# Управление и автоматизация процессов ИБ на предприятиях промышленного сектора

**Федор Горловский**
Директор по развитию бизнеса

**20 сентября 2016 года**

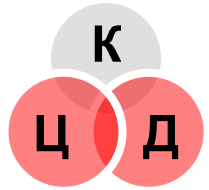
# Содержание

Роль CISO в промышленности – цели и задачи
Управление информационной безопасностью (ИБ)
Архитектура СУАИБ
SIEM (Система мониторинга событий ИБ)
Ситуационный центр (ISOC)
Управление инцидентами ИБ
Управление уязвимостями, базы репутации (российские и иностранные, СОПКА (GOV-CERT) и FinCERT)
Управление активами
Управление рисками ИБ
Управление соответствием (Compliance), требования бизнеса и «бумажная безопасность»
Управление решениями
Управление осведомленностью
Визуализация (Графики, KPI, отчеты)
Развитие отделов ИБ

© 2016 ООО «Интеллектуальная безопасность»

# Роль CISO в промышленности – цели и задачи

Цель CISO – защитить наиболее ценные информационные активы компании (АСУТП, интеллектуальную собственность, деньги, данные о клиентах, бренд, др.)




## Задачи CISO:

1

**Операционные**

Реагирование на инциденты ИБ;

Приобретение и настройка СЗИ;

Внедрение неотложных процедур для обеспечения ИБ.

2

**Тактические**

Планирование активностей по ИБ на ближайшее будущее;

Обеспечение соответствия требованиям законодательства и стандартам (Compliance);

Выполнение проектов по ИБ.

3

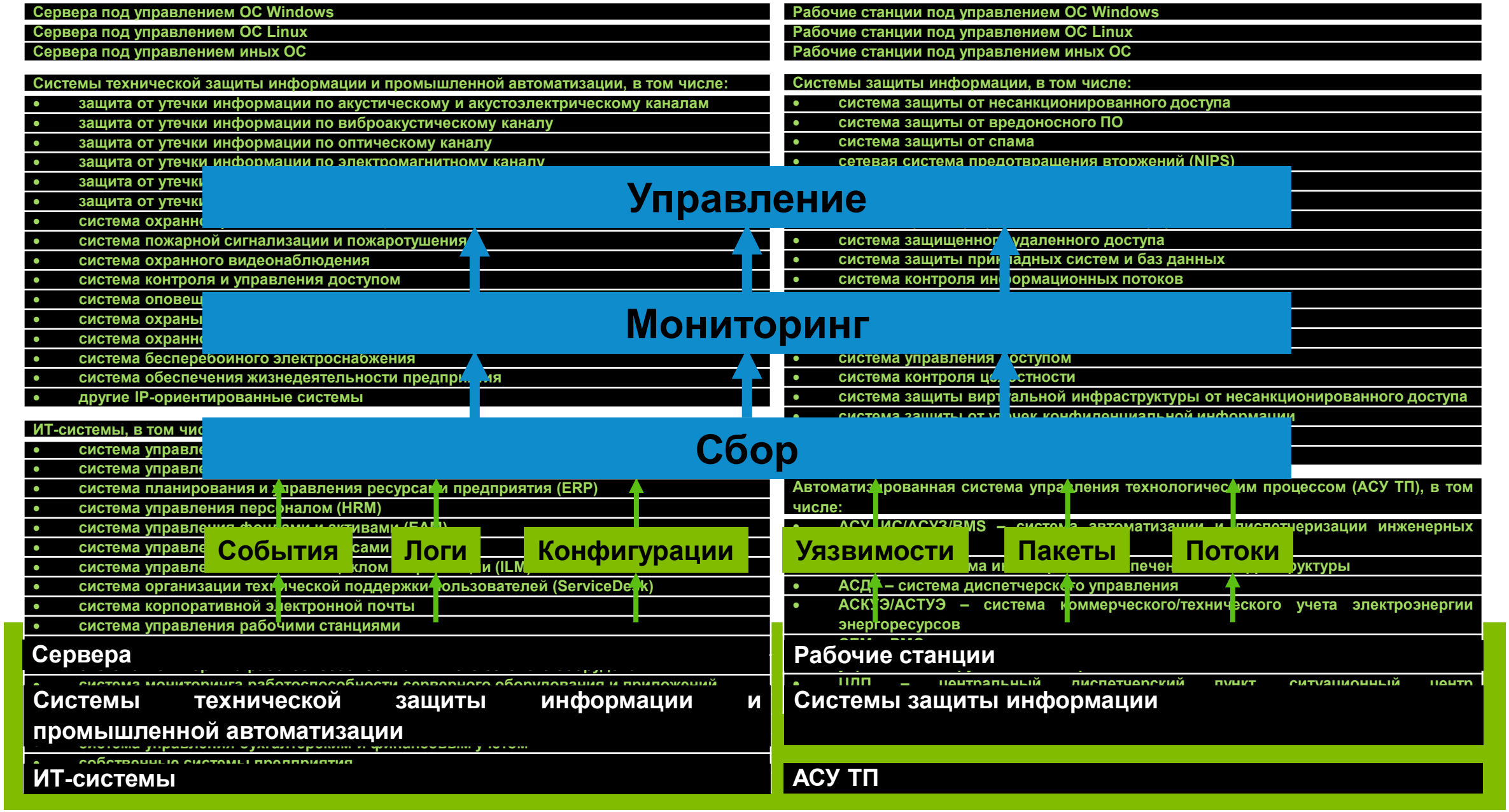
**Стратегические**

Стратегическое планирование, взаимодействие с CEO, CIO и др. CXOs;

Разработка политики ИБ, регламентов, инструкций;

Дизайн, управление и автоматизация процессов ИБ.

© 2016 ООО «Интеллектуальная безопасность»




© 2016 ООО «Интеллектуальная безопасность»

# Архитектура СУАИБ

На уровне сбора собирается информация (события, логи, конфигурации, уязвимости, пакеты, потоки, доступность) со всего IP-ориентированного оборудования.

Собранная информация передается на уровень ядра, где она обрабатывается, приводится к единому формату и нормализуется. Сохраняется информация по событиям не связанным с инцидентами ИБ, а вся информация об инцидентах ИБ передается на уровень управления.

На уровне управления единый портал позволяет управлять и автоматизировать инциденты ИБ, активы, риски, инвентаризацию и контроль целостности, отчетность и другие процессы. Здесь работают модули для визуализации ИБ-картины.


© 2016 ООО «Интеллектуальная безопасность»

# SIEM (Система мониторинга событий ИБ)

В России сегодня **отсутствуют** полноценные аналоги западных SIEM-систем.

В России сегодня есть:

- качественные продукты с урезанным функционалом полноценных SIEM-систем;
- продукты крайне сомнительного качества.

При выборе SIEM-системы **особое** внимание следует уделить **пилотированию**.

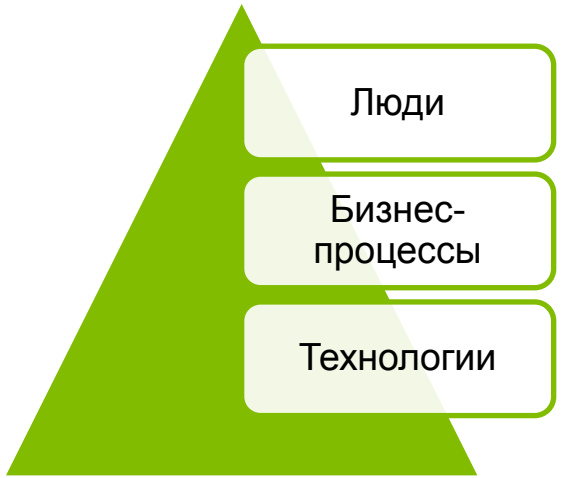
Во многих (не во всех) случаях есть возможность использовать западную SIEM-систему **российской сборки** в рамках программы импортозамещения.

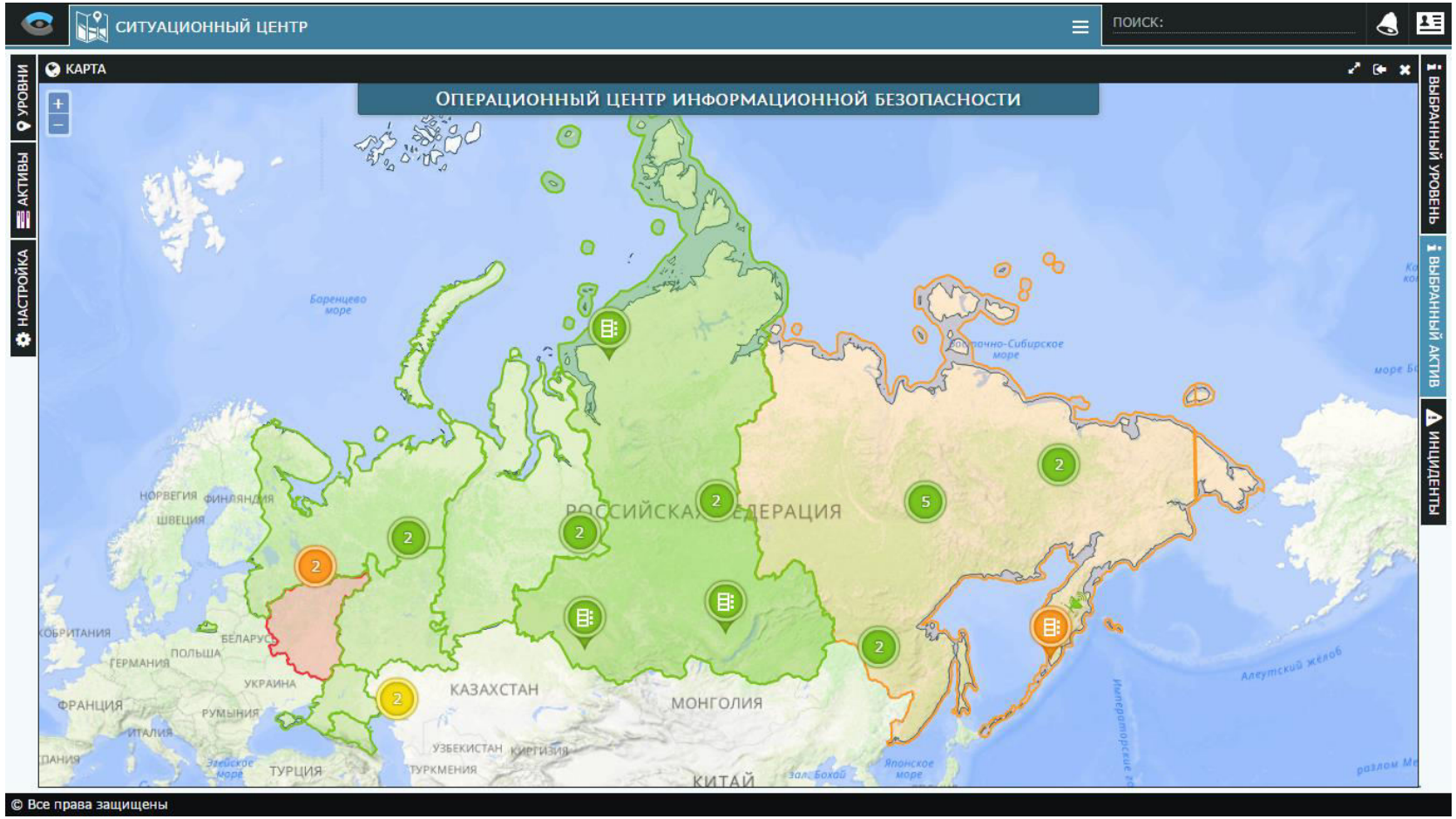

© 2016 ООО «Интеллектуальная безопасность»

# Ситуационный центр (ISOC)

ISOC – это не просто SIEM. SIEM лишь одна из составляющих ISOC.

ISOC – это:




© 2016 ООО «Интеллектуальная безопасность»

# Управление инцидентами ИБ

Управление != мониторинг

Управление инцидентами != мониторинг инцидентов

Современный инструментарий управления инцидентами представляет собой:

- ✓ комплекс представлений (от табличных до масштабируемой карты мира)
- ✓ интегрирован с системой управления активами ИБ
- ✓ с возможностью полного управления процессом (от назначения ответственного до закрытия инцидента)
- ✓ с сохранением всей истории по данному инциденту
- ✓ и с гибкой системой предоставления прав администраторам ИБ.

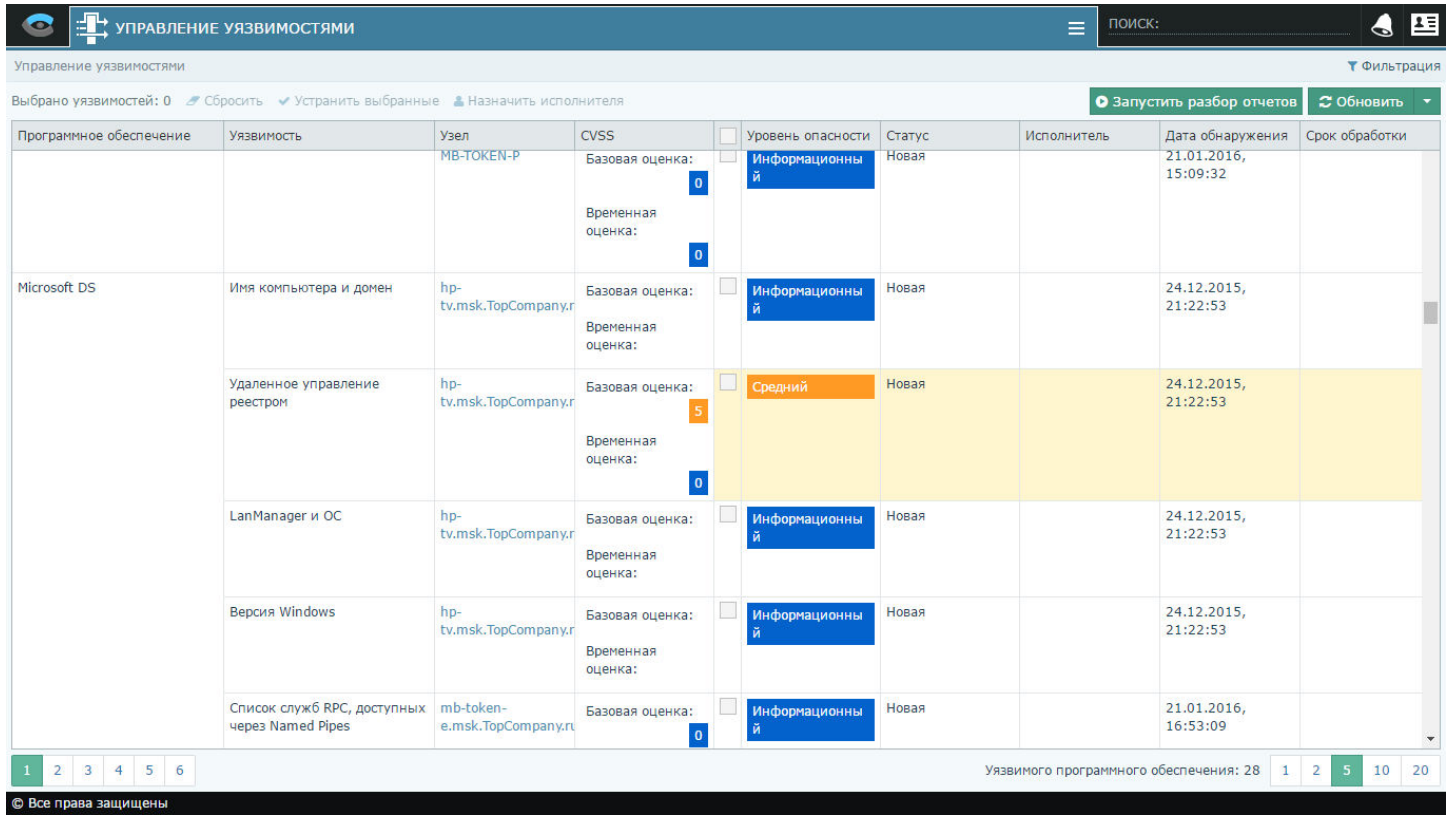

© 2016 ООО «Интеллектуальная безопасность»

# Управление уязвимостями, базы репутации (коммерческие российские и иностранные, государственные СОПКА (GOV-CERT) и FinCERT)

В России создан ряд государственных и частных центров реагирования на инциденты компьютерной безопасности. В международной практике известные как Computer Emergency Response Team CERT или Computer Security Incident Response Team CSIRT. В отечественных силовых структурах и Минобороны больше известные как СОПКА/СПОКА.

Среди наиболее известных центры: GOV-CERT.RU, FinCERT, CERT-GIB, RU-CERT, WebPlus ISP, CSIRT АРСИБ, CERT Ростеха.

ISOC должен иметь возможность интегрироваться с репутационными сервисами и с CERTами для обогащения актуальной информацией и качественного реагирования на современные угрозы ИБ.



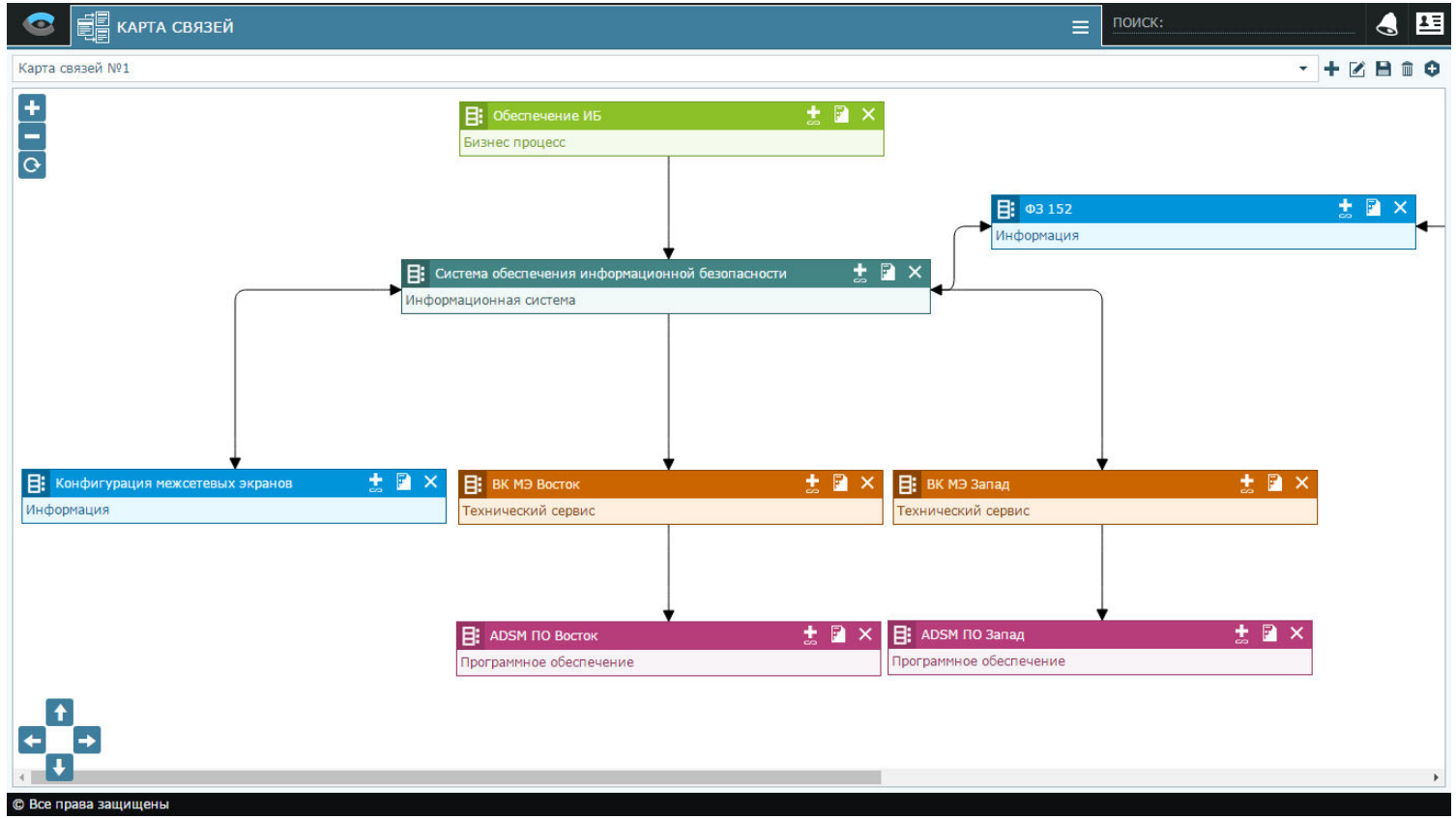

© 2016 ООО «Интеллектуальная безопасность»

# Управление активами

Управление активами – фундамент для построения СУИБ.

Современный инструментарий управления активами представляет собой:

- ✓ комплекс представлений (от табличных до карты связей активов)
- ✓ используется для каталогизации информации по всем активам, важным с точки зрения ИБ
- ✓ интегрирован с другими модулями СУИБ
- ✓ с возможностью управления разными типами активов
- ✓ с функционалом импорта/экспорта активов
- ✓ и с гибкой системой предоставления прав администраторам ИБ.



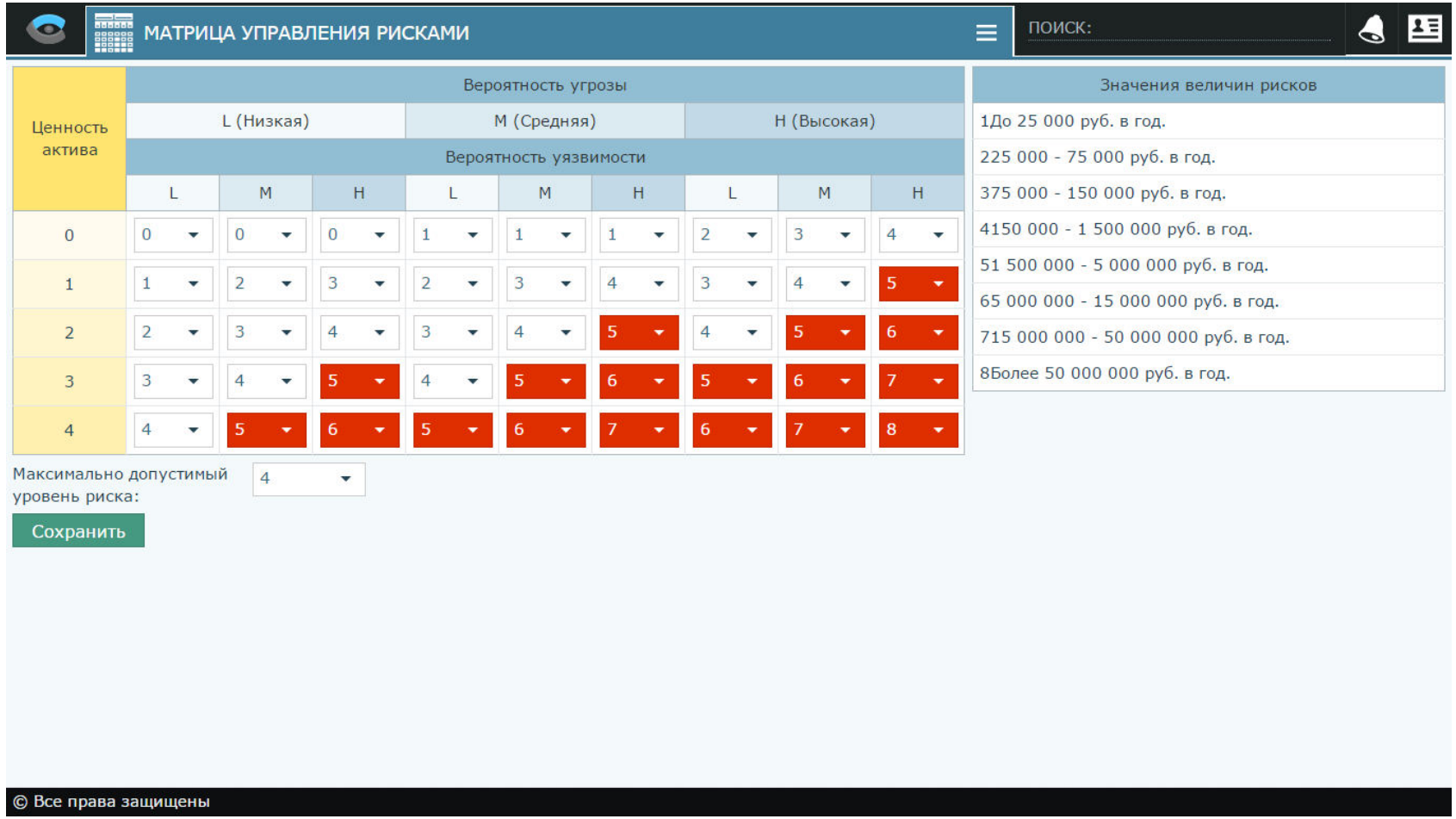

© 2016 ООО «Интеллектуальная безопасность»

# Управление рисками ИБ

Управление рисками ИБ позволяет организации снижать ущерб от реализации рисков.

Должны быть интеграция с системой по управлению активами, модель угроз и др. персонализированные под конкретную организацию функции.

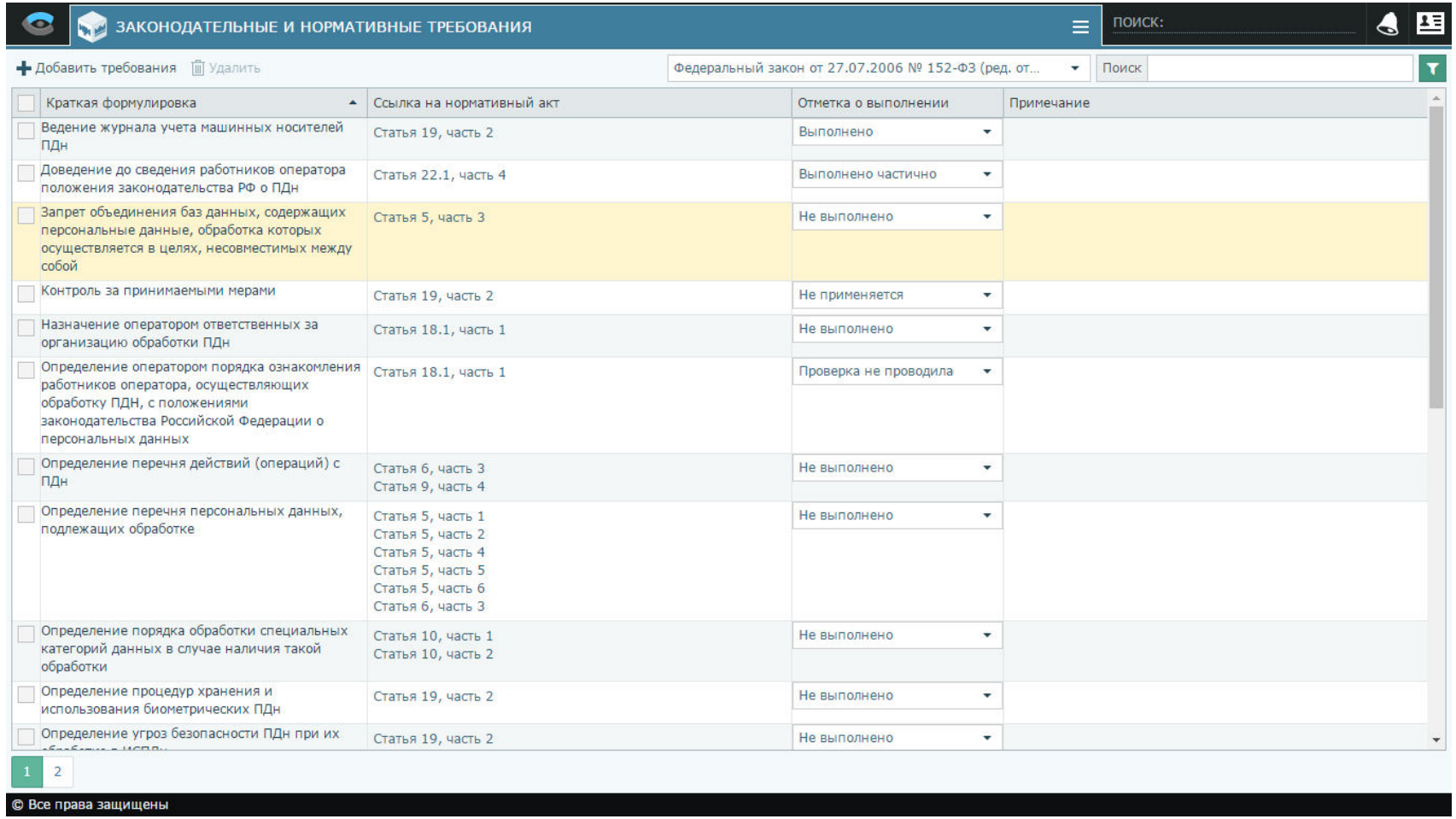
Система управления рисками ИБ должна быть совместима со стандартами по управлению рисками, например ISO/IEC 27005.




© 2016 ООО «Интеллектуальная безопасность»

# Управление соответствием (Compliance), требования бизнеса и «бумажная безопасность»

Современная система управления соответствием (Compliance) требованиям стандартов, законодательства и бизнеса позволяет автоматизировать внутренние аудиты.



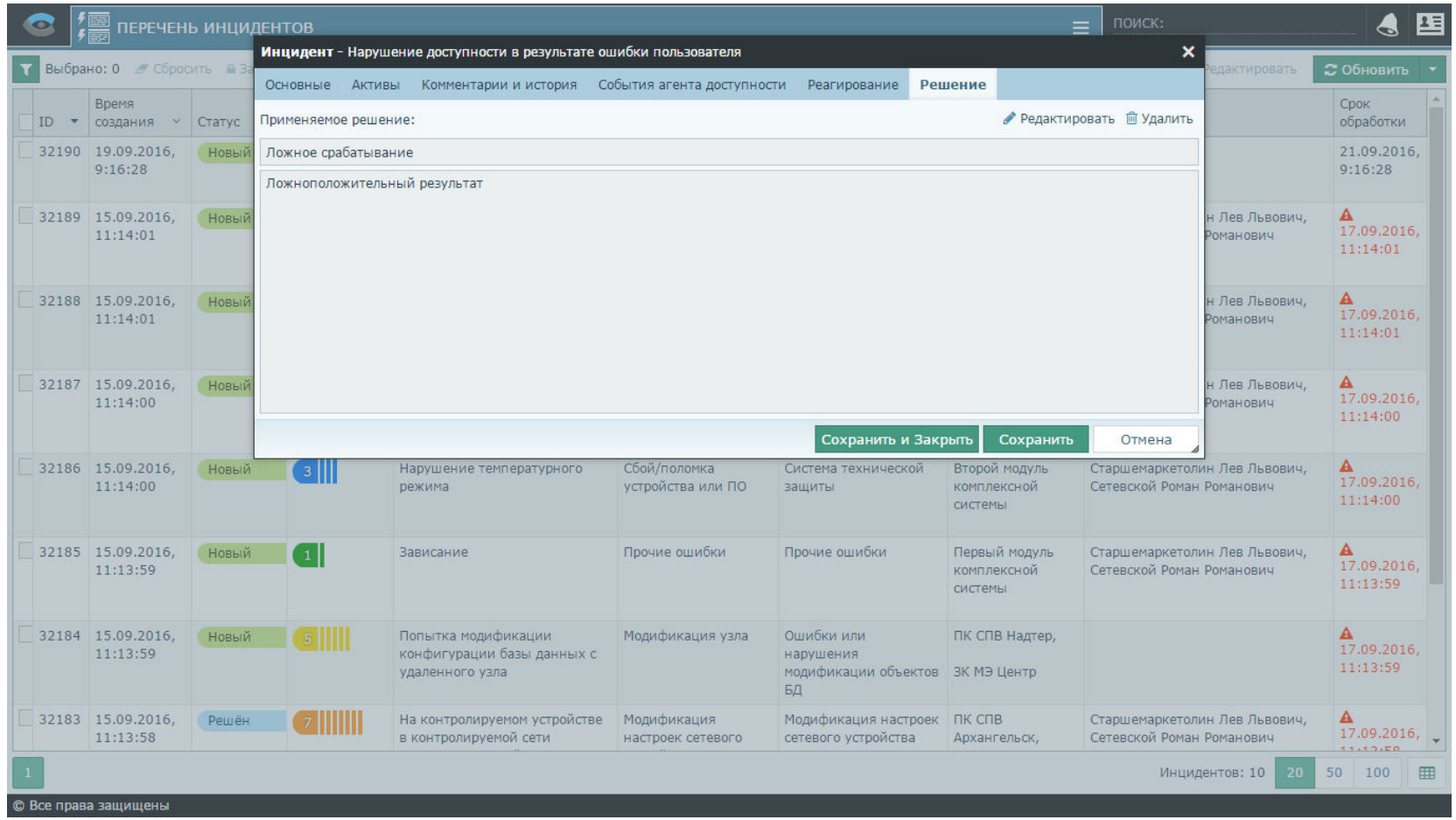

© 2016 ООО «Интеллектуальная безопасность»

# Управление решениями

Система управления знаниями предлагает ответственному за инцидент администратору ИБ варианты решения инцидента.

Источники решений системы:

- ✓ база решений производителя ПО
- ✓ данные по решенным ранее схожим инцидентам
- ✓ математическое моделирование вероятных решений

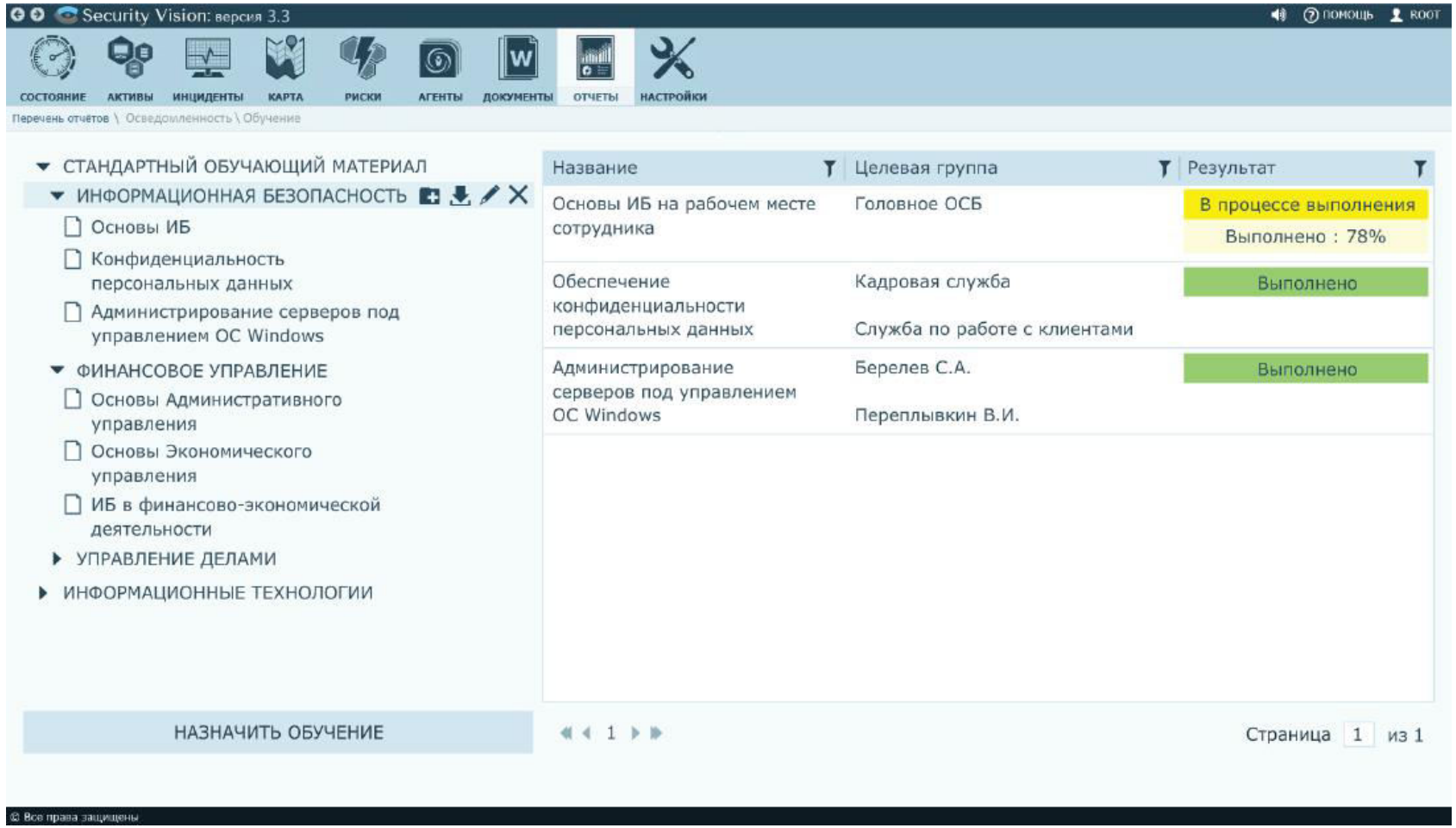



© 2016 ООО «Интеллектуальная безопасность»

# Управление осведомленностью

Система управления осведомленностью позволяет:

- ✓ разрабатывать планы обучения персонала в области ИБ
- ✓ контролировать сроки и завершенность обучений сотрудников организации
- ✓ формировать отчеты

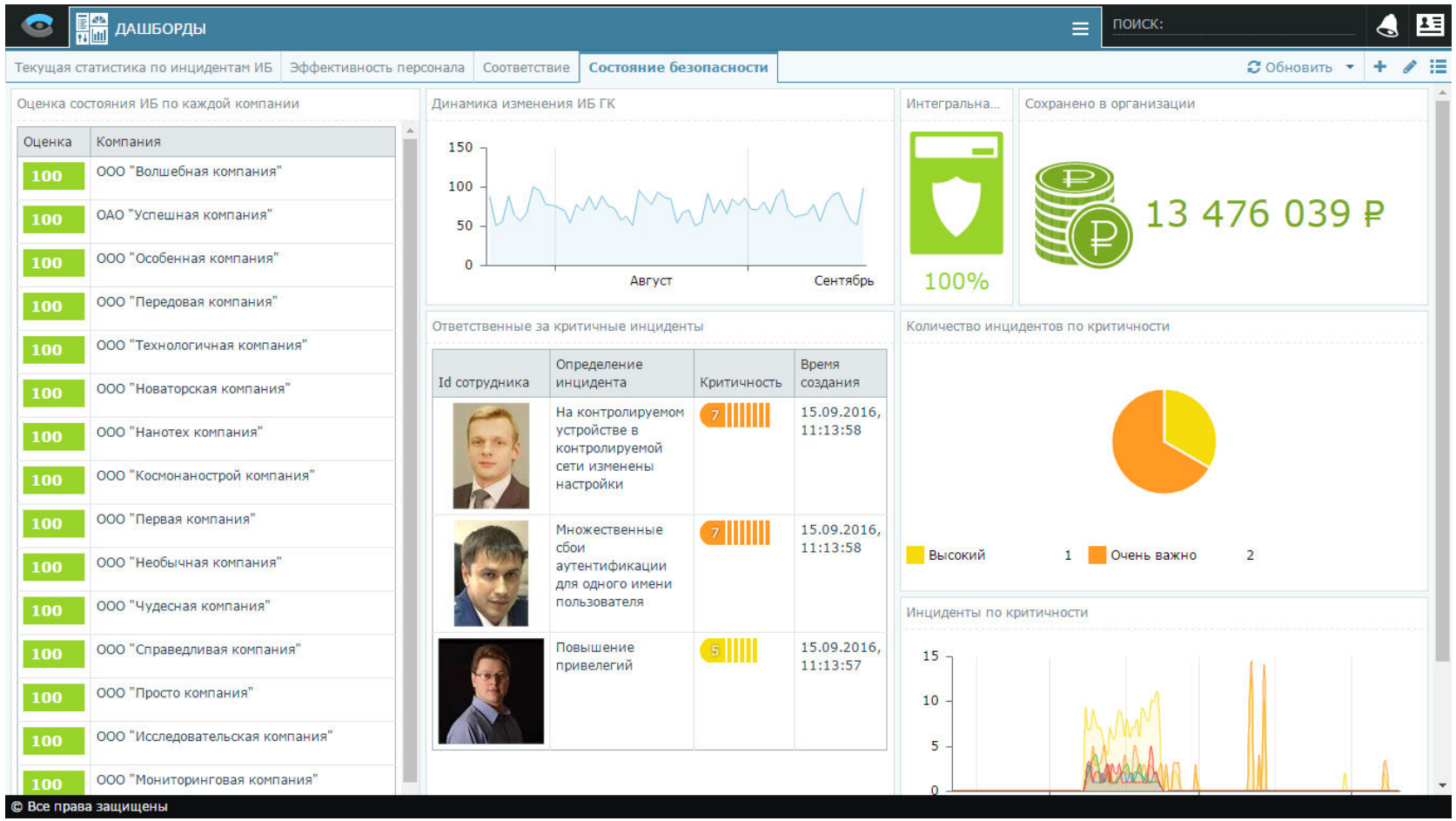



© 2016 ООО «Интеллектуальная безопасность»

# Визуализация (Графики, KPI, отчеты)

Единая точка, где можно все увидеть:

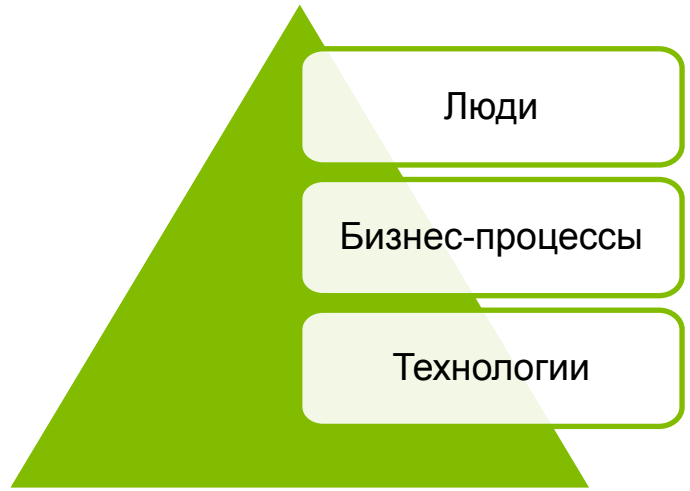
- ✓ Гибкая ролевая модель
- ✓ Модуль KPI
- ✓ Конструктор графиков с предустановленными шаблонами и возможностью написания собственного кода
- ✓ Конструктор отчетов с возможностью забора данных как из разных БД




© 2016 ООО «Интеллектуальная безопасность»

# Развитие отделов ИБ

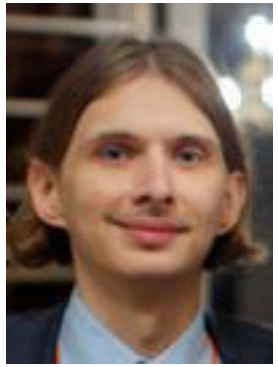
| Текущий уровень | Переход | Точки роста |
|---|---|---|
| 0. ИБ отсутствует | 0 → 1 | ✓ Назначить ответственного за ИБ сотрудника;<br>✓ Начать с решения самых горящих ИБ вопросов |
| 1. Работаем на операционном уровне (тушим пожары) | 1 → 2 | ✓ Посоветоваться с «коллегами по цеху» (другими директорами ИБ) о дальнейшем развитии ИБ;<br>✓ Запланировать ИБ проекты на ближайшую перспективу и реализовать их. |
| 2. Работаем на тактическом уровне (среднесрочное планирование) | 2 → 3<br>СУАИБ<br>ISOC | ✓ Войти в контакт с советом директоров по вопросам ИБ;<br>✓ Разработать и выполнять стратегию ИБ;<br>✓ Произвести дизайн процессов ИБ, управлять процессами ИБ;<br>✓ Начать управлять рисками ИБ. |
| 3. Работаем на стратегическом уровне (долгосрочное планирование) | 3 → 4 | ✓ Повышать эффективность управления ИБ;<br>✓ Автоматизировать все, что целесообразно автоматизировать;<br>✓ Повышать осведомленность (собственную, подчиненных, всех сотрудников организации) в области ИБ. |




Слагаемые успеха

© 2016 ООО «Интеллектуальная безопасность»

# Контакты




**Федор Горловский**

Директор по развитию бизнеса

fg@securityvision.ru

M: +7 (926) 619 3379


**www.sintelligence.ru**

**О компании «Интеллектуальная безопасность»**

Компания Интеллектуальная безопасность специализируется в области разработки и внедрения инновационного программного обеспечения по управлению информационной безопасностью. Все технические решения компании Интеллектуальная безопасность основаны на новейших достижениях в области сетевых, компьютерных и коммуникационных технологий и используют оборудование и программное обеспечение производства ведущих компаний.

Компания Интеллектуальная безопасность использует индивидуальный подход, учитывая отраслевую специфику работы Заказчика. Компания Интеллектуальная безопасность использует комплексный подход, оценивая состояние информационной безопасности Заказчика и защищенность активов компании со всех сторон: Организационную составляющую; Физическую/техническую безопасность; Комплексную информационную безопасность.


Настоящее сообщение содержит информацию только общего характера. При этом ни компания Интеллектуальная безопасность, ни входящие в нее юридические лица, ни их аффилированные лица (далее — «группа «Интеллектуальная безопасность») не представляют посредством данного сообщения каких-либо консультаций или услуг профессионального характера. Ни одно из юридических лиц, входящих в группу «Интеллектуальная безопасность», не несет ответственности за какие-либо убытки, понесенные любым лицом, использующим настоящее сообщение.