектов уровней опасности проведения целевых атак. (далее – План мероприятий)

План реагирования

- **Типичный план**

Объект (КИИ)

События

Ответственные

Мероприятия

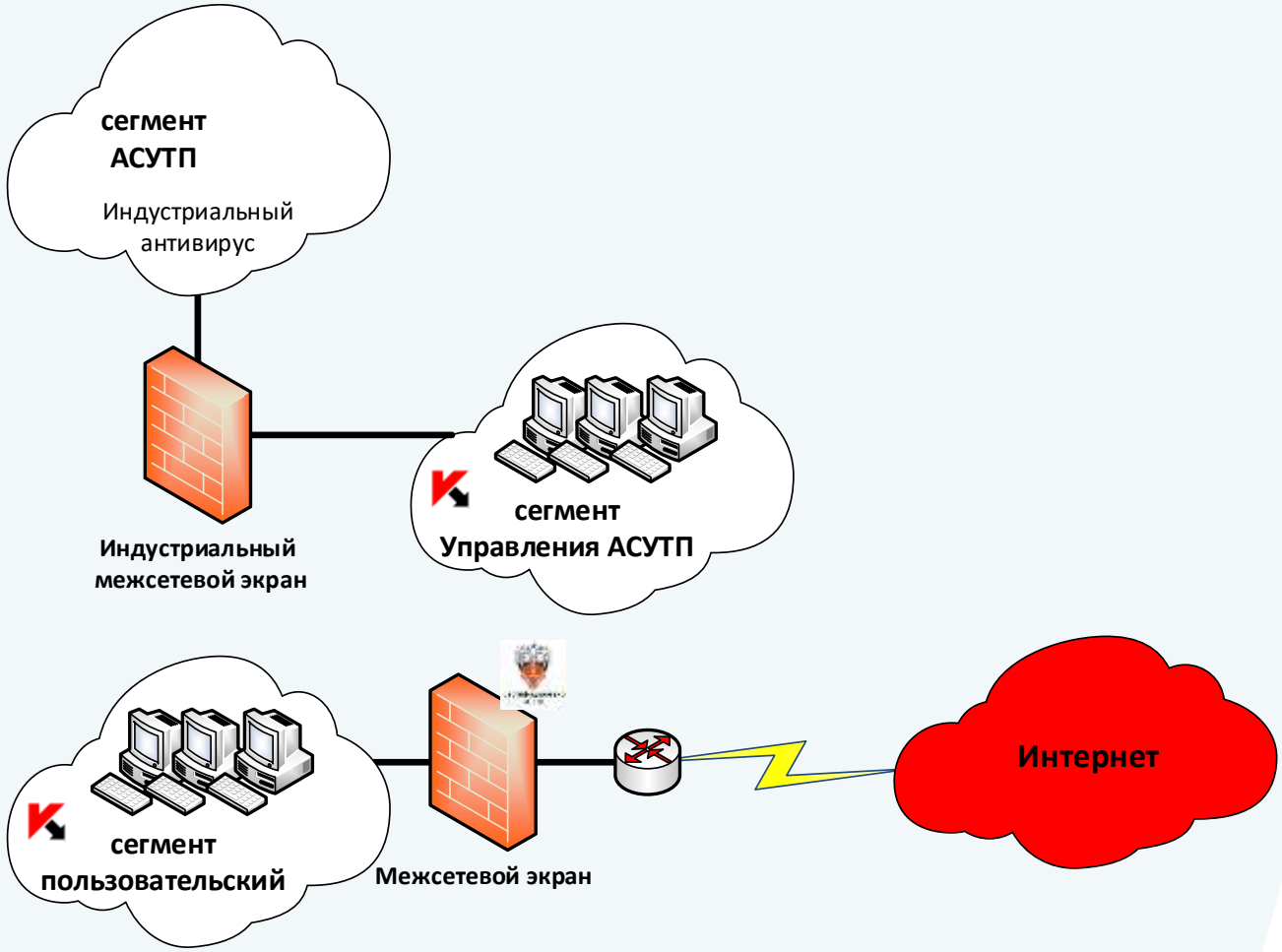
План реагирования

❖События (виды атак)

- Отказ в обслуживании
- Несанкционированный доступ
- Утечка данных
- Модификация данных
- Нарушение функционирования технических средств
- Несанкционированное использование вычислительных ресурсов

План реагирования

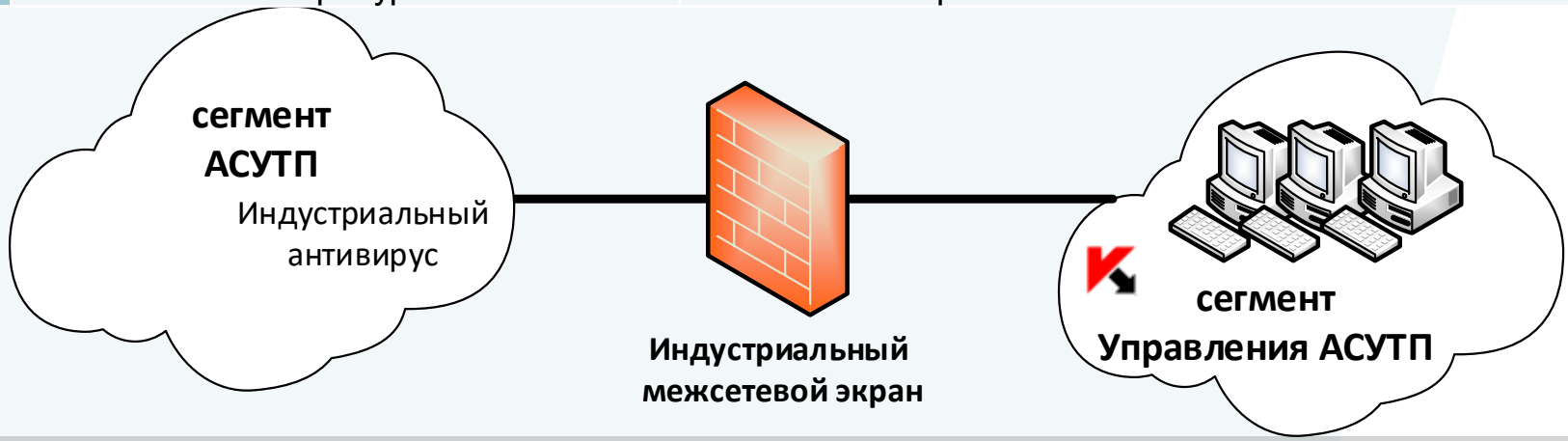
Типичная схема



План реагирования

Актуальность угроз

№	События	Источник нарушения
1	Отказ в обслуживании	Вирусное ПО – не применимо
2	Несанкционированный доступ	Только физическое присутствие нарушителя на объекте – не применимо
3	Утечка данных (нарушение конфиденциальности)	Тех поддержка при перепрошивке или перезоливки ПО - применимо
4	Модификация (подмена) данных	Тех поддержка при перепрошивке или перезоливки ПО, вирусное ПО - применимо
5	Нарушение функционирования технических средств	Только физическое присутствие нарушителя на объекте – не применимо
6	Несанкционированное использование вычислительных ресурсов объекта	Только физическое присутствие нарушителя на объекте – не применимо



План реагирования

- Техподдержка потенциальная угроза

Максимальный контроль действий и проверка устанавливаемого ПО

План мероприятий

❖Режимы опасности (светофор)

Устанавливаются три уровня опасности:
повышенный («желтый») - при получении данных о подготовке целевой компьютерной атаки без сроков ее проведения;

высокий («оранжевый») - при получении данных о возможном проведении целевой компьютерной атаки в краткосрочной перспективе;

критический («красный») - при получении данных, что принято решение о проведении целевой компьютерной атаки в краткосрочной перспективе.

План мероприятий

- **Какие из предложенных мероприятий вызвали вопросы**

Организация круглосуточного мониторинга информационной безопасности объектов КИИ и круглосуточного дежурства групп оперативного реагирования на компьютерные инциденты из числа наиболее подготовленных специалистов субъекта КИИ, предусматривающего круглосуточную готовность к реализации мер по обеспечению безопасности объектов КИИ.

MaxPatrol SIEM

План мероприятий

- **Какие из предложенных мероприятий вызвали вопросы**

Реализация мер обеспечения бесперебойного функционирования субъекта КИИ при осуществлении в отношении принадлежащих ему объектов КИИ компьютерной атаки.

План мероприятий

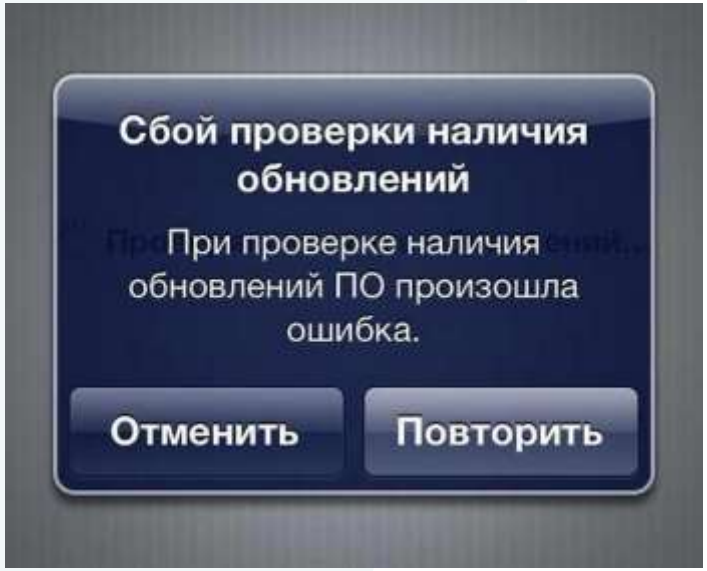
- Какие из предложенных мероприятий вызвали вопросы

Реализация временного ограничения доступа к объектам КИИ.

План мероприятий

- **Какие из предложенных мероприятий вызвали вопросы**

Проверка актуальности версий программного обеспечения средств защиты информации (далее - СЗИ), применяемых для обеспечения безопасности объектов КИИ, а также их баз данных, осуществляемая не реже, чем раз в день, при наличии их обновлений - незамедлительное применение этих обновлений



План мероприятий

- **Какие из предложенных мероприятий вызвали вопросы**

Минимизация состава программного обеспечения, установленного на соответствующих узлах сети, с учетом технологической необходимости.

План мероприятий

- Какие из предложенных мероприятий вызвали вопросы

Исключение из состава объектов КИИ беспроводных сетей.

План мероприятий

- **Какие из предложенных мероприятий вызвали вопросы**

Настройка средств антивирусной защиты, средств предотвращения утечек данных, систем обнаружения вторжений и систем управления событиями информационной безопасности, применяемых для обеспечения безопасности объектов защиты, на максимально детализированный анализ соответствующих данных.

План мероприятий

- **Какие из предложенных мероприятий вызвали вопросы**

Ограничение до минимально необходимого количества автоматизированных рабочих мест, на которых реализованы сервисы электронной почты, и обеспечение контроля почтовых вложений на предмет наличия вредоносного программного обеспечения;

План мероприятий

- **Какие из предложенных мероприятий вызвали вопросы**

Обеспечение ежедневного резервирования информации, обрабатываемой в объектах КИИ, а также хранения резервных копий, исключающих несанкционированный доступ к ним в результате компьютерных атак.

План мероприятий

- **Какие из предложенных мероприятий вызвали вопросы**

Реализация многофакторной аутентификации для удаленного доступа администраторов к объектам КИИ

План мероприятий

- Какие из предложенных мероприятий вызвали вопросы

Принятие мер по обеспечению физической защиты объекта КИИ


ПРЕЗЕНТАЦИЯ ОКОНЧЕНА.
СПАСИБО ЗА ВНИМАНИЕ!
risovach.ru