Что стоит учитывать при создании и сопровождении Процесса реагирования на инциденты ИБ

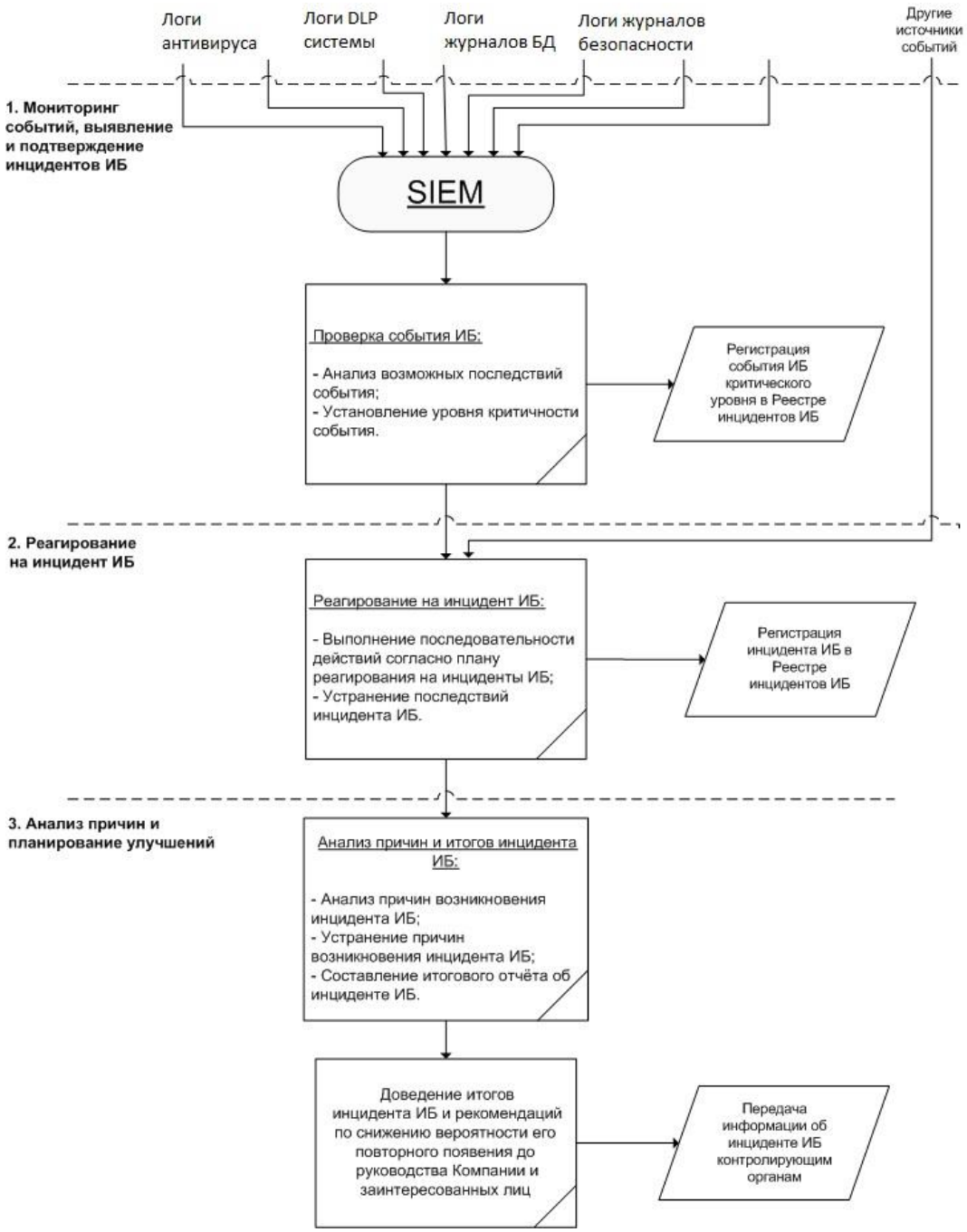
Руководитель направления реагирования на инциденты ИБ – Богданов Д.В.

Создание процесса

- - Регламент (источники событий, алгоритм)
- - Инструменты для реагирования (SIEM, DLP и др.)
- - Планы реагирования на инциденты

Сопровождение процесса

- - Тестирование реагирования на инциденты ИБ
- - Корректировка правил реагирования
- - Доработка и автоматизация существующих инструментов для реагирования


Логи антивируса
Логи DLP системы
Логи журналов БД
Логи журналов безопасности
Другие источники событий
1. Мониторинг событий, выявление и подтверждение инцидентов ИБ
SIEM
Проверка события ИБ:
- Анализ возможных последствий события;
- Установление уровня критичности события.
Регистрация события ИБ критического уровня в Реестре инцидентов ИБ
2. Реагирование на инцидент ИБ
Реагирование на инцидент ИБ:
- Выполнение последовательности действий согласно плану реагирования на инциденты ИБ;
- Устранение последствий инцидента ИБ.
Регистрация инцидента ИБ в Реестре инцидентов ИБ
3. Анализ причин и планирование улучшений
Анализ причин и итогов инцидента ИБ:
- Анализ причин возникновения инцидента ИБ;
- Устранение причин возникновения инцидента ИБ;
- Составление итогового отчёта об инциденте ИБ.
Доведение итогов инцидента ИБ и рекомендаций по снижению вероятности его повторного появления до руководства Компании и заинтересованных лиц
Передача информации об инциденте ИБ контролирующим органам

Пример плана реагирования: «Утечка ПДн»

1. Оповещение системных администраторов, ответственных за СЗИ, и руководства о возникновении потенциального инцидента ИБ.
2. Подтверждение факта передачи ПДн, либо факта блокировки передачи ПДн.
3. Если имеется факт передачи ПДн, производится определение критичности инцидента, исходя из количества переданной информации и её состава. Если факта передачи нет, производится сбор материалов, подтверждающий это и оповещение руководства.
4. Определение способа передачи ПДн за пределы контура и ответственных за это лиц.
5. Проведение расследования: фиксирование причин, способов и последствий инцидента.
6. Составление отчёта по результатам расследования.
7. Оповещение руководства об итогах расследования.
8. Описание выявленной уязвимости информационной безопасности, из-за которой произошёл инцидент, и постановка задач на её устранение/минимизации.
9. В случаях предусмотренных законом РФ: передача данных о инциденте с ПДн в Роскомнадзор, ФинЦерт.

Спасибо за внимание!