KPMG

Реагирование на инциденты. Передовые практики и методологии

Сентябрь, 2017

—

Кристина Боровикова, Старший консультант АО «КПМГ»

Реагирование на инциденты

Методологии и стандарты

ISO 27002:2013
А 16. Управление инцидентами ИБ: процедуры, ответственность, реагирование, отчетность, сбор свидетельств

ISO 27035-2:2016
Управление инцидентами ИБ. Руководящие принципы по планированию и реагированию на инциденты

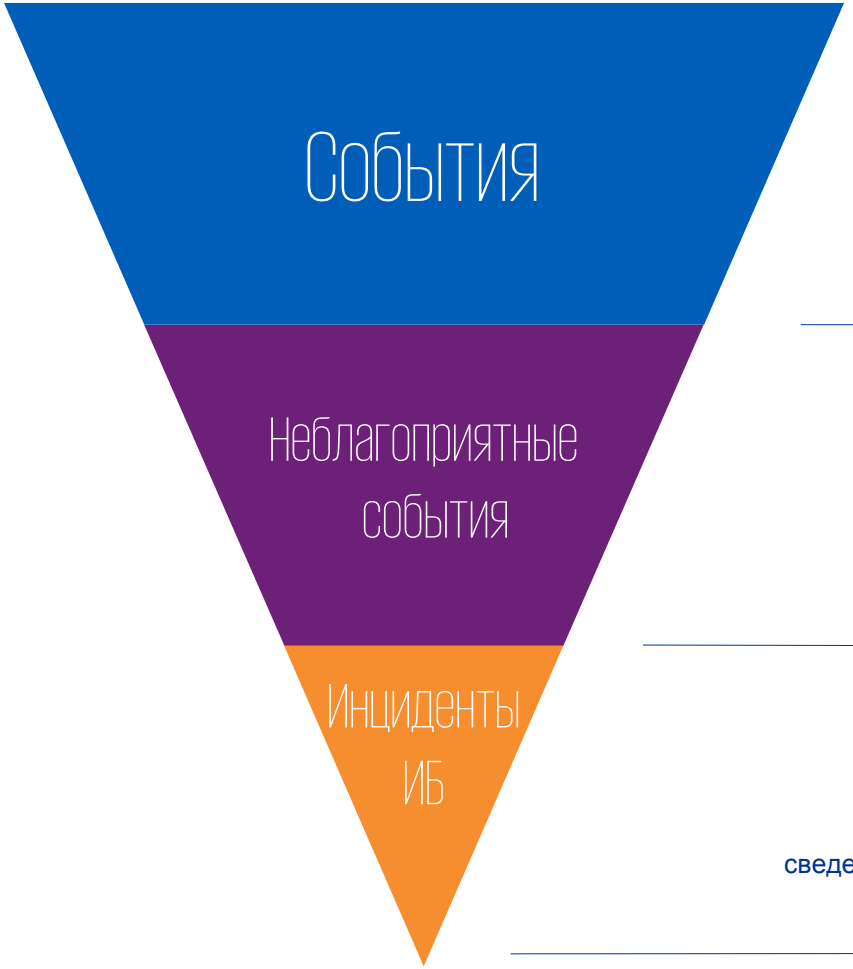
NIST 800-61
Руководство по обработке инцидентов ИБ

ITIL Service Operation
Раздел 4.2, управление инцидентами

Cobit 5 for Information Security
Реагирование на инциденты, сервисы

SWIFT Customer Security Framework
Раздел 7, реагирование на инциденты и обмен информацией

События и инциденты



Любое наблюдаемое событие в системе или сети.

К примеру, получение сервером запроса на доступ к веб-странице, заблокированная МЭ попытка соединения.

События с негативными последствиями.

К примеру, выход из строя оборудования, неавторизованное использование системных привилегий.

Нарушение или непосредственная угроза нарушения политик ИБ.

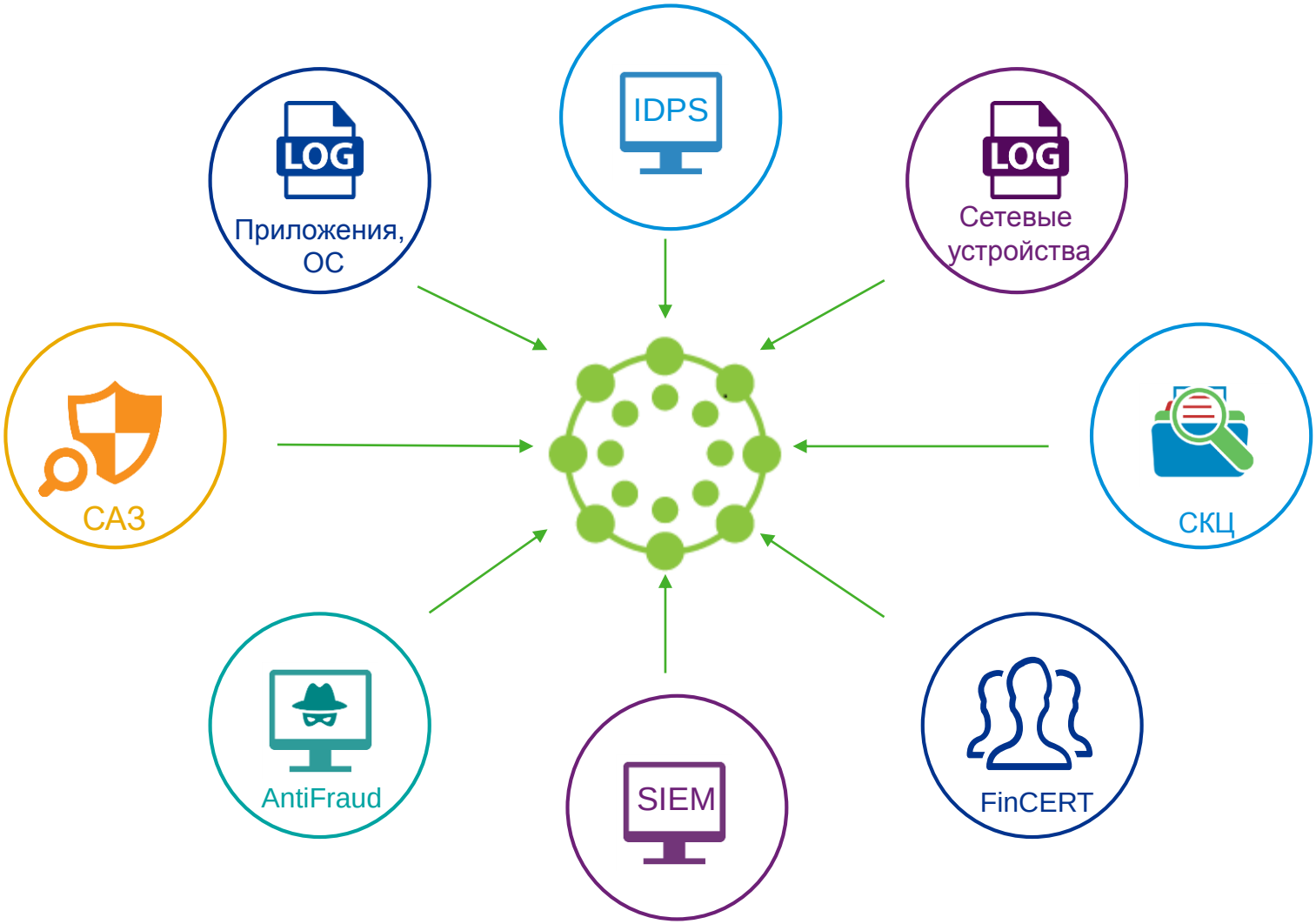
К примеру, злоумышленник получает конфиденциальные данные и угрожает, что сведения будут обнародованы публично, если организация не заплатит определенную сумму денег.

NIST 800-61

Последствия нереагирования на инциденты

1. Нарушение требований законодательства
2. Последующие атаки
3. Нарушение требований клиентов
4. Потеря клиентов
5. Увеличение расходов
6. Репутационные риски

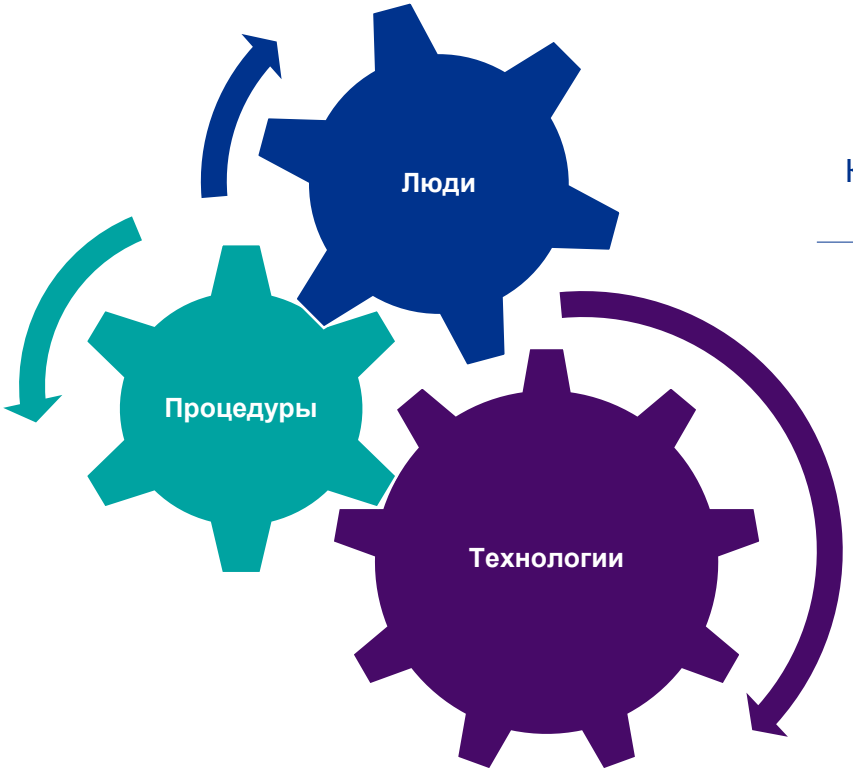
Источники информации о событиях



Процедура управления инцидентами

Источники информации о событиях	Получение данных о событиях из разнообразных источников
Идентификация инцидента	Выявление неблагоприятных событий, которые могут привести к инцидентам ИБ
Регистрация инцидента	Запись всей доступной информации об инциденте ИБ, к примеру, дата и время инцидента, симптомы, данные пользователя, статус инцидента, ответственные специалисты
Категорирование инцидента	Присвоение инциденту определенной ранее категории, к примеру, аппаратное обеспечение – сервер – карта памяти – отказ карты
Приоритизации инцидента	Определение уровня инцидента с учетом степени воздействия на бизнес и информацию, времени восстановления после инцидента
Эскалация, расследование и диагностика инцидента	Построение хронологической последовательности событий, подтверждение ущерба, выявление событий, которые могли бы вызвать инцидент, поиск информации
Решение инцидента и восстановление	Централизованное и локальное устранение последствий, координация пользователей, привлечение сторонних организаций, тестирование
Закрытие инцидента	Проведение опросов пользователей, указание причины закрытия инцидента, подготовка документации по инциденту, внесение необходимых изменений в процессы и процедуры

Составляющие процесса управления инцидентами



Квалифицированные специалисты по информационным технологиям и безопасности

Документированные, доступные и понятные процедуры идентификации, категорирования, приоритизации, реагирования на инциденты ИБ

Технологии, используемые для быстрого и эффективного реагирования на инциденты ИБ

Процедуры реагирования на инциденты

Ключевые моменты

1. Определить и задокументировать действия, которые необходимо выполнять на всех этапах жизненного цикла инцидентов ИБ
2. Определить и задокументировать роли и ответственность сторон, вовлеченных в процесс управления инцидентами ИБ
3. Определить руководителей, принимающих решения в отношении инцидентов ИБ

Опыт предыдущих инцидентов

Политика и **План** реагирования на инциденты

Процедуры по обработке инцидентов и подготовке отчетности

Руководства по взаимодействию с внешними организациями

Структура и **штатное расписание** группы реагирования на инциденты

Линии взаимодействия между группой реагирования на инциденты и другими группами

Перечень сервисов, предоставляемых группой реагирования на инциденты

Процедуры реагирования на инциденты

Приоритизации инцидентов

Категории функционального воздействия

Нет	Предоставление всех сервисов всем пользователям не нарушено
Низкое	Организация может предоставлять все критичные сервисы всем пользователям, но не с прежней эффективностью
Среднее	Организация не может предоставлять критичные сервисы некоторым пользователям
Высокое	Организация больше не может предоставлять некоторые критичные сервисы всем пользователям

Категории воздействия на информацию

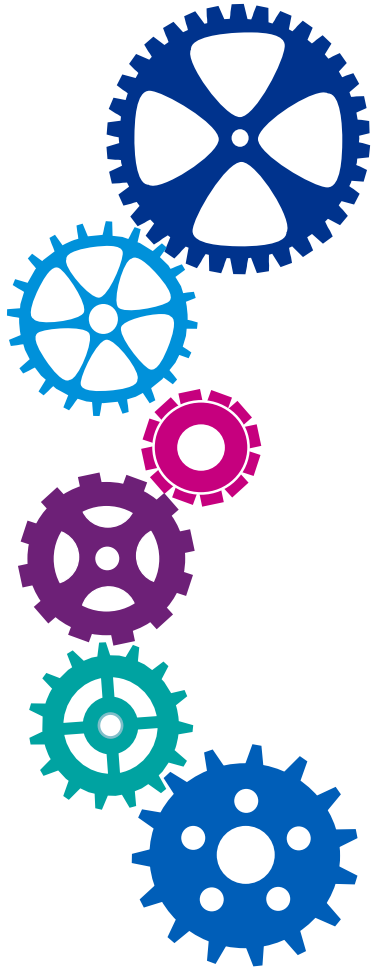
Нет	Информация не была экспортирована, изменена, удалена или иным образом скомпрометирована
Утечка персональных данных	Несанкционированный доступ и/или утечка персональных данных работников, клиентов, поставщиков и т.д.
Утечка коммерческой тайны	Несанкционированный доступ и/или утечка конфиденциальной информации организации
Нарушение целостности	Удаление или изменение конфиденциальной информации организации

Категории восстановления

Регулярное	Время восстановления предсказуемо при текущих ресурсах
Дополняемое	Время восстановления предсказуемо при дополнительных ресурсах
Расширяемое	Время восстановления непредсказуемо, необходимы дополнительные ресурсы и внешняя помощь
Не восстанавливаемое	Восстановление после инцидента невозможно

NIST 800-61

Основные рекомендации



- ☑ Обеспечьте возможность реагирования на инциденты. Организуйте SOC/CIRT.
- ☑ Задокументируйте политики и процедуры управления инцидентами.
- ☑ Своевременно предоставляйте информацию об инцидентах ИБ регулирующим органам и клиентам.
- ☑ Выберете модель группы реагирования на инциденты (штатные работники, аутсорсинг, время занятости).
- ☑ Привлекайте в группу реагирования на инциденты специалистов с соответствующей квалификацией.
- ☑ Проводите регулярные тренинги для работников, имитируя инциденты ИБ.
- ☑ Повышайте осведомленность работников в части реагирования и раскрытия информации об инцидентах ИБ.
- ☑ Используйте передовые практики, методологии, опыт коллег, клиентов по управлению инцидентами ИБ.

KPMG

cyber@kpmg.ru

KPMG

Спасибо!

Илья Шаленков
Старший менеджер,
Управление информационными рисками
КПМГ Россия, Москва

+7 (495) 937-44-77
asksecurity@kpmg.ru
www.kpmg.ru

Кристина Боровикова
Старший консультант,
Управление информационными рисками
КПМГ Россия, Москва

+7 (495) 937-44-77
asksecurity@kpmg.ru
www.kpmg.ru

kpmg.ru

kpmg.com/app