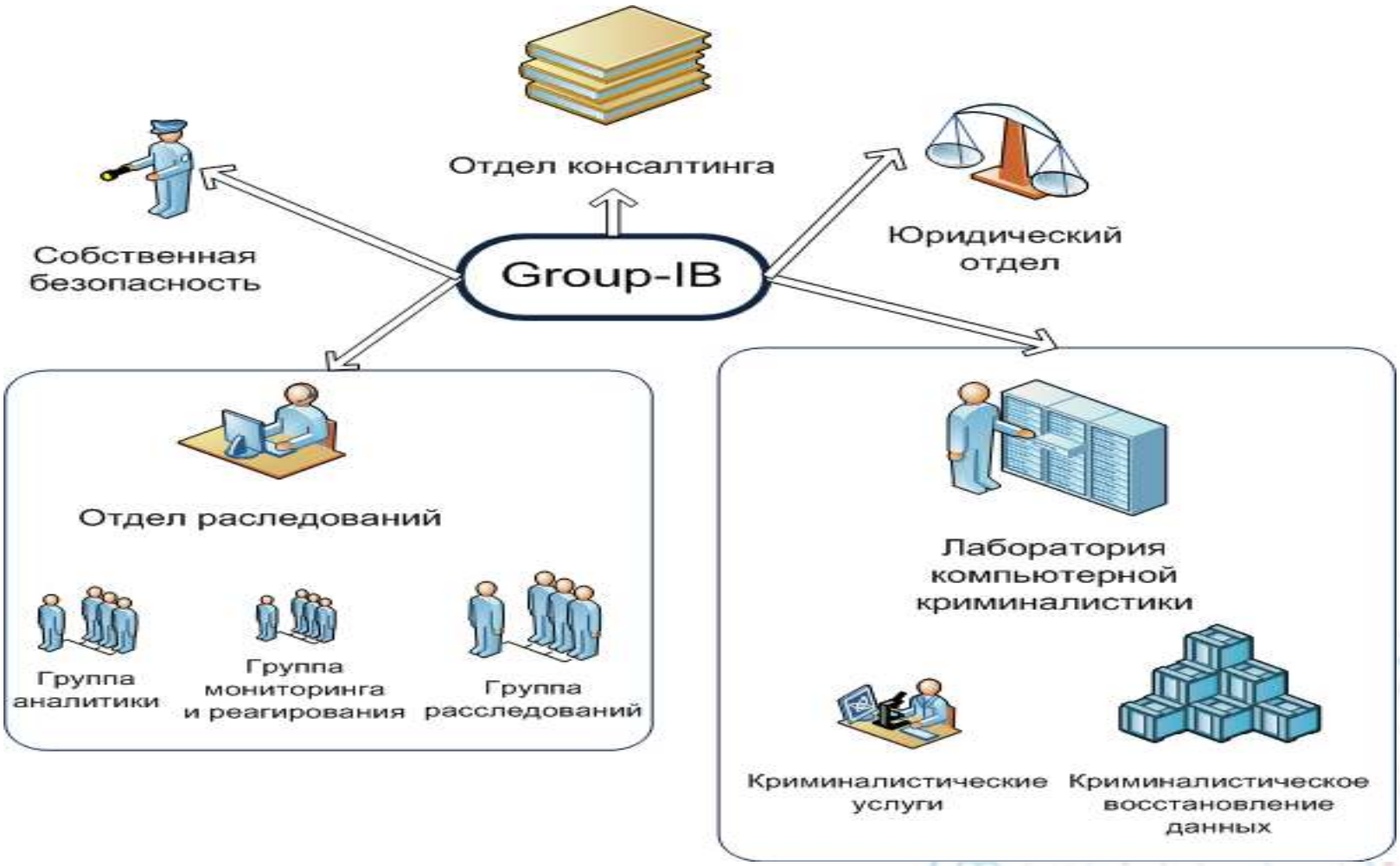
Построение системы управления инцидентами в онлайн-банкинге

Group-IB

- ✓ Первая и единственная негосударственная компания в РФ, оказывающая комплексные услуги консалтинга в области расследования инцидентов информационной безопасности
- ✓Основана в 2003
- ✓Сотрудничество с экспертными организациями в 52 странах
- ✓24/7мониторинг и поддержка


Отдел консалтинга
Собственная безопасность
Group-IB
Юридический отдел
Отдел расследований
Группа аналитики
Группа мониторинга и реагирования
Группа расследований
Лаборатория компьютерной криминалистики
Криминалистические услуги
Криминалистическое восстановление данных

- ✓ Группы по реагированию на инциденты (CERT) в 52 странах мира
- ✓ Антивирусные компании
- ✓ Производители решений по компьютерной криминалистике и информационной безопасности
- ✓ Университеты США и Европы
- ✓ Международные организации по компьютерной криминалистике
- ✓ Ассоциация сертифицированных специалистов по борьбе с мошенничествами (ACFE)
- ✓ Центры изучения угроз информационной безопасности

Инциденты информационной безопасности

Инцидент

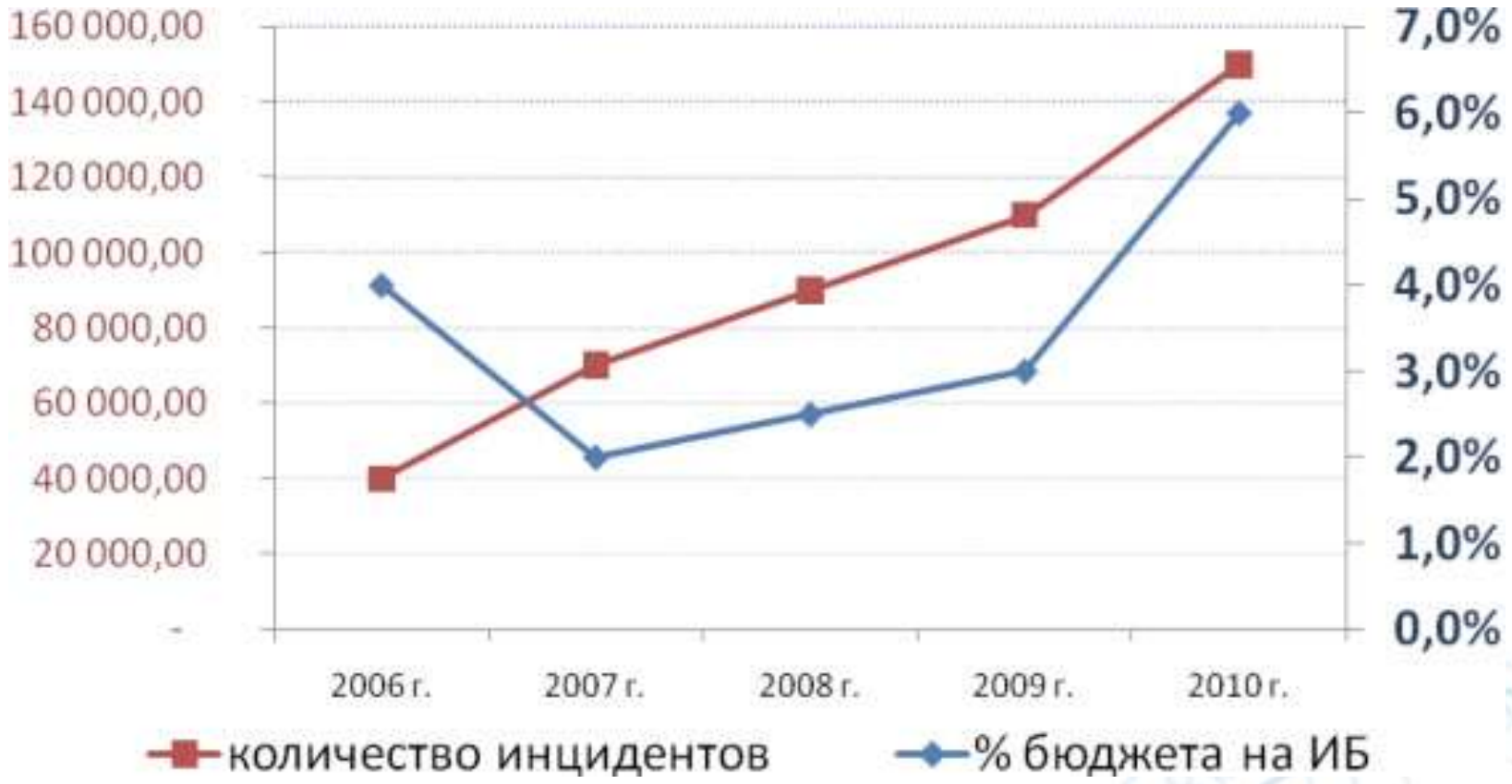
Инцидент информационной безопасности (Инцидент ИБ) – Одно или серия нежелательных или неожиданных событий в системе информационной безопасности, которые имеют большой шанс скомпрометировать деловые операции и поставить под угрозу защиту информации.

Источник: ГОСТ Р ИСО/МЭК 27001–2006

Типы инцидентов в системе ДБО:

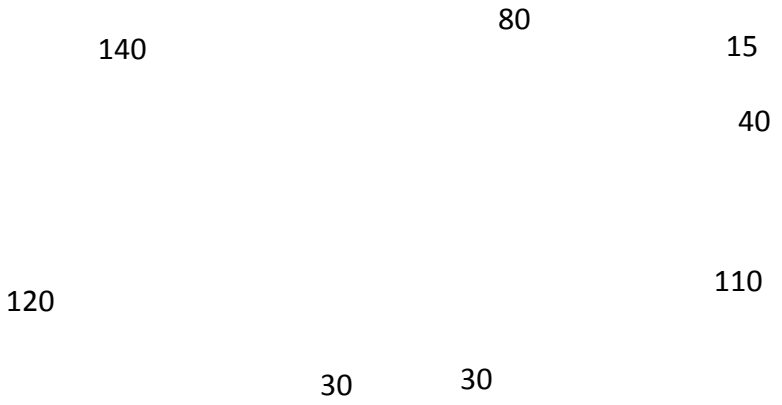
- ✓ Удаленное управление
- ✓ Подмена реквизитов
- ✓ Перехват сессии
- ✓ Несанкционированный доступ к логинам/паролям и ключевой информации
- ✓ …

Гонка бюджетов



Статистика

- ✓ Проведены работы и собрана база знаний по более чем 560 инцидентам



Мошенничества в ДБО

DDoS-атаки

Компрометации серверов и АРМ

Атака на Бренд в сети Интернет

Утечка информации

Фишинг и незаконное использование бренда

Криминалистические исследования

Восстановление данных

Признаки инцидента в ДБО

- ✓ Обнаружение платежных поручений, которые не передавались уполномоченными сотрудниками организации
- ✓ Сообщение из банка, содержащее требование подтвердить исполнение платежных поручений, которые не передавались уполномоченными сотрудниками организации
- ✓ Уменьшение или отсутствие денежных средств на счете при условии, что передача денежных средств не проводилась
- ✓ Невозможность входа в систему ДБО из-за ошибок различного характера, достоверно не связанных с техническими проблемами на стороне банка
- ✓ Невозможность загрузки операционной системы ЭВМ, на которой работали с системой ДБО

Система управления инцидентами

Решаемые задачи

- ✓ Обеспечение своевременной реакции на инцидент
- ✓ Минимизация ущерба от инцидента
- ✓ Корректный сбор доказательной информации
- ✓ Закрытие уязвимостей
- ✓ Обеспечение возможности юридического преследования злоумышленников
- ✓ Обеспечение возможности возмещения ущерба от инцидента ИБ

Структура системы

Структура системы управления инцидентами

Реагирование

- ✓ Принятие мер по остановке инцидента и сохранению доказательной информации
- ✓ Сбор доказательной информации
- ✓ Привлечение внешних экспертных организаций
- ✓ Проведение криминалистических исследований
- ✓ Взаимодействие с внутренними подразделениями, партнерами, пострадавшими сторонами

Расследование

- ✓ Установление обстоятельств инцидентов ИБ
- ✓ Привлечение внешних экспертных организаций
- ✓ Взаимодействие с правоохранительными органами и судебными инстанциями
- ✓ Взаимодействие с внутренними подразделениями, партнерами и пострадавшими сторонами

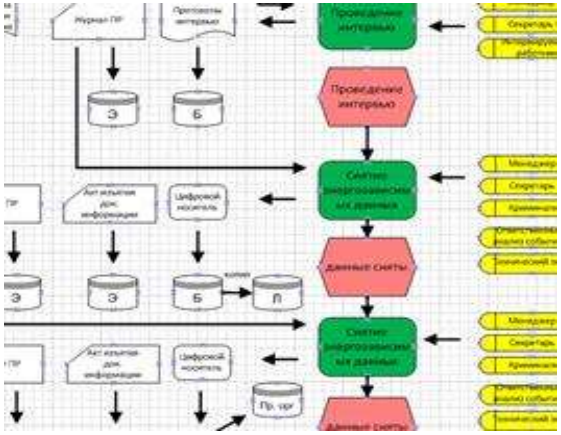
Этапы построения

- ✓ Анализ общего состояния ИБ, а так же перечня и типов инцидентов, относящихся к инцидентам ИБ
- ✓ Определение первичного порядка управления инцидентами
- ✓ Организационное закрепление классификации инцидентов, порядка мониторинга инцидентов
- ✓ Формирование группы расследования
- ✓ Определение жизненного цикла инцидента ИБ
- ✓ Описание этапов жизненного цикла процесса расследования
- ✓ Разработка полной карты процесса
- ✓ Приведение действующих документов в соответствие с процессом расследования

Эффективность

Подготовленная команда по реагированию

Диаграмма процесса управления инцидентами



Организационно-распорядительная документация

Группа расследования

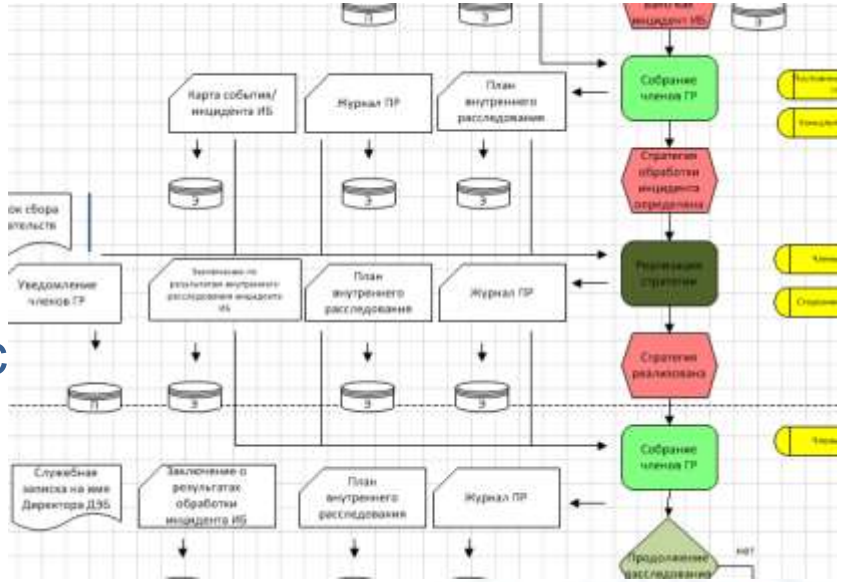
Роли в рамках группы по расследованию инцидентов ИБ

- ✓ Руководитель группы
- ✓ Менеджер группы
- ✓ Технический эксперт
- ✓ Секретарь
- ✓ Владельцы ресурсов, попадающих в рамки инцидента (на непостоянной основе)

Процесс управления

Диаграмма процесса управления инцидентами

- ✓ Рассмотрение и классификация инцидентов ИБ
- ✓ Реагирование и сбор доказательс
- ✓ Расследование инцидента ИБ



Цель – отражение целостной картины процесса расследования инцидентов

Документация

Описание процесса управления инцидентами

- ✓ Политика управления инцидентами ИБ
- ✓ Регламент и процедура мониторинга и регистрации событий ИБ
- ✓ Процедура анализа и классификации инцидента ИБ
- ✓ Процедура реагирования и проведения внутреннего расследования обстоятельств инцидента ИБ
- ✓ Процедура сбора доказательной информации

Документация

Описание процесса управления инцидентами

- ✓ Процедура проведения внешнего расследования инцидента ИБ
- ✓ Процедура взаимодействия с внешними организациями по инцидентам ИБ
- ✓ Процедура анализа эффективности и модернизация процесса расследования инцидентов ИБ и улучшения системы защиты
- ✓ Рекомендации по внесению изменений в действующую ОРД

Вопросы?

Татьяна Скрипкарь

skripkar@group-ib.ru

+7 495 66I 55 38 www.group-ib.ru www.letagroup.ru