

# ОТ ПОДХОДОВ К СОЗДАНИЮ СИТУАЦИОННОГО ЦЕНТРА К ПОСТРОЕНИЮ ЭФФЕКТИВНЫХ МЕТОДОВ ВЫЯВЛЕНИЯ ИНЦИДЕНТОВ ИБ

Ксения Засецкая

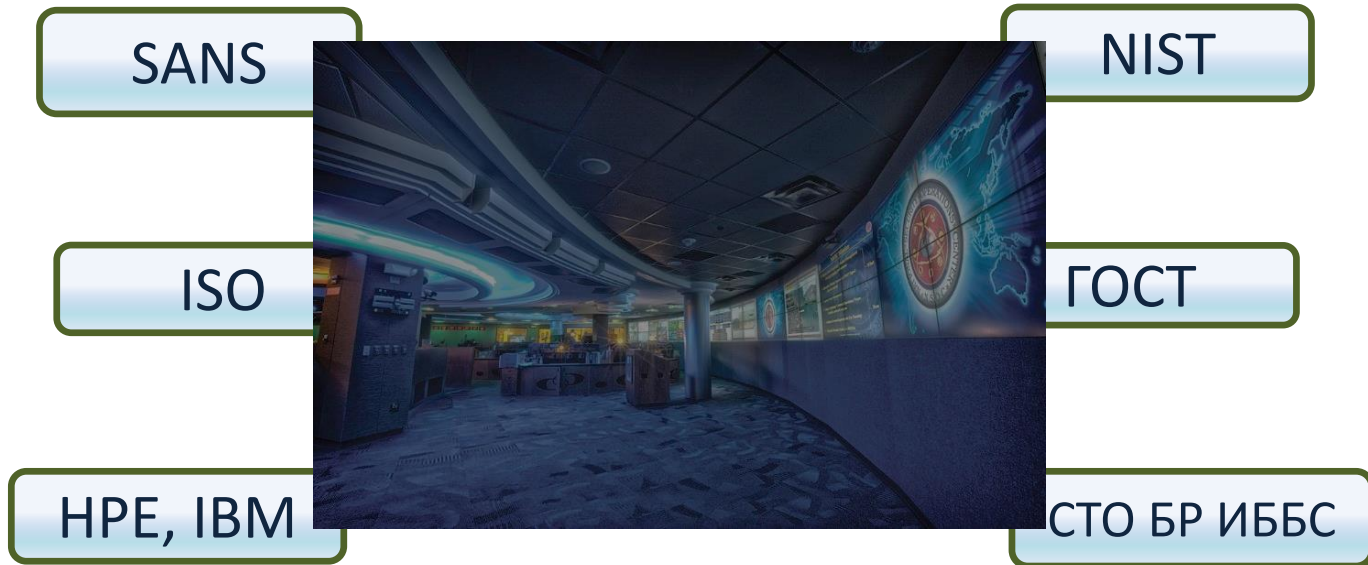
Старший консультант Отдела консалтинга  
АО «ДиалогНаука»

Роман Ванерке

Руководитель отдела технических решений  
АО «ДиалогНаука»

# Ситуационные центры ИБ (SOC)

- ✓ Уровень зрелости компании и готова ли компания к построению SOC?
- ✓ Какая форма организации SOC предпочтительнее?
- ✓ Какой целевой уровень зрелости SOC?



# Критичные параметры для SOC

---

- ✓ Управляемые процессы - в основе успеха!
  - ✓ Определенность в целях и режиме работы
  - ✓ Документированность
  - ✓ Взаимодействие участников
  - ✓ Оценка эффективности
  - ✓ Анализ и совершенствование

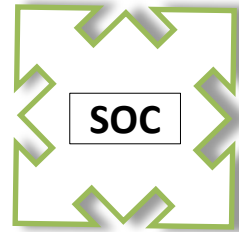
# Ключевые элементы SOC

## Рабочие процессы:

Определение ролей и обязанностей  
Управление событиями  
Планирование  
Управление инцидентами  
Кризисное реагирование  
Выявление проблем и изменения  
Адаптация сотрудников  
Обучение и оценка навыков

## Аналитические процессы:

Киберразведка  
Расследование  
Исследование данных  
Целенаправленный мониторинг  
Криминалистика  
Обобщенная информация



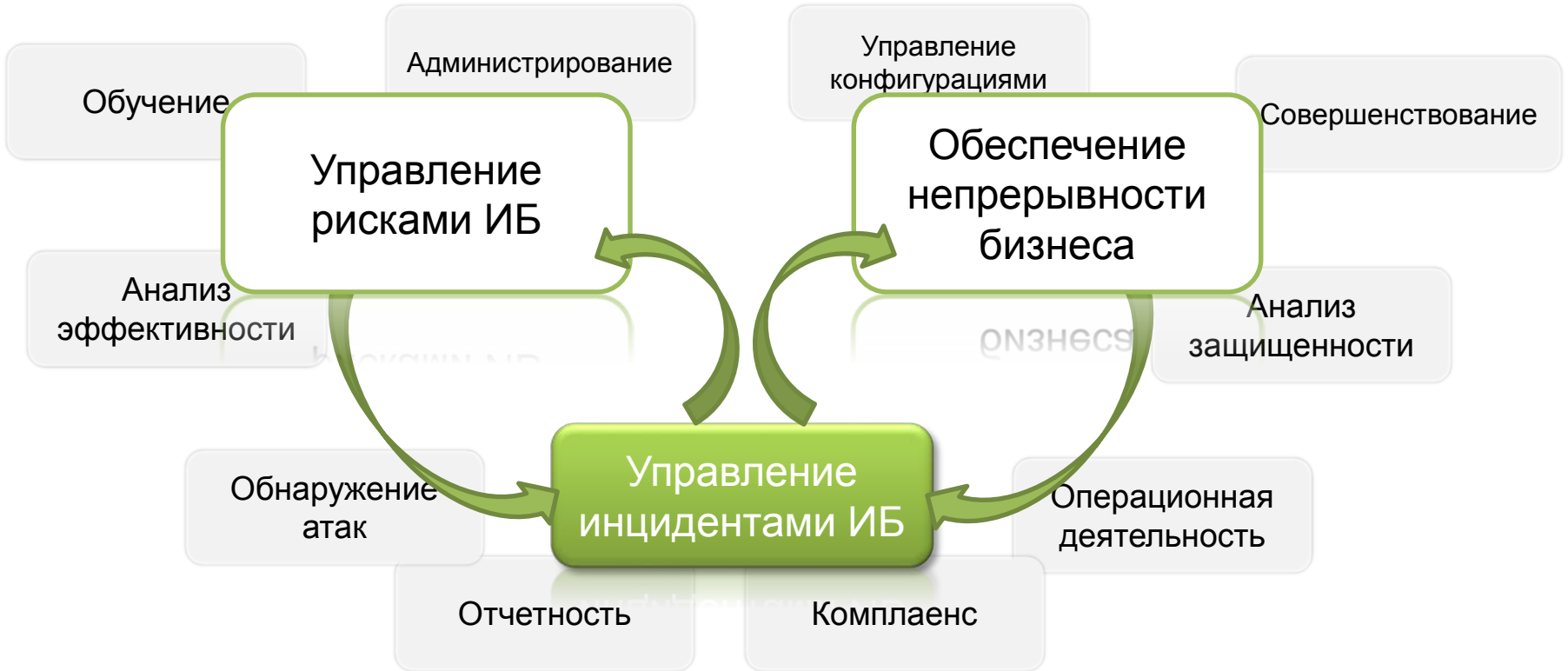
## Технологические процессы:

Архитектура систем и решений  
Поток данных и ценность данных  
Адаптация данных  
Выделение пользовательских ресурсов  
Управление конфигурациями  
Жизненный цикл инцидента  
Техподдержка  
Жизнеспособность и доступность  
Резервное копирование и восстановление  
Источники информации

## Бизнес-процессы:

Миссия  
Спонсорство  
Служебные обязательства  
Метрики и KPI  
Комплаенс  
Управление проектами  
Постоянное совершенствование  
Управление знаниями  
Обеспечение непрерывности бизнеса  
Управление

# Взаимосвязанные процессы



## Инцидент информационной безопасности

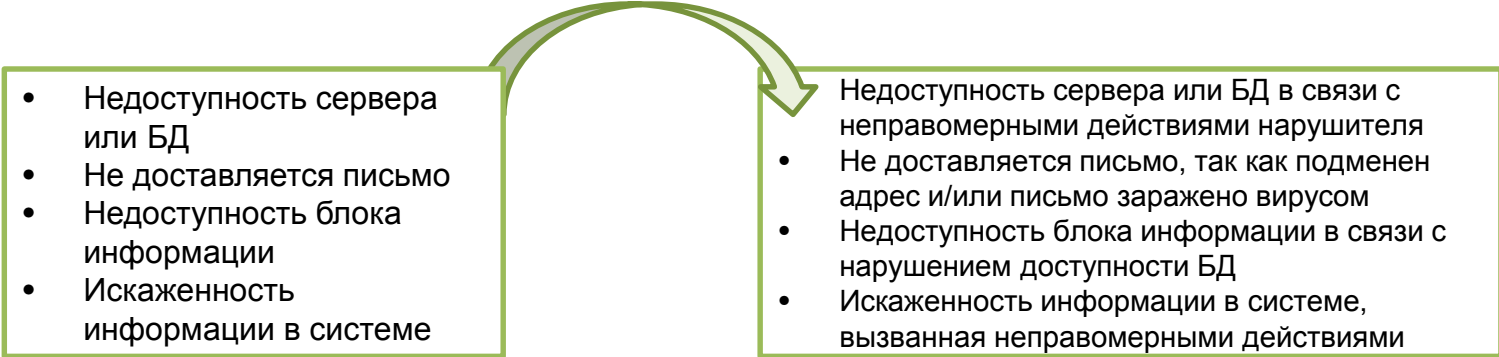
One or multiple related and identified information security events that can harm an organization's assets or compromise its operations  
(ISO/IEC 27035-1:2016)

Событие ИБ или их комбинация, указывающие на свершившуюся, предпринимаемую или вероятную реализацию угрозы ИБ, результатом которой является ряд негативных событий

- ✓ События ИБ – не всегда инциденты.
- ✓ Должны быть определены **критерии** отнесения событий информационной безопасности к инцидентам

# Инциденты ИТ и инциденты ИБ

- ✓ Инциденты ИТ – не всегда инциденты ИБ, но могут ими быть

- 
- Недоступность сервера или БД
  - Не доставляется письмо
  - Недоступность блока информации
  - Искаженность информации в системе

- Недоступность сервера или БД в связи с неправомерными действиями нарушителя
- Не доставляется письмо, так как подменен адрес и/или письмо заражено вирусом
- Недоступность блока информации в связи с нарушением доступности БД
- Искаженность информации в системе, вызванная неправомерными действиями

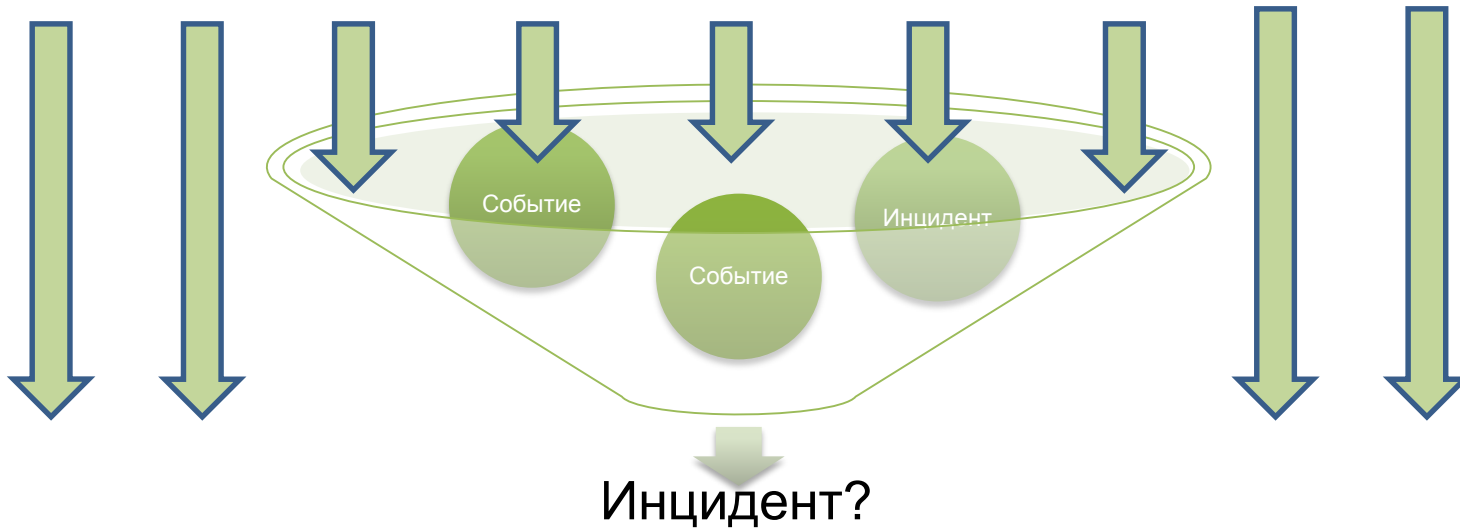
- ✓ Критерии перехода инцидентов ИТ в инциденты ИБ!
- ✓ Специалисты ИТ - активные участники жизненного цикла инцидента
- ✓ Не все инциденты ИТ нужны подразделениям ИБ
- ✓ Определение и формализация зон ответственности подразделений ИТ и ИБ
- ✓ Информированность об инцидентах ИТ и ИБ

# Выявление инцидентов

Основные источники информации о потенциальных инцидентах:

- ✓ пользователи
- ✓ информационные системы
- ✓ компоненты ИТ-инфраструктуры

- ✓ средства защиты информации
- ✓ клиенты
- ✓ контрагенты
- ✓ внешние сервисы

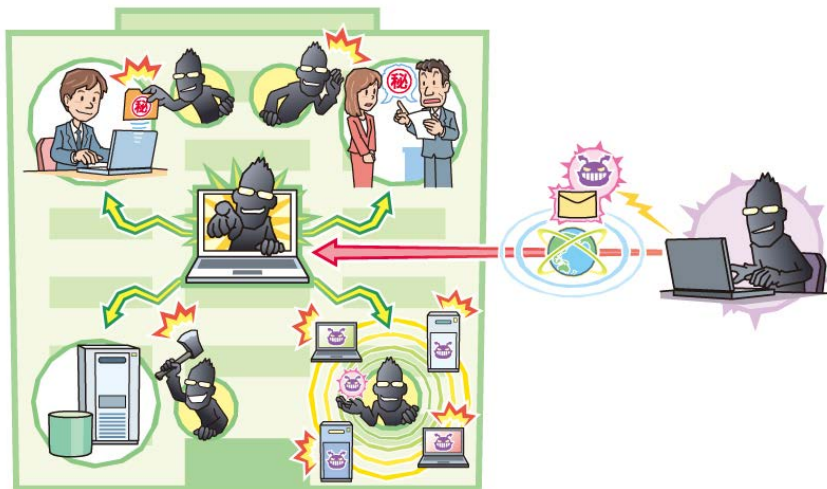




# Оценка угроз в основе управления

Для организации успешного процесса управления инцидентами:

- ✓ выделить критичные информационные ресурсы
- ✓ провести оценку угроз информационной безопасности, актуальных для критичных ресурсов
- ✓ использовать полученные результаты при реализации механизмов выявления инцидентов



# Информированность

Отлаженные и известные способы взаимодействия с внутренними и внешними источниками информации



# Угрозы ИБ и методы реализации угроз

---

- ✓ Три основных параметра, на которые направлены угрозы:

Конфиденциальность

Целостность

Доступность

- ✓ 8 типов угроз информационной безопасности, охватывающих все варианты
- ✓ 14 комплексных методов реализации угроз безопасности

# Методы и сценарии

Описание угрозы	Описание метода	Связанные сценарии	Описание уровня среды обработки	Код сценария выявления	Сценарий выявления
хищение информации (получение доступа к информации)	Несанкционированный доступ	Доступ к информационным ресурсам с использованием скомпрометированных аутентификационных данных	прикладной уровень	1.04.26.05.00001	«Спящие» учетные записи сотрудников и хостов - по которым не было активности в заданный период (30 дней)
хищение информации (получение доступа к информации)	Несанкционированный доступ	Доступ к информационным ресурсам с использованием скомпрометированных аутентификационных данных	Общесистемный уровень (ОС)	1.04.26.03.00001	«Спящие» учетные записи сотрудников и хостов - по которым не было активности в заданный период (30 дней)
блокирование информации	Несанкционированный доступ	Подбор аутентификационной информации	Общесистемный уровень (ОС)	7.04.27.03.00012	Блокировка X учетных записей за Y минут
утрата (неумышленная потеря) информации и/или средств ее обработки	Ошибки персонала	Нарушение процесса путем удаления критичных объектов	Уровень баз данных	3.14.17.04.00015	Удаление критичных объектов (таблиц, файлов)
модификация (искажение) информации	Ошибки персонала	Нарушение процесса путем внесения изменений в критичные объекты	Уровень баз данных	4.14.18.04.00016	Изменение критичных объектов (таблиц, файлов)

Тип нарушителя может быть классифицирован только в ходе расследования и аналитики

# От сценариев выявления к сценариям реализации



## L2 - инцидент

- Срабатывание на L0 или L1, использование списков
- Унификация подхода к созданию сценариев



## L1 - обогащение

- Дополнительная обработка и обогащение
- Использование Active List\Session List



## L0 – нормализация

- Приведение к единой таксономии одностипных событий
- Упрощение условий
- Возможность использования в разных сценариях

- ✓ Сложные покинет к
- ✓ Необщ данные
- ✓ Отсутс
- ✓ Сложн
- ✓ Отсутс

black\_ip  
& AND  
InActiveList("/All Active Lists/ /Network/BLACK IP")

11/20/17 11:08:00 AM to 11/21/17 11:08:00 AM



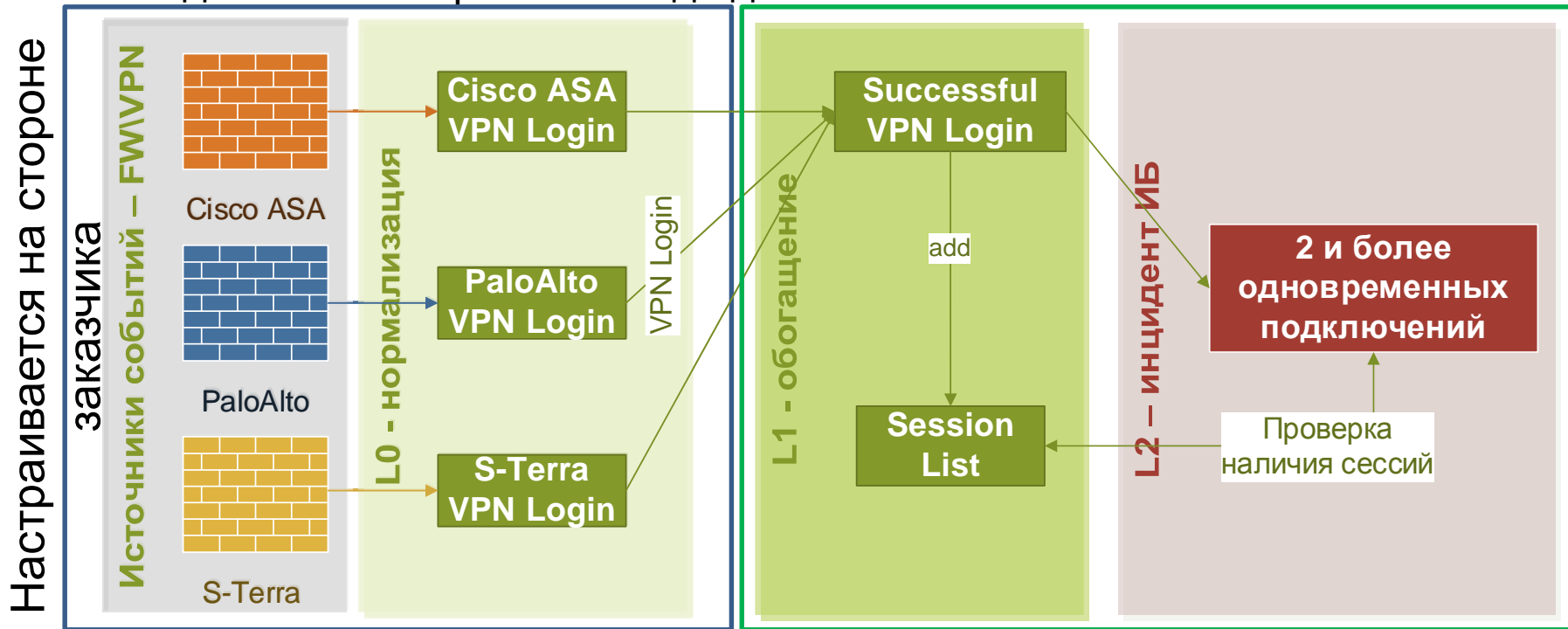
Success authentication[Preview]

Category Behavior	Category Outcome	Device Vendor	Count(Category Behavior)
/Authentication/Verify	/Success	Microsoft	56472268
/Authentication	/Success	Microsoft	24390
/Authentication/Modify	/Success	Microsoft	942
/Authentication/Verify	/Success	ArcSight	148
/Authentication/Verify	/Success	CISCO	102
/Authentication/Add	/Success	Microsoft	22
/Authentication/Modify	/Success	ArcSight	12

OR  
Name Contains establish [ignore case]  
Name Contains allow [ignore case]  
Name Contains success [ignore case]  
Device Vendor = Symantec  
Target Address = 192.168.1.8  
ifTargetA  
& AND  
Name StartsWith Intrusion Detected [ignore case]

# Как это работает в ArcSight

- Рассмотрим настройку следующего сценария выявления «2 и более подключений через VPN под одним пользователем»



**Спасибо за внимание!**

**АО «ДиалогНаука»**

Телефон: +7 (495) 980-67-76

Факс: +7 (495) 980-67-75

<http://www.DialogNauka.ru>

e-mail: [k.zasetskaya@DialogNauka.ru](mailto:k.zasetskaya@DialogNauka.ru)

[rv@DialogNauka.ru](mailto:rv@DialogNauka.ru)