



SECURITY VISION



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

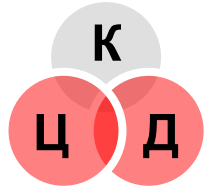
Визуализация (Графики, KPI, отчеты)

Развитие отделов ИБ

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.

Сервера под управлением ОС Windows
Сервера под управлением ОС Linux
Сервера под управлением иных ОС

Рабочие станции под управлением ОС Windows
Рабочие станции под управлением ОС Linux
Рабочие станции под управлением иных ОС

Системы технической защиты информации и промышленной автоматизации, в том числе:

- защита от утечки информации по акустическому и акустоэлектрическому каналам
- защита от утечки информации по виброакустическому каналу
- защита от утечки информации по оптическому каналу
- защита от утечки информации по электромагнитному каналу

Системы защиты информации, в том числе:

- система защиты от несанкционированного доступа
- система защиты от вредоносного ПО
- система защиты от спама
- сетевая система предотвращения вторжений (NIPS)

Управление

- система охранного видеонаблюдения
- система пожарной сигнализации и пожаротушения
- система контроля и управления доступом
- система оповещения

- система защищенного удаленного доступа
- система защиты прикладных систем и баз данных
- система контроля информационных потоков

Мониторинг

- система охраны
- система охраны
- система бесперебойного электроснабжения
- система обеспечения жизнедеятельности предприятия
- другие IP-ориентированные системы

- система управления доступом
- система контроля целостности
- система защиты виртуальной инфраструктуры от несанкционированного доступа
- система защиты от утечек конфиденциальной информации

Сбор

ИТ-системы, в том числе:

- система управления
- система управления
- система планирования и управления ресурсами предприятия (ERP)
- система управления персоналом (HRM)
- система управления финансами и активами (FAM)
- система управления самими собой (ILM)
- система управления рабочими станциями
- система организации технической поддержки пользователей (ServiceDesk)
- система корпоративной электронной почты
- система управления рабочими станциями

Автоматизированная система управления технологическим процессом (АСУ ТП), в том числе:

- АСУ ИС/АСУЗ/ВМС – система автоматизации и диспетчеризации инженерных систем и печен
- АСД – система диспетчерского управления
- АСКУЭ/АСТУЭ – система коммерческого/технического учета электроэнергии

События

Логи

Конфигурации

Уязвимости

Пакеты

Потоки

Сервера

Системы технической защиты информации и промышленной автоматизации

ИТ-системы

Рабочие станции

Системы защиты информации

АСУ ТП

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.



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**.

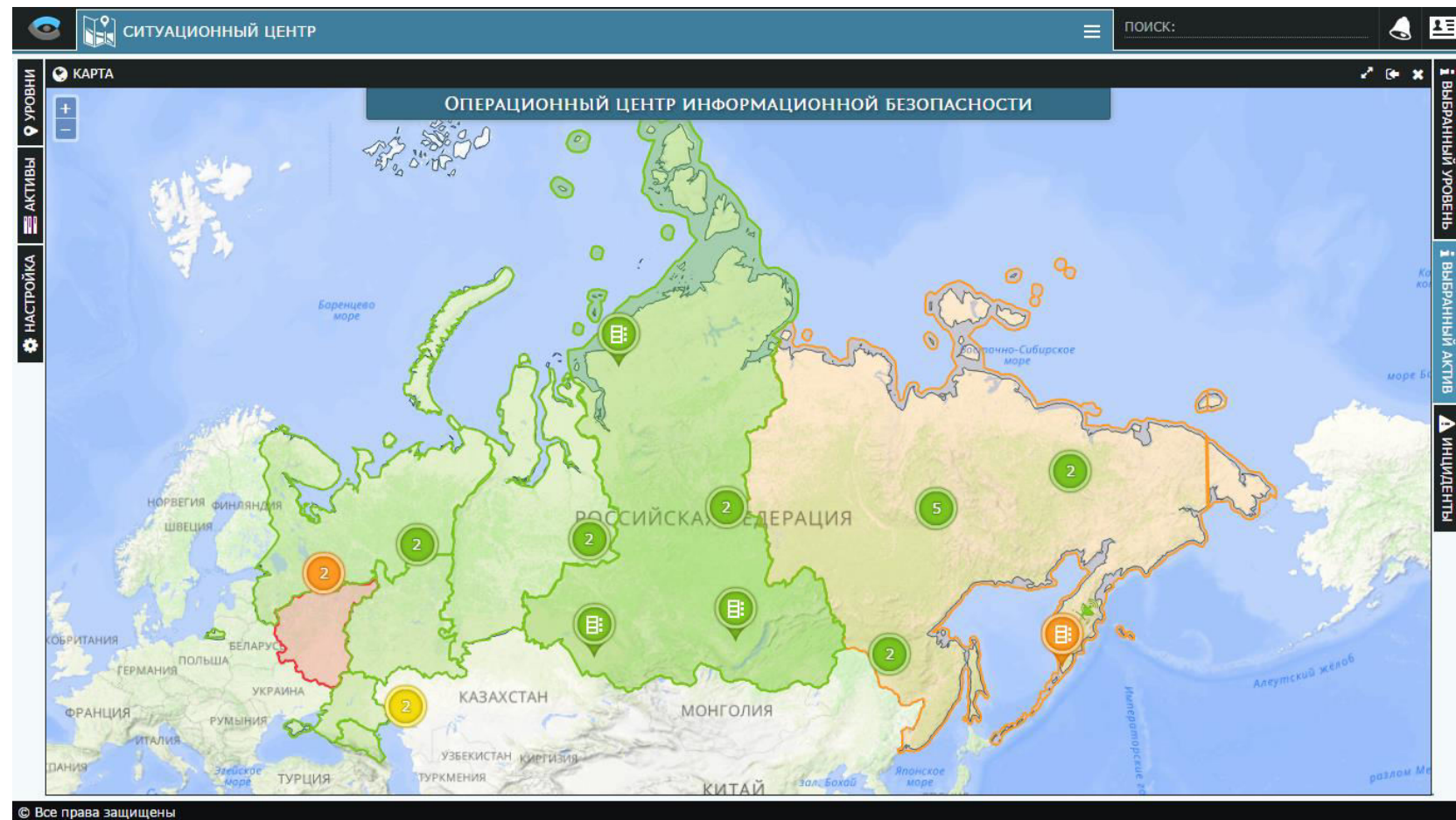
Во многих (не во всех) случаях есть возможность использовать западную SIEM-систему **российской сборки** в рамках программы импортозамещения.



Ситуационный центр (ISOC)

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

ISOC – это:



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.

ID	Время создания	Статус	Критичность	Название	Класс	Подкласс	Активы	Исполнители	Срок обработки
32190	19.09.2016, 9:16:28	Новый	7	Нарушение доступности в результате ошибки пользователя	Ошибка пользователя	Нарушение доступности	Проверка DNS		21.09.2016, 9:16:28
32189	15.09.2016, 11:14:01	Новый	9	Полный выход из строя	Сбой/поломка устройства или ПО	Сервер/АРМ	Пятый модуль комплексной системы	Старшемаркетолин Лев Львович, Сетевской Роман Романович	17.09.2016, 11:14:01
32188	15.09.2016, 11:14:01	Новый	7	Закреплен троян	Подозрительная локальная активность	Подозрительная локальная активность	Четвёртый модуль комплексной системы	Старшемаркетолин Лев Львович, Сетевской Роман Романович	17.09.2016, 11:14:01
32187	15.09.2016, 11:14:00	Новый	5	Попытка неправомерного доступа	Подозрительная сетевая активность	Нехарактерный или иной подозрительный сетевой трафик	Третий модуль комплексной системы	Старшемаркетолин Лев Львович, Сетевской Роман Романович	17.09.2016, 11:14:00
32186	15.09.2016, 11:14:00	Новый	3	Нарушение температурного режима	Сбой/поломка устройства или ПО	Система технической защиты	Второй модуль комплексной системы	Старшемаркетолин Лев Львович, Сетевской Роман Романович	17.09.2016, 11:14:00
32185	15.09.2016, 11:13:59	Новый	1	Зависание	Прочие ошибки	Прочие ошибки	Первый модуль комплексной системы	Старшемаркетолин Лев Львович, Сетевской Роман Романович	17.09.2016, 11:13:59
32184	15.09.2016, 11:13:59	Новый	5	Попытка модификации конфигурации базы данных с удаленного узла	Модификация узла	Ошибки или нарушения модификации объектов БД	ПК СПВ Надтер, ЭК МЭ Центр		17.09.2016, 11:13:59
32183	15.09.2016, 11:13:58	Решён	7	На контролируемом устройстве в контролируемой сети	Модификация настроек сетевого	Модификация настроек сетевого устройства	ПК СПВ Архангельск,	Старшемаркетолин Лев Львович, Сетевской Роман Романович	17.09.2016, 11:13:58

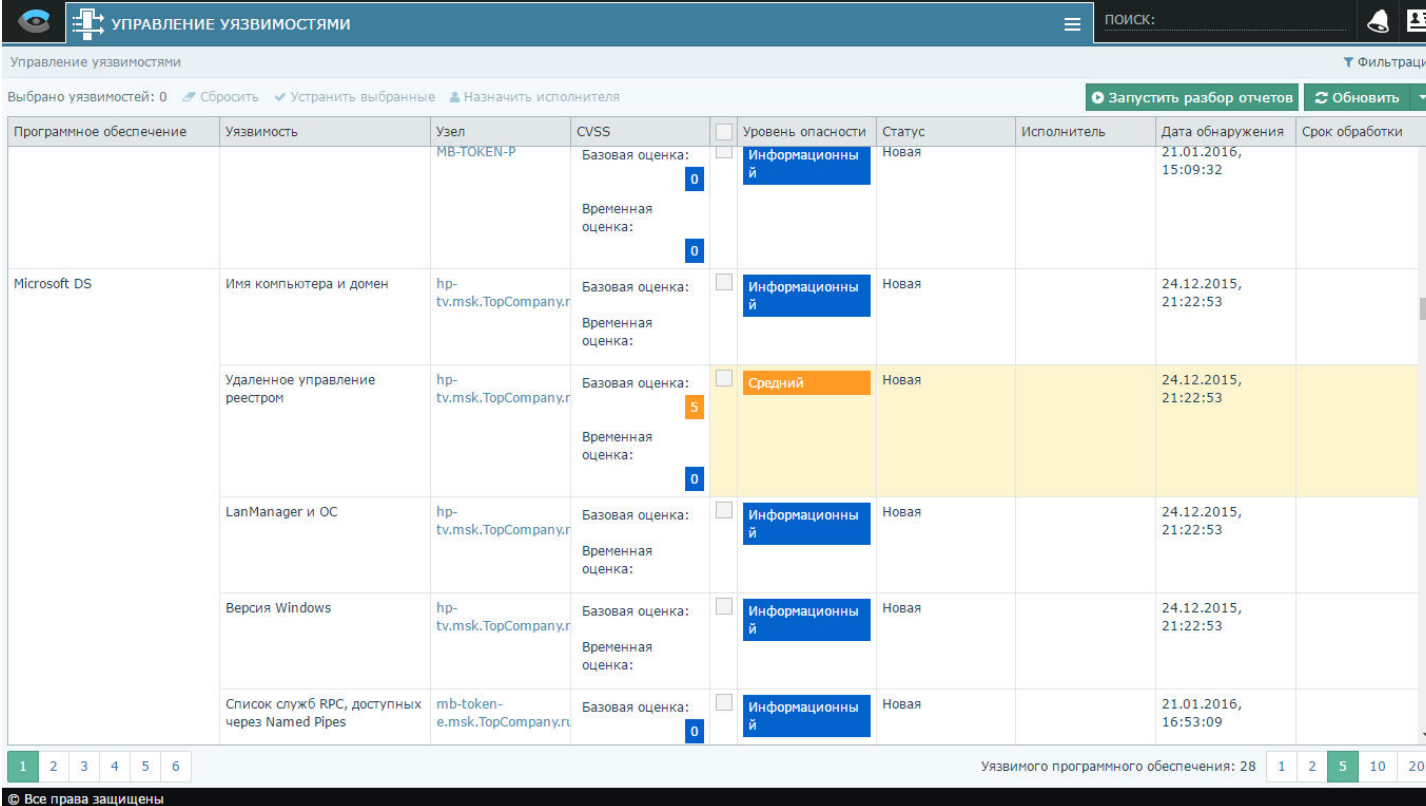
Инцидентов: 10 20 50 100

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 известны как Computer Emergency Response Team CERT или Computer Security Incident Response Team CSIRT. В отечественных силовых структурах и Минобороны больше известны 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.



УПРАВЛЕНИЕ УЯЗВИМОСТЯМИ

Управление уязвимостями

Выбрано уязвимостей: 0 Сбросить Устранить выбранные Назначить исполнителя

Запустить разбор отчетов Обновить

Программное обеспечение	Уязвимость	Узел	CVSS	Уровень опасности	Статус	Исполнитель	Дата обнаружения	Срок обработки
		MB-TOKEN-P	Базовая оценка: 0 Временная оценка: 0	Информационный	Новая		21.01.2016, 15:09:32	
Microsoft DS	Имя компьютера и домен	hp-tv.msk.TopCompany.ru	Базовая оценка: 0 Временная оценка: 0	Информационный	Новая		24.12.2015, 21:22:53	
	Удаленное управление реестром	hp-tv.msk.TopCompany.ru	Базовая оценка: 5 Временная оценка: 0	Средний	Новая		24.12.2015, 21:22:53	
LanManager и ОС		hp-tv.msk.TopCompany.ru	Базовая оценка: 0 Временная оценка: 0	Информационный	Новая		24.12.2015, 21:22:53	
Версия Windows		hp-tv.msk.TopCompany.ru	Базовая оценка: 0 Временная оценка: 0	Информационный	Новая		24.12.2015, 21:22:53	
Список служб RPC, доступных через Named Pipes		mb-token-e.msk.TopCompany.ru	Базовая оценка: 0	Информационный	Новая		21.01.2016, 16:53:09	

Уязвимость программного обеспечения: 28

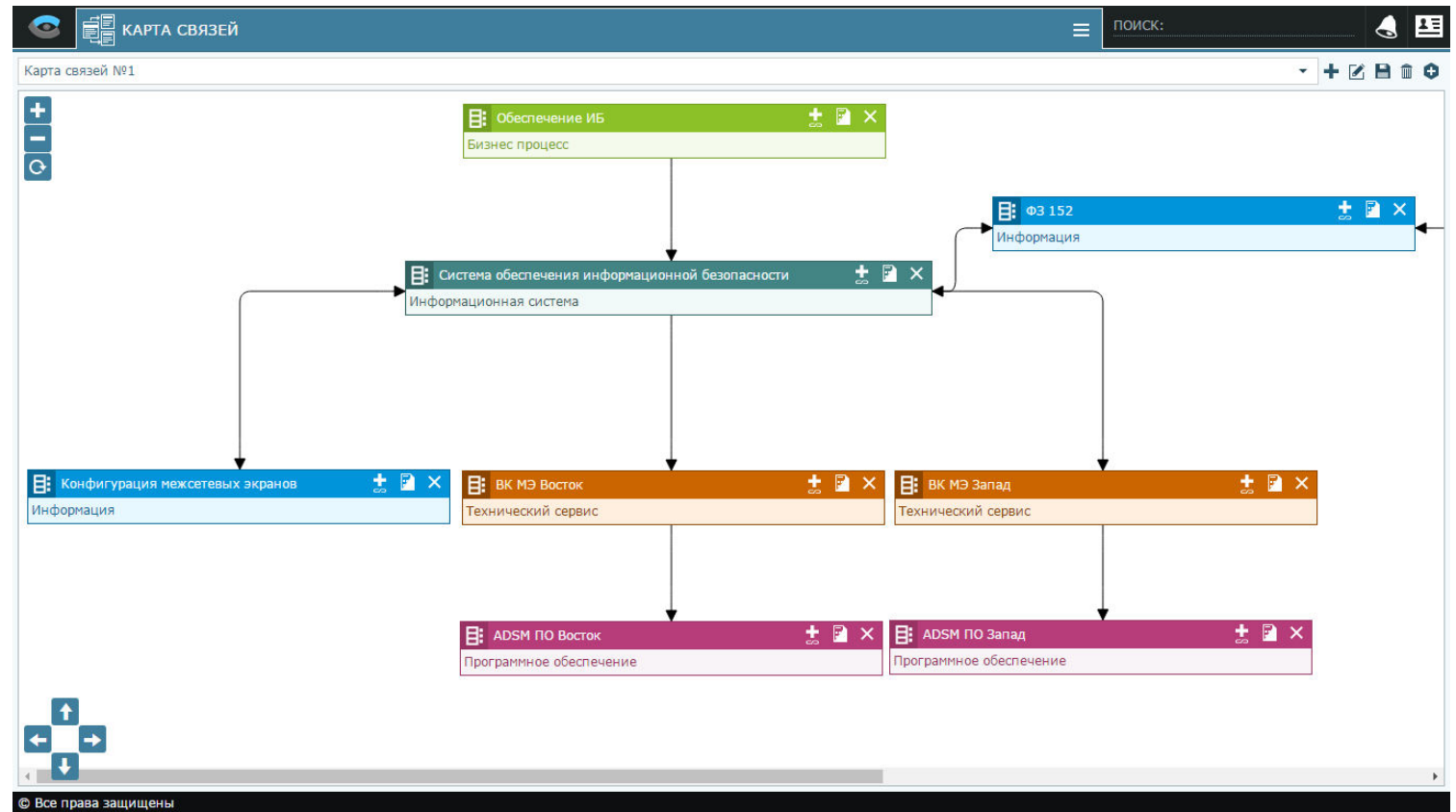
© Все права защищены

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.



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.

МАТРИЦА УПРАВЛЕНИЯ РИСКАМИ

ПОИСК: _____

Ценность актива	Вероятность угрозы								
	L (Низкая)			M (Средняя)			H (Высокая)		
	Вероятность уязвимости								
	L	M	H	L	M	H	L	M	H
0	0	0	0	1	1	1	2	3	4
1	1	2	3	2	3	4	3	4	5
2	2	3	4	3	4	5	4	5	6
3	3	4	5	4	5	6	5	6	7
4	4	5	6	5	6	7	6	7	8

Максимально допустимый уровень риска: 4

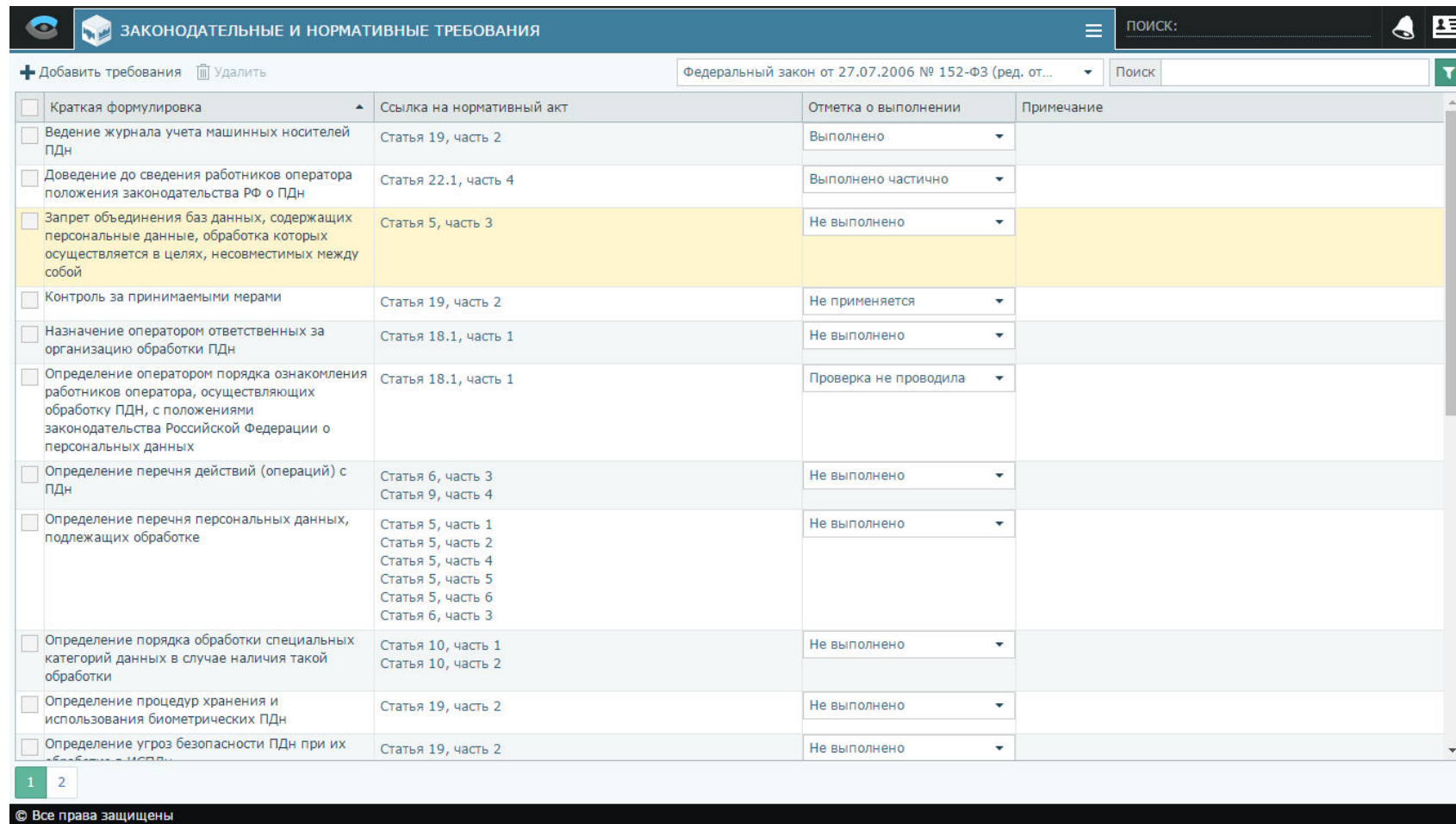
Сохранить

Значения величин рисков
1 До 25 000 руб. в год.
225 000 - 75 000 руб. в год.
375 000 - 150 000 руб. в год.
4150 000 - 1 500 000 руб. в год.
51 500 000 - 5 000 000 руб. в год.
65 000 000 - 15 000 000 руб. в год.
715 000 000 - 50 000 000 руб. в год.
8 Более 50 000 000 руб. в год.

© Все права защищены

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

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



Краткая формулировка	Ссылка на нормативный акт	Отметка о выполнении	Примечание
<input type="checkbox"/> Ведение журнала учета машинных носителей ПДн	Статья 19, часть 2	Выполнено	
<input type="checkbox"/> Доведение до сведения работников оператора положения законодательства РФ о ПДн	Статья 22.1, часть 4	Выполнено частично	
<input type="checkbox"/> Запрет объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой	Статья 5, часть 3	Не выполнено	
<input type="checkbox"/> Контроль за принимаемыми мерами	Статья 19, часть 2	Не применяется	
<input type="checkbox"/> Назначение оператором ответственных за организацию обработки ПДн	Статья 18.1, часть 1	Не выполнено	
<input type="checkbox"/> Определение оператором порядка ознакомления работников оператора, осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о персональных данных	Статья 18.1, часть 1	Проверка не проводила	
<input type="checkbox"/> Определение перечня действий (операций) с ПДн	Статья 6, часть 3 Статья 9, часть 4	Не выполнено	
<input type="checkbox"/> Определение перечня персональных данных, подлежащих обработке	Статья 5, часть 1 Статья 5, часть 2 Статья 5, часть 4 Статья 5, часть 5 Статья 5, часть 6 Статья 6, часть 3	Не выполнено	
<input type="checkbox"/> Определение порядка обработки специальных категорий данных в случае наличия такой обработки	Статья 10, часть 1 Статья 10, часть 2	Не выполнено	
<input type="checkbox"/> Определение процедур хранения и использования биометрических ПДн	Статья 19, часть 2	Не выполнено	
<input type="checkbox"/> Определение угроз безопасности ПДн при их обработке ИСПДн	Статья 19, часть 2	Не выполнено	

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

The screenshot displays a web-based incident management system. The main window is titled "ПЕРЕЧЕНЬ ИНЦИДЕНТОВ" (List of Incidents) and contains a table of incidents. A modal window titled "Инцидент - Нарушение доступности в результате ошибки пользователя" (Incident - Availability violation due to user error) is open, showing the "Решение" (Solution) tab. The solution applied is "Ложное срабатывание" (False alarm), with a "Ложноположительный результат" (False positive result) noted. The background table lists incidents with columns for ID, creation time, status, and a detailed description of the incident and its resolution.

ID	Время создания	Статус	Описание инцидента	Причина	Система	Модуль	Исполнитель	Срок обработки
32190	19.09.2016, 9:16:28	Новый						21.09.2016, 9:16:28
32189	15.09.2016, 11:14:01	Новый					Лев Львович, Романович	17.09.2016, 11:14:01
32188	15.09.2016, 11:14:01	Новый					Лев Львович, Романович	17.09.2016, 11:14:01
32187	15.09.2016, 11:14:00	Новый					Лев Львович, Романович	17.09.2016, 11:14:00
32186	15.09.2016, 11:14:00	Новый	Нарушение температурного режима	Сбой/поломка устройства или ПО	Система технической защиты	Второй модуль комплексной системы	Старшемаркетолог Лев Львович, Сетевской Роман Романович	17.09.2016, 11:14:00
32185	15.09.2016, 11:13:59	Новый	Зависание	Прочие ошибки	Прочие ошибки	Первый модуль комплексной системы	Старшемаркетолог Лев Львович, Сетевской Роман Романович	17.09.2016, 11:13:59
32184	15.09.2016, 11:13:59	Новый	Попытка модификации конфигурации базы данных с удаленного узла	Модификация узла	Ошибки или нарушения модификации объектов БД	ПК СПВ Надтер, ЗК МЭ Центр		17.09.2016, 11:13:59
32183	15.09.2016, 11:13:58	Решён	На контролируемом устройстве в контролируемой сети	Модификация настроек сетевого	Модификация настроек сетевого устройства	ПК СПВ Архангельск,	Старшемаркетолог Лев Львович, Сетевской Роман Романович	17.09.2016, 11:13:58

Управление осведомленностью

Система управления осведомленностью позволяет:

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

The screenshot displays the Security Vision 3.3 interface. The top navigation bar includes icons for various modules: СОСТОЯНИЕ, АКТИВЫ, ИНЦИДЕНТЫ, КАРТА, РИСКИ, АГЕНТЫ, ДОКУМЕНТЫ, ОТЧЕТЫ, and НАСТРОЙКИ. The main content area is titled 'Перечень отчетов \ Оседамленность \ Обучение' and shows a tree view on the left with categories like 'СТАНДАРТНЫЙ ОБУЧАЮЩИЙ МАТЕРИАЛ' and 'ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ'. The right side features a table with columns for 'Название', 'Целевая группа', and 'Результат'. The table lists training items such as 'Основы ИБ на рабочем месте сотрудника' and 'Обеспечение конфиденциальности персональных данных', with their respective target groups and completion statuses.

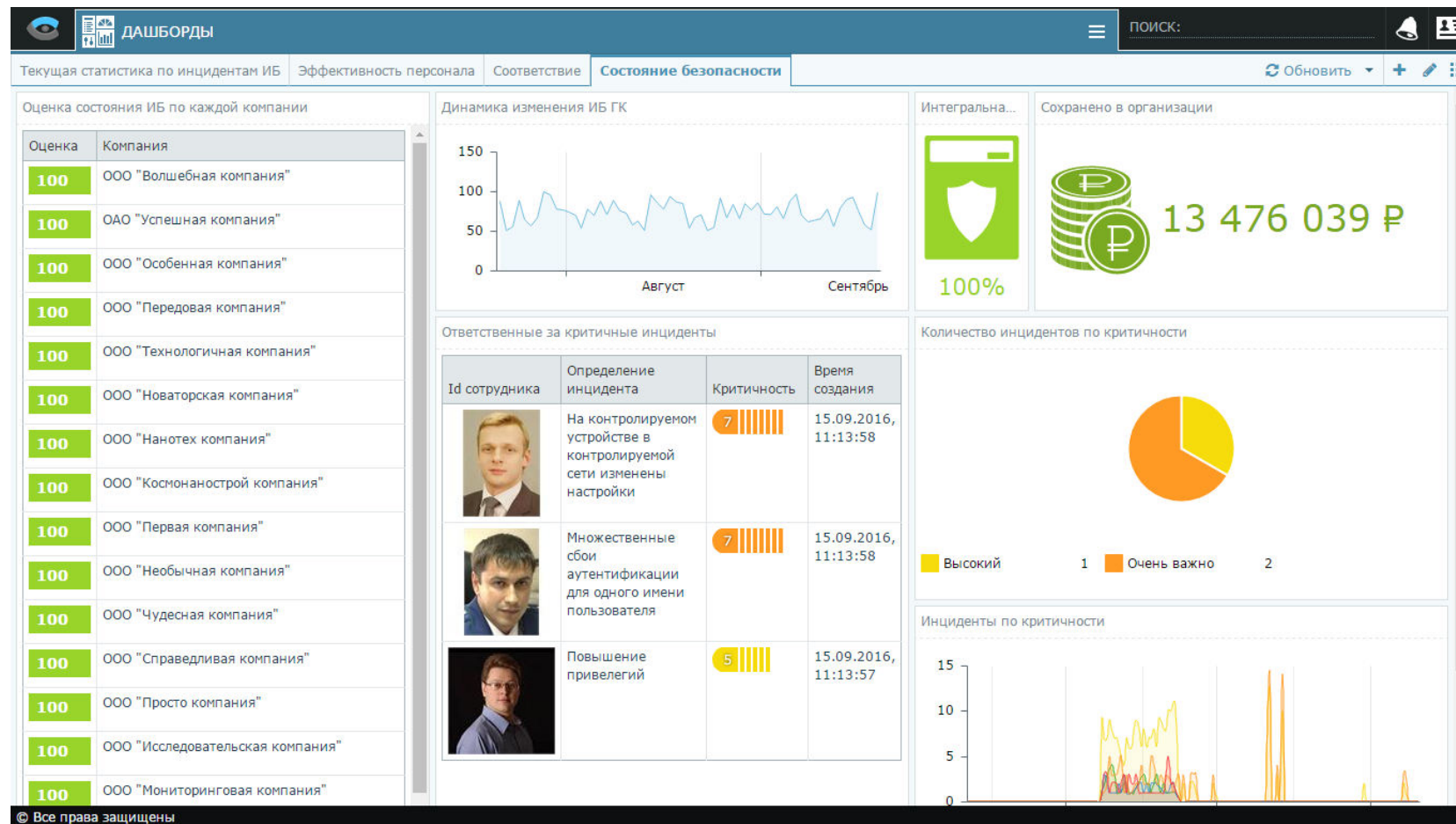
Название	Целевая группа	Результат
Основы ИБ на рабочем месте сотрудника	Головное ОСБ	В процессе выполнения Выполнено : 78%
Обеспечение конфиденциальности персональных данных	Кадровая служба Служба по работе с клиентами	Выполнено
Администрирование серверов под управлением ОС Windows	Берелев С.А. Переплывкин В.И.	Выполнено

At the bottom of the interface, there is a button labeled 'НАЗНАЧИТЬ ОБУЧЕНИЕ' and a page indicator showing 'Страница 1 из 1'.

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



Развитие отделов ИБ

Текущий уровень	Переход	Точки роста
0. ИБ отсутствует	0 → 1	<ul style="list-style-type: none"> ✓ Назначить ответственного за ИБ сотрудника; ✓ Начать с решения самых горящих ИБ вопросов
1. Работаем на операционном уровне (тушим пожары)	1 → 2	<ul style="list-style-type: none"> ✓ Посоветоваться с «коллегами по цеху» (другими директорами ИБ) о дальнейшем развитии ИБ; ✓ Запланировать ИБ проекты на ближайшую перспективу и реализовать их.
2. Работаем на тактическом уровне (среднесрочное планирование)	2 → 3 СУАИБ ISOC	<ul style="list-style-type: none"> ✓ Войти в контакт с советом директоров по вопросам ИБ; ✓ Разработать и выполнять стратегию ИБ; ✓ Произвести дизайн процессов ИБ, управлять процессами ИБ; ✓ Начать управлять рисками ИБ.
3. Работаем на стратегическом уровне (долгосрочное планирование)	3 → 4	<ul style="list-style-type: none"> ✓ Повышать эффективность управления ИБ; ✓ Автоматизировать все, что целесообразно автоматизировать; ✓ Повышать осведомленность (собственную, подчиненных, всех сотрудников организации) в области ИБ.



Контакты



Федор Горловский

Директор по развитию бизнеса

fg@securityvision.ru

М: +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.