# Управление инцидентами информационной безопасности с помощью DLP Solar Dozor

v.1.3 2015-08

# Термины по ГОСТ 27000-2012

- **Событие ИБ** – выявленное состояние системы, услуги или состояние сети, указывающее на возможное нарушение политики обеспечения ИБ, нарушение или отказ мер и средств контроля и управления или прежде неизвестная ситуации, которая может иметь значение для безопасности.

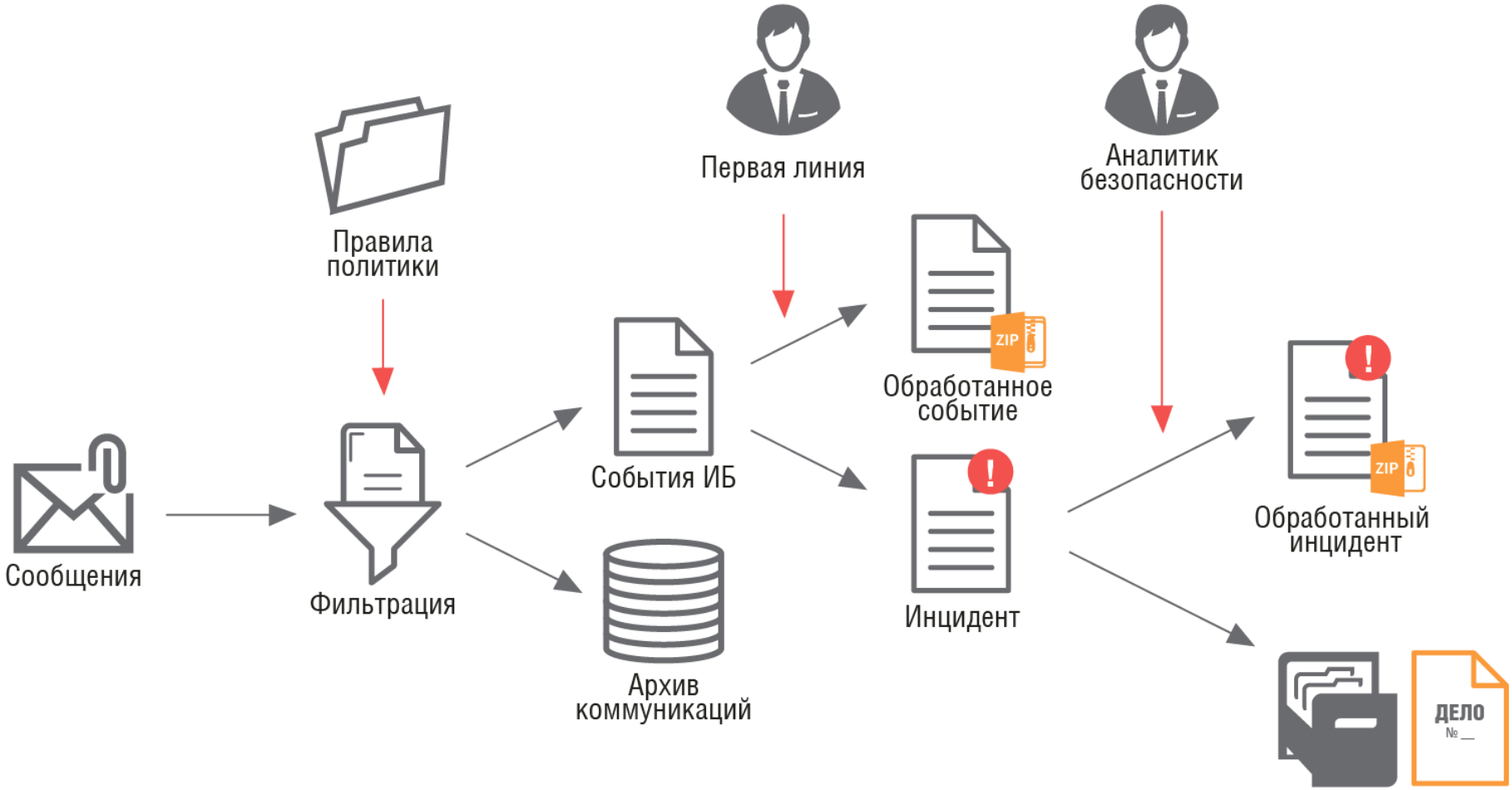
- **Инцидент ИБ** – одно или несколько нежелательных или неожиданных событий ИБ, которые со значительной степенью вероятности приводят к компрометации бизнеса и создают угрозы для ИБ.

# Типовые инциденты, выявляемые DLP

(утечки информации и внутрикорпоративное мошенничество)

- Увольняющийся сотрудник скопировал на флешку все, что с мог достать (наработки, методологии, базу клиентов, проектную документацию, стратегии и планы)
- Сотрудник отдела закупок договорился с поставщиком о завышении закупочных цен при условии личной мотивации (откат)
- Операционист в банке пересылает заявления на кредиты своему коллеге в конкурирующем банке, который переманивает этих клиентов, делая целевые контрпредложения
- Сотрудник одела продаж некоторые заказы проводит через свою фирму
- Секретарь регулярно пересылает протоколы совещаний руководства на незнакомый внешний ящик электронной почты
- …

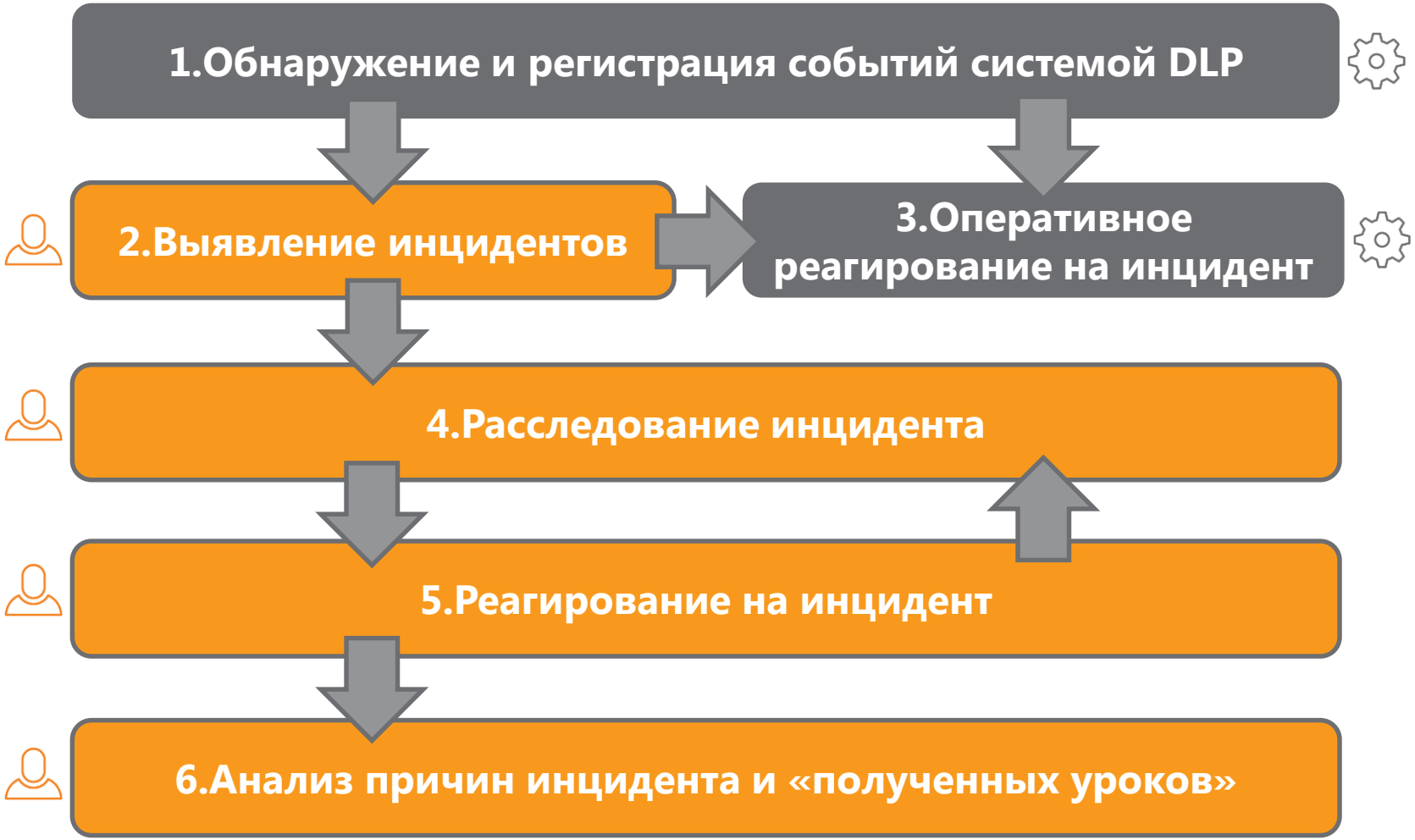
# Управление событиями и инцидентами DLP



# Процедура управления инцидентами (DLP)

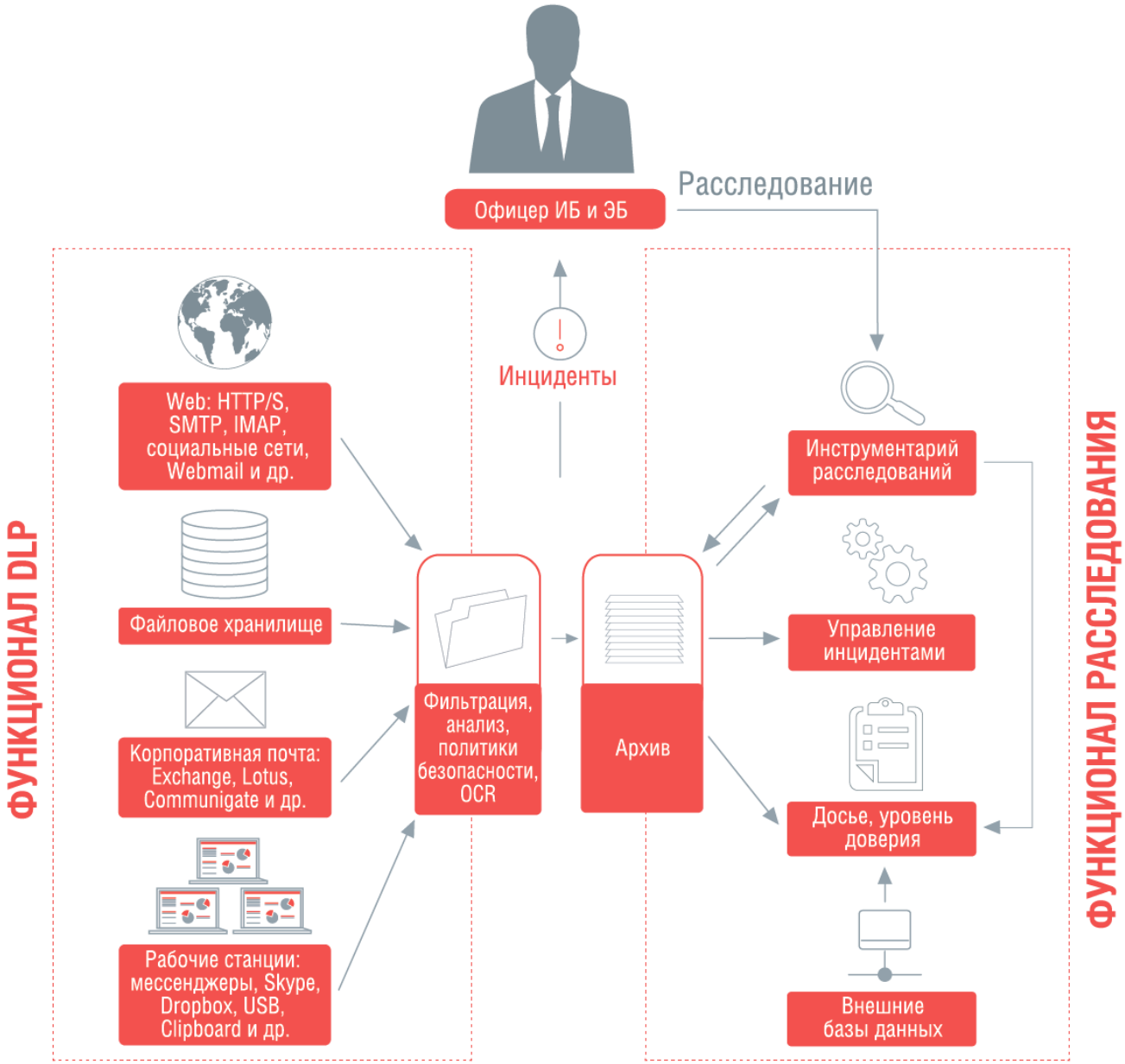
1. Обнаружение и регистрация событий ИБ
2. Категорирование событий, сбор дополнительной информации и выявление инцидентов ИБ
3. Оперативное реагирование на инцидент
4. Разбор (расследование) инцидента
5. Реагирование на инцидент
6. Анализ причин инцидента и «полученных уроков», подготовка рекомендаций по повышению общего уровня ИБ (при необходимости)

# Процедура управления инцидентами (DLP)



# Ограничение по времени реагирования по ТК РФ


1. Обнаружение и регистрация событий




Концептуальная архитектура решения

# Контролируемые каналы

## Корпоративная почта

Exchange

Lotus

CommuniGate SYSTEMS

## Файловое хранилище

Файлы на ПК и общедоступных ресурсах, FTP


## Web

Web-почта

@mail.ru

Yandex Mail

Резюме

hh.ru HeadHunter

JOB.RU

Соцсети

IM ICQ
MRA MSN
IRC XMPP

## Рабочие станции

Буфер обмена

USB

Принтеры

iTunes

Lync

Yandex.Disk

Google Drive

Dropbox

# Рекомендации ФСТЭК России по функционалу DLP

**ОЦЛ.5** КОНТРОЛЬ СОДЕРЖАНИЯ ИНФОРМАЦИИ, ПЕРЕДАВАЕМОЙ ИЗ ИНФОРМАЦИОННОЙ СИСТЕМЫ (КОНТЕЙНЕРНЫЙ, ОСНОВАННЫЙ НА СВОЙСТВАХ ОБЪЕКТА ДОСТУПА, И КОНТЕНТНЫЙ, ОСНОВАННЫЙ НА ПОИСКЕ ЗАПРЕЩЕННОЙ К ПЕРЕДАЧЕ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ СИГНАТУР, МАСОК И ИНЫХ МЕТОДОВ), И ИСКЛЮЧЕНИЕ НЕПРАВОМЕРНОЙ ПЕРЕДАЧИ ИНФОРМАЦИИ ИЗ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Контроль содержания информации, передаваемой из информационной системы, должен предусматривать:

- выявление фактов неправомерной передачи защищаемой информации из информационной системы через различные типы **сетевых соединений**, включая сети связи общего пользования, и реагирование на них;
- выявление фактов неправомерной записи защищаемой информации на неучтенные **съемные машинные носители** информации и реагирование на них;
- выявление фактов неправомерного вывода на **печать документов**, содержащих защищаемую информацию, и реагирование на них;
- выявление фактов неправомерного копирования защищаемой информации в прикладное программное обеспечение **из буфера обмена** и реагирование на них;
- **контроль хранения** защищаемой информации **на серверах и автоматизированных рабочих местах**;
- **выявление фактов хранения** информации **на общих сетевых ресурсах** (общие папки, системы документооборота, базы данных, почтовые архивы и иные ресурсы).

Требования к усилению

- в информационной системе должно осуществляться **хранение всей** передаваемой из информационной системы **информации** и (или) информации с недопустимым к передаче из информационной системы содержанием, в течение времени, определяемого оператором;
- в информационной системе должна осуществляться **блокировка** передачи из информационной системы информации с недопустимым содержанием

**Методический документ. Меры защиты информации в государственных ИС**

# Как DLP понимает события?

# Контекстный анализ

- Дата/Время
- Отправитель (права пользователя, группы (втч под особым контролем, например, «На увольнении») и роли)
- Получатель (внутренний/внешний, знакомый/неизвестный, «из перечня» и пр.)
- Канал передачи
- Местоположение (географическое и аппаратное)

# Контентный анализ

| Технологии анализа | Комментарии |
|---|---|
| Шаблоны документов | Поиск документов определенной структуры и содержания<br>+ поиск подобных |
| Цифровые отпечатки | • Текст<br>• Бинарные файлы |
| Идентификаторы | Например, номера паспорта, телефона, кредитной карты, ИНН и пр. (~50 категорий) |
| Дополнительные проверки | Тип вложения (формат), наименование файла, объем, регулярные выражения<br>+ внешние скрипты для специальных проверок (например, выявление наложенных слоев на геокартах) |

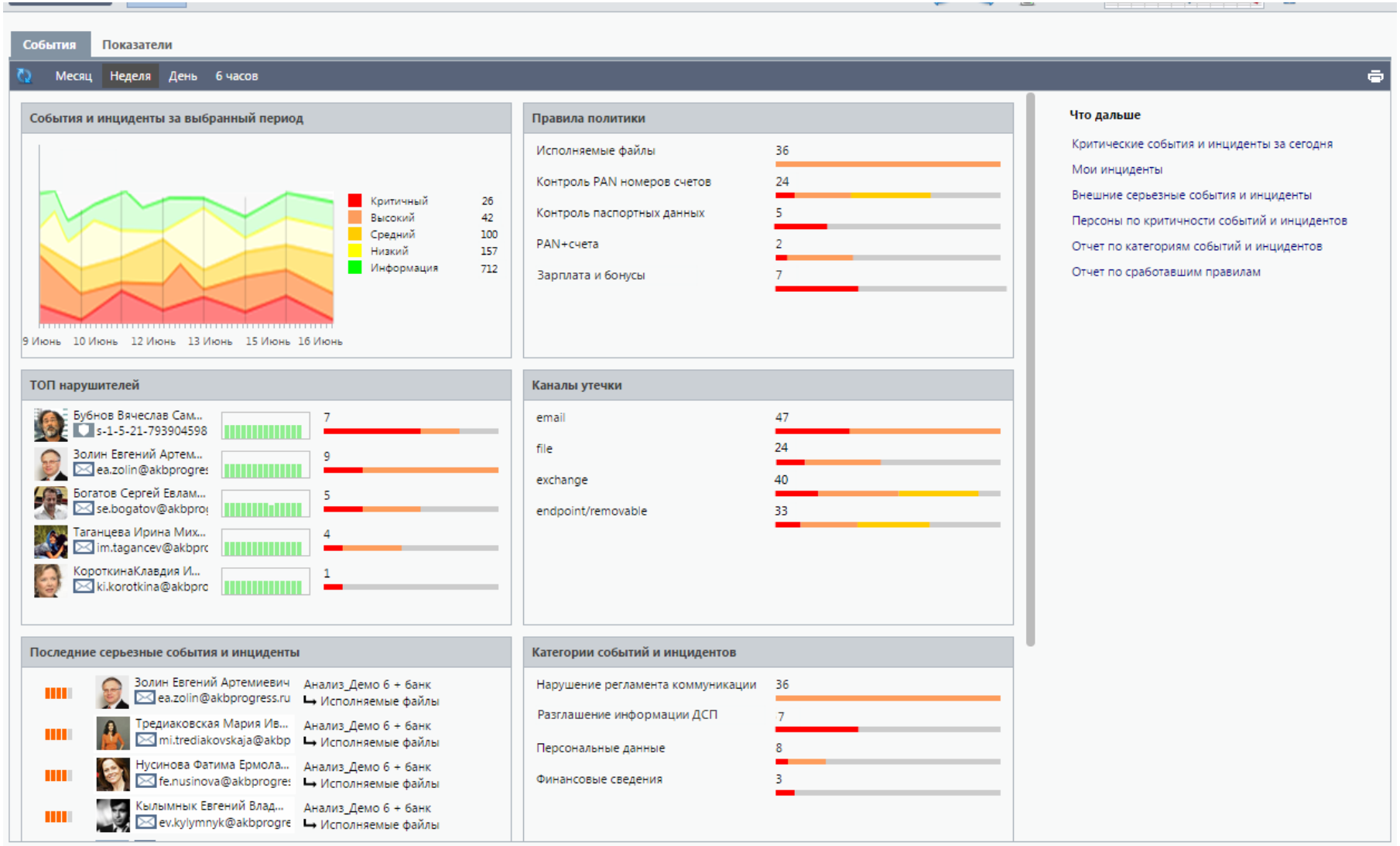
Фотографии и картинки проверяются с использованием технологии OCR (позволяет выявлять и понимать текст)


# 2. Выявление инцидентов

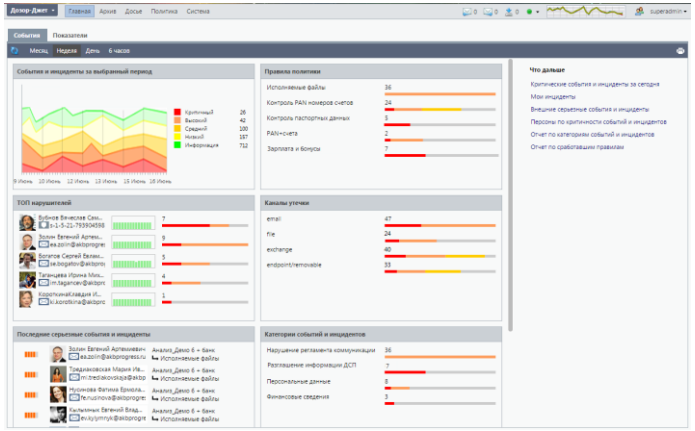
# Что запускает работу специалиста ИБ?

| Источник | Оперативность |
|---|---|
| 1. Оповещение по email | Высокая |
| 2. Оповещение в системе DLP | Высокая |
| 3. Оповещение по SMS | Высокая |
| 4. Информация на рабочем столе (Dashboard) | Средняя |
| 5. Информация из автоматического регулярного отчета | Средняя |
| 6. Информация из отчетов по запросу | Низкая |
| 7. Регулярный мониторинг и анализ | Низкая |
| 8. Внешняя информация об инциденте | Низкая |
| 9. Запрос со стороны руководства / заинтересованных лиц | Низкая |
| 10. «Чутье» (Подозрение на инцидент) | Низкая |
| 11. Скука / Интерес | Низкая |

# Рабочий стол офицера ИБ (v.5.0.4)

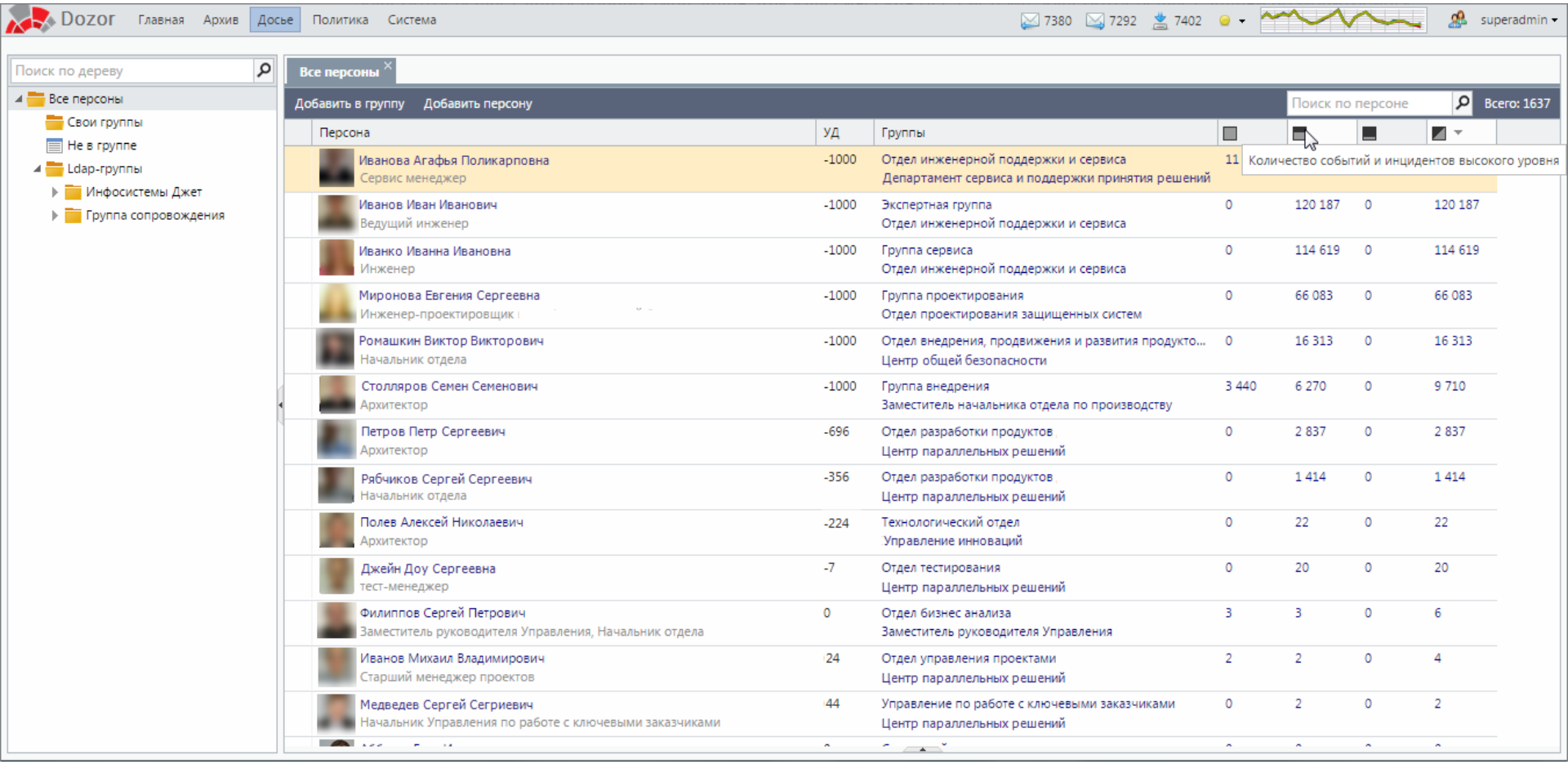


# Основные элементы консоли (v.5.0.4)



- Распределение событий по критичности и по времени
- Перечень ТОП нарушителей
- Лента последних событий
- Статистика нарушений:
  - правила политики
  - каналы утечки
  - тип угроз

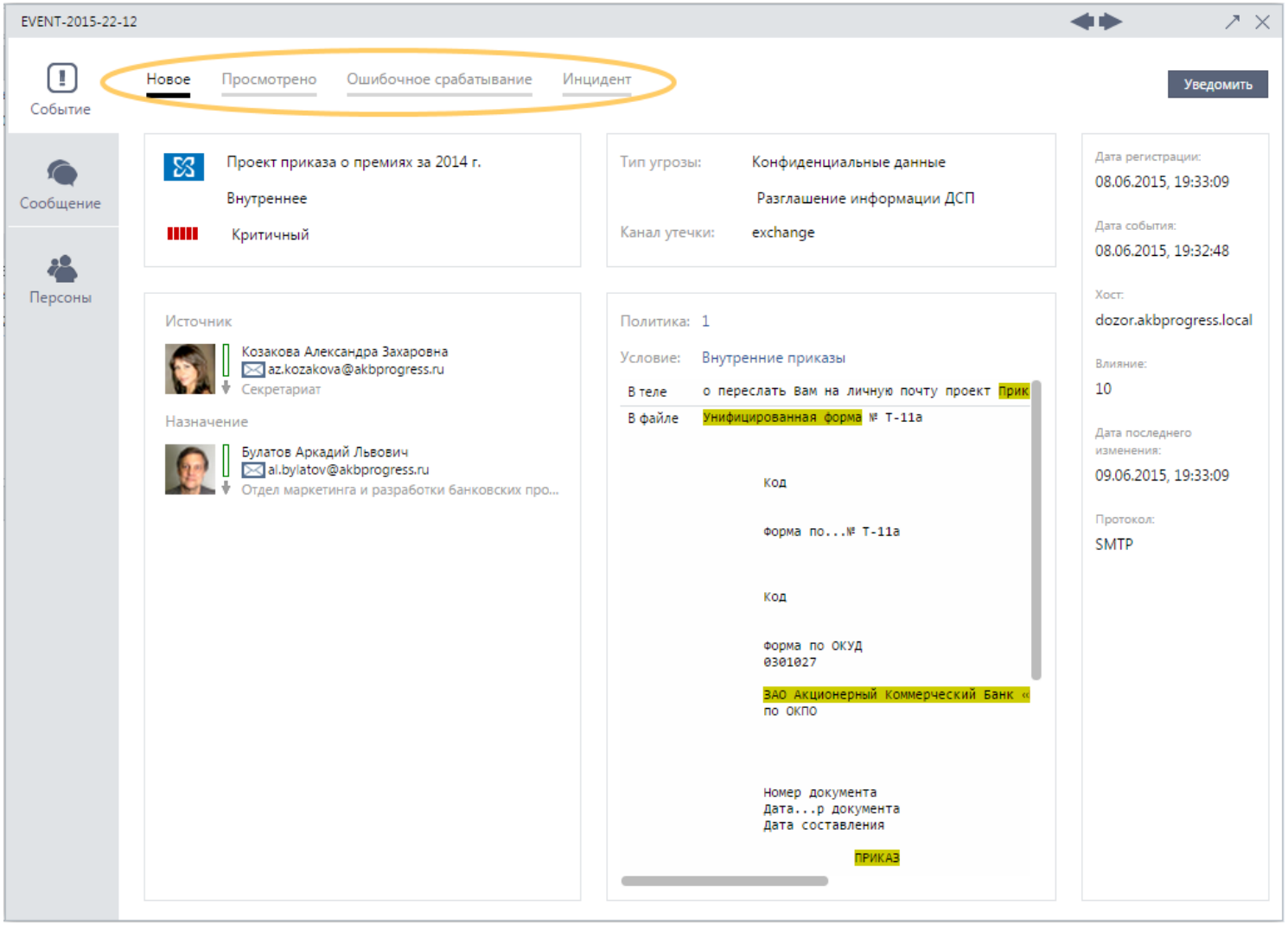
# «Уровень доверия» (неоф. «Карма»)



# «Уровень доверия» (неоф. «Карма»)

- По каждому субъекту отображается «уровень доверия» и динамика его изменений (аномалии поведения)
- Уровень доверия определяется на основании различных параметров выявленных событий (критичность инцидента, контекст, история событий и пр.) с использованием встроенных справочников
- Уровни критичности событий в системе: критичный, высокий, средний, низкий, инфо
- Одно и тоже событие для отправителя и получателя сообщения приведет к разному изменению уровня доверия (у отправителя, очевидно, измениться сильнее)
- При необходимости можно изменять (повышать / понижать / замораживать) уровень доверия для конкретных субъектов
- Можно делать выборку по всем сотрудниками или по конкретным группам (например, по отделу)

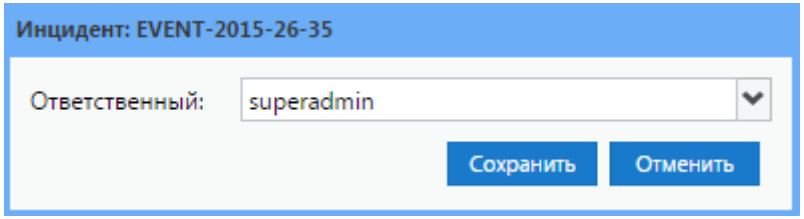
# От событий к инцидентам (v.5.0.4)



# От событий к инцидентам (v.5.0.4)

| Статус события | Статус инцидента |
|---|---|
| • новое<br>• просмотрено<br>• ошибочное срабатывание | • открыт<br>• закрыт<br>• не инцидент |

- На каждый инцидент назначается ответственный для его расследования:




- Расследование инцидента может быть отложенным


# 3. Оперативное реагирование на инцидент

# Оперативное реагирование

| Технические | Организационные |
| --- | --- |
| • Блокировка передачи (с уведомлением / без уведомления)<br>• Блокировка передачи до подтверждения<br>• Отправка сообщения с реконструкцией:<br>  • Удаление информации ограниченного доступа<br>  • Замена информации на предупреждение<br>  • Добавление предупреждения<br>• Блокирование доступа к ИС<br>• Оповещение службы охраны / ЧОП | • Получение объяснительной<br>• Изъятие оборудования*<br>• Досмотр*<br>• Обращение в МВД России / ФСБ России<br>• Задержание до выяснения* |


# 4. Расследование инцидента

# Инструменты расследования DLP

1. Детальная информация об инциденте
2. Архив сообщений
3. «Уровень доверия»
4. «Досье» (на субъекта)
5. Интерактивный «Граф связей»
6. Снимки экрана
7. Отчеты
8. Поиск

# Контроль персон. Досье

Общая информация

**Адресная информация**

**Профиль поведения**

Уровень доверия

Обогащение досье

Организационно-штатная структура

**Связи**

# Досье

Досье

Бубнов Вячеслав Самуилович

Добавить в группу | Добавить свойство | Удалить персону | Соединить карточки | Связи

**Бубнов Вячеслав Самуилович**

Динамика уровня доверия:

Сегодня: -86 Среднее: -34

**Дата рождения:**
05.12.1968

**Должность:**
Заместитель начальника отдела

**Подчиняется:**
Печеников Алексей Кириллович

**Отдел:** Отдел развития информационных тех...

**ID персоны:** 108

**Адреса**

| | |
|---|---|
| **email** | vs.bubnov@akbprogress.ru |
| **email** | bubnov1968@mail.ru |
| **icq** | 546878654845 |
| **ip** | 192.105.172.239 |
| **login** | vs.bubnov |
| **sid** | s-1-5-21-793904598-208165932-29... |
| **skype** | buben4ik |
| **url** | https://vk.com/id347832 |

Группы +

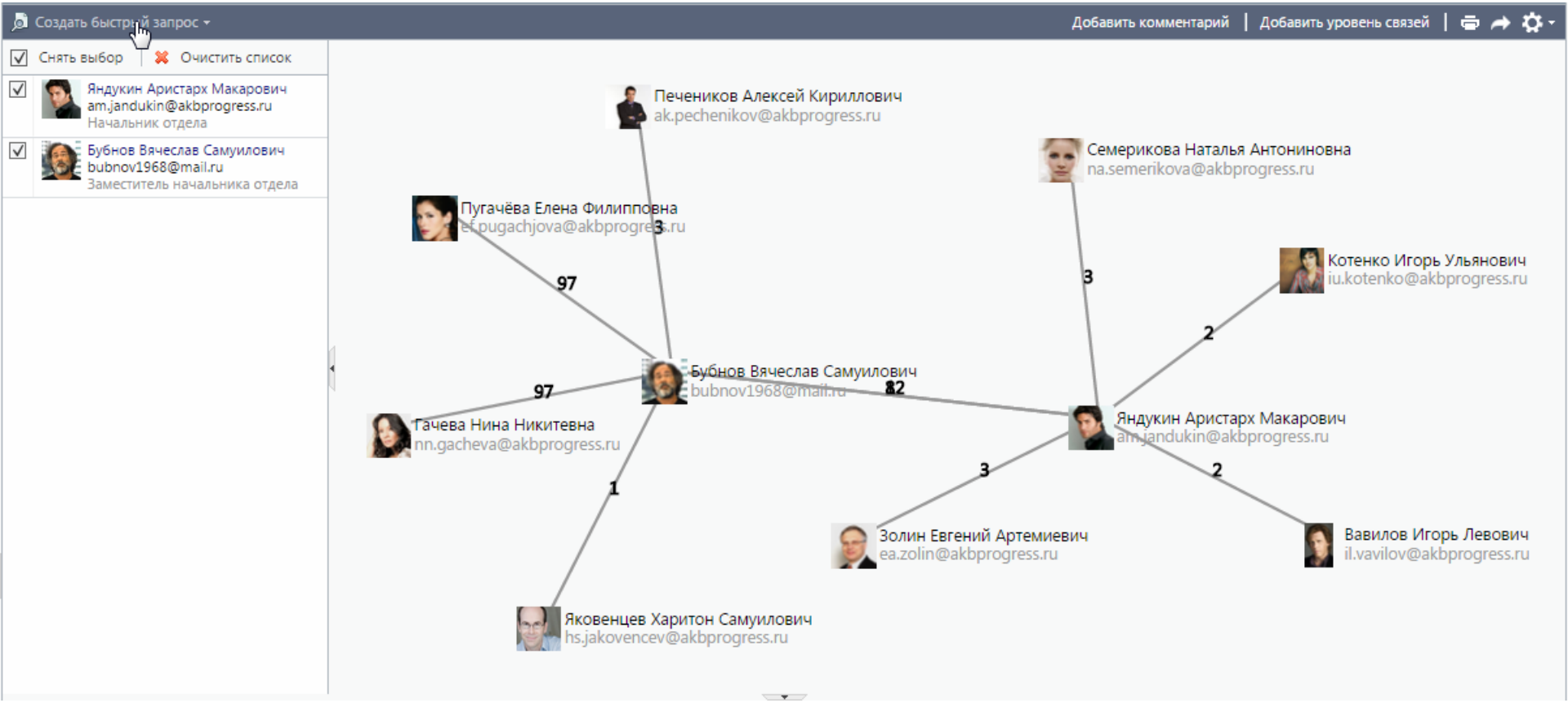
Свойства +

Уровни доверия +

**События и инциденты** | Сообщения | Переписка | Примечания | История изменений УД

| Уровень критичности | 06.2015 | 05.2015 | 04.2015 | 03.2015 | Всего |
|---|---|---|---|---|---|
| Критичный | 0 | 5 | 0 | 0 | 5 |
| Высокий | 2 | 0 | 0 | 0 | 2 |
| Средний | 0 | 0 | 0 | 0 | 0 |
| Низкий | 0 | 0 | 0 | 0 | 0 |
| Информация | 0 | 10 | 0 | 0 | 10 |
| **Всего** | **2** | **15** | **0** | **0** | **17** |

# Граф связей


Создать быстрый запрос
Добавить комментарий
Добавить уровень связей
Снять выбор
Очистить список
Яндукин Аристарх Макарович
am.jandukin@akbprogress.ru
Начальник отдела
Бубнов Вячеслав Самуилович
bubnov1968@mail.ru
Заместитель начальника отдела
Печеников Алексей Кириллович
ak.pechenikov@akbprogress.ru
Семерикова Наталья Антониновна
na.semerikova@akbprogress.ru
Пугачёва Елена Филипповна
Котенко Игорь Ульянович
iu.kotenko@akbprogress.ru
Бубнов Вячеслав Самуилович
bubnov1968@mail.ru
Гачева Нина Никитевна
nn.gacheva@akbprogress.ru
Яндукин Аристарх Макарович
am.jandukin@akbprogress.ru
Золин Евгений Артемиевич
ea.zolin@akbprogress.ru
Вавилов Игорь Левович
il.vavilov@akbprogress.ru
Яковенцев Харитон Самуилович
hs.jakovencev@akbprogress.ru
97
3
3
2
97
82
3
2
1

# Про поиск

- Можем искать:
  - Коммуникации (сообщения)
  - Пересылаемые файлы
  - Персон, участвующих в переписке

- Возможность создавать сложные поисковые запросы (более 50 атрибутов сообщений)
- Реализован «поиск похожих» (сообщения со сходным содержанием)
- Возможность поиска по пометкам в документах (аналог «тегов»)
- "Умный поиск" - возможность в один клик создать поисковый запрос


5. Реагирование на инцидент

# Решение в случае виновности сотрудника

А) По решению ИБ

1. Перевод в группу «Особый контроль»
2. Получение объяснительной
3. Профилактическая беседа

Б) По решению руководства и HR

4. Лишение благ и привилегий (втч и лишение прав доступа)
5. Дисциплинарные взыскания:
   - замечание
   - выговор

В) По решению руководства, HR, юристов и ИБ. Необходимо четкое понимание процедур и высокий уровень «бумажной безопасности»

   - увольнение по соответствующим основаниям
6. Увольнение по инициативе работника / по соглашению сторон
7. Возмещение ущерба
8. Уголовное преследование
9. Прочее

# Пример модели принятия решения по инциденту (по сумме баллов)

1. ***Какова величина ущерба?***
   Крупный – 6; Неизвестно или пока нет, но может быть – 3; Ущерба нет – 1
2. ***Выявлен ли умысел сотрудника?***
   Да – 3; Неизвестно – 1; Нет, инцидент по ошибке – 0
3. ***Какой уровень доверия к сотруднику?***
   Низкий – 3; Обычный – 1; Высокий – 0
4. ***Были ли у сотрудника инциденты до этого?***
   Да – 2; Нет – 0
5. ***Какова вероятность, что инцидент повториться у этого сотрудника?***
   Высокая – 3; Средняя (скорее нет, маловероятно) – 1; Низкая – 0

до 6 – вариант А; 6-12 – вариант Б; 13 и больше – вариант В

# Дисциплинарные взыскания по ТК РФ

ТК РФ ст.192-193

- 1 дисциплинарный проступок – 1 дисциплинарное взыскание
- Не позднее 6 месяцев со дня совершения проступка
- Не позднее 1 месяца со дня обнаружения проступка
- Необходимо запросить от работника письменное объяснение

Статья 81. Расторжение трудового договора по инициативе работодателя

6) однократного грубого нарушения работником трудовых обязанностей:

в) разглашения охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей, в том числе разглашения персональных данных другого работника

# Материальная ответственность по ТК РФ

ТК РФ ст.238-250

- Работник обязан возместить работодателю причиненный ему **прямой действительный ущерб**. Неполученные доходы (упущенная выгода) взысканию с работника **не подлежат**.
- Работник несет материальную ответственность в пределах своего среднего месячного заработка. Если больше, то нужно **судебное решение**.

# Статьи УК РФ

- Статья 183. Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну
- Статья 185.6. Неправомерное использование инсайдерской информации
- Статья 147. Нарушение изобретательских и патентных прав
- Статья 159. Мошенничество
- Статья 163. Вымогательство
- Статья 272. Неправомерный доступ к компьютерной информации
- Статья 273. Создание, использование и распространение вредоносных компьютерных программ
- Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей
- Статья 276. Шпионаж
- Статья 283. Разглашение государственной тайны

# Про доказательства для Суда

**Важные**:

- По ТК РФ: *Объяснительная от работника* (либо *Акт об отказе*), *Служебная записка об инциденте* и *Протокол заседания комиссии*, рассматривающей инцидент. В документах следует указать краткое описание инцидента, оценку тяжести и обстоятельства совершенного проступка.
- По УПК: *Показания потерпевшего, свидетеля*, *Заключение и показания эксперта* и *Заключение и показания специалиста*, *Вещественные доказательства*.

Отчеты DLP вторичны, но тоже принимаются Судом. Дополнительно к отчету рекомендуется приложить краткое описание решения с указанием сертификатов (подойдет брошюра от производителя).


# 6. Анализ причин инцидента и «полученных уроков»

# Что после реагирования?

- Подготовка и передача материалов на хранение (архив)
- Анализ причин инцидента
- Подготовка итогового отчета (при необходимости)
- Проведение итогового совещания (при необходимости)
- Награждение (или наказание) участников процедуры управления инцидентами (при необходимости)
- Решение о том, «что делать дальше»

# Что дальше?

- Ничего, все молодцы
- Проведение Аудита ИБ и/или дополнительных проверок
- Совершенствование процедуры управления инцидентами
- Совершенствование системы ИБ:
  - Пересмотр прав доступа
  - Пересмотр требований по обработке и хранению информации
  - Обучение и повышение осведомленности:
  - «Точная» настройка СЗИ
  - Внедрение новых мер и СЗИ
  - …
- Пересмотр кадровой политики (процедура найма и увольнения, мотивация персонала, корпоративная культура)
- Изменение бизнес-процессов

# Обучение и повышение осведомленности

| Кто? | Тематики |
|---|---|
| Рядовые пользователи | • Правила работы с информацией и средствами обработки<br>• Базовые требования по защите информации<br>• Кейсы (типовые ошибки, соц.инженерия)<br>• Ответственность |
| ИТ и ИБ-специалисты | • Процедуры обнаружения и реагирования на инциденты<br>• Расследование инцидентов<br>• Сбор цифровых доказательств<br>• Работа со средствами мониторинга и защиты информации |
| HR и юристы | • Вопросы подбора, развития, обучения, оценки, аттестации, мотивации, взысканий, увольнения персонала<br>• Судебная практика<br>• Развитие корпоративной культуры<br>• Compliance (соблюдение требований) |
| Менеджмент | • Кейсы (инциденты и ущерб)<br>• Базовые рекомендации по защите информации |


## Ключевые преимущества DLP Solar Dozor:

- Автоматизированная процедура управления инцидентами
- Удобные инструменты расследования инцидентов («Досье», «Граф связей», «Уровень доверия» и пр.)
- Архив всех сообщений, эффективный Поиск и настраиваемые Отчеты

**С уважением**,
Команда Solar Security

http://solarsecurity.ru
+7 (499) 755-07-70
info@solarsecurity.ru

# Приложение А.

## Стандарты и «лучшие практики» по управлению инцидентами

# «Лучшие практики» по управлению инцидентами ИБ (eng 1)

- Выписка из **ISO/IEC 27002:2013** (A.16 Information security incident management)
- **ISO/IEC 27035:2011** Information technology. Security techniques. Information security incident management. И проекты:
  - **CD 27035-1 Part 1**: Principles of incident management
  - **CD 27035-2 Part 2**: Guidelines to plan and prepare for incident response
  - **CD 27035-3 Part 3**: Guidelines for CSIRT operations
- **ISO/IEC 27037:2012** Information technology. Security techniques. Guidelines for identification, collection, acquisition and preservation of digital evidence
- **ISO/IEC 27043:2015** Information technology. Security techniques. Incident investigation principles and processes

# «Лучшие практики» по управлению инцидентами ИБ (eng 2)

- **NIST SP 800-61** Rev. 2 Computer Security Incident Handling Guide
- **NIST SP 800-83** Rev.1 Guide to Malware Incident Prevention and Handling for Desktops and Laptops
- **NIST SP 800-86** Guide to Integrating Forensic Techniques into Incident Response
- Выписка из **NIST SP 800-53 Rev. 4** Security and Privacy Controls for Federal Information Systems and Organizations (Security control: IR - Incident Response)
- **ENISA** Good Practice Guide for Incident Management
- Материалы **SANS Institute** InfoSec Reading Room. Incident Handling (более 100 документов)

# «Лучшие практики» по управлению инцидентами ИБ (rus)

- **РС БР ИББС-2.5-2014** Менеджмент инцидентов ИБ
- Выписка из **СТО БР ИББС-1.0-2014** (8.10. Требования к организации обнаружения и реагирования на инциденты информационной безопасности)
- **ГОСТ Р ИСО/МЭК 27037-2014** Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме
- Устаревшие версии:
  - Выписка из **ГОСТ Р ИСО/МЭК 27002-2012** (А13. Менеджмент инцидентов ИБ)
  - **ГОСТ Р ИСО/МЭК ТО 18044-2007** Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности

# «Лучшие практики» по управлению инцидентами (ITSM)

- **Процессы COBIT5** (книги COBIT5 Enabling Processes и COBIT5 for Information Security):
  - DSS 02  Manage Service Requests and Incidents
  - DSS 03 Manage Problems
- **Процессы ITIL** (книга Service operation):
  - Event management
  - Incident management
  - Problem management
- **Процессы ISO 20000**:
  - Incident Management
  - Problem management