www.skc.ru

СКЦ РОСАТОМА

Информационная безопасность распределенной системы мониторинга. Практический опыт

Москва, МГУ
16.05.2019

Заместитель директора ФГУП «СКЦ Росатома»
Смирнов С.Н., д.т.н., профессор

Структура предметной области и объекта оценки

Структура предметной области обеспечения информационной безопасности объектов мониторинга

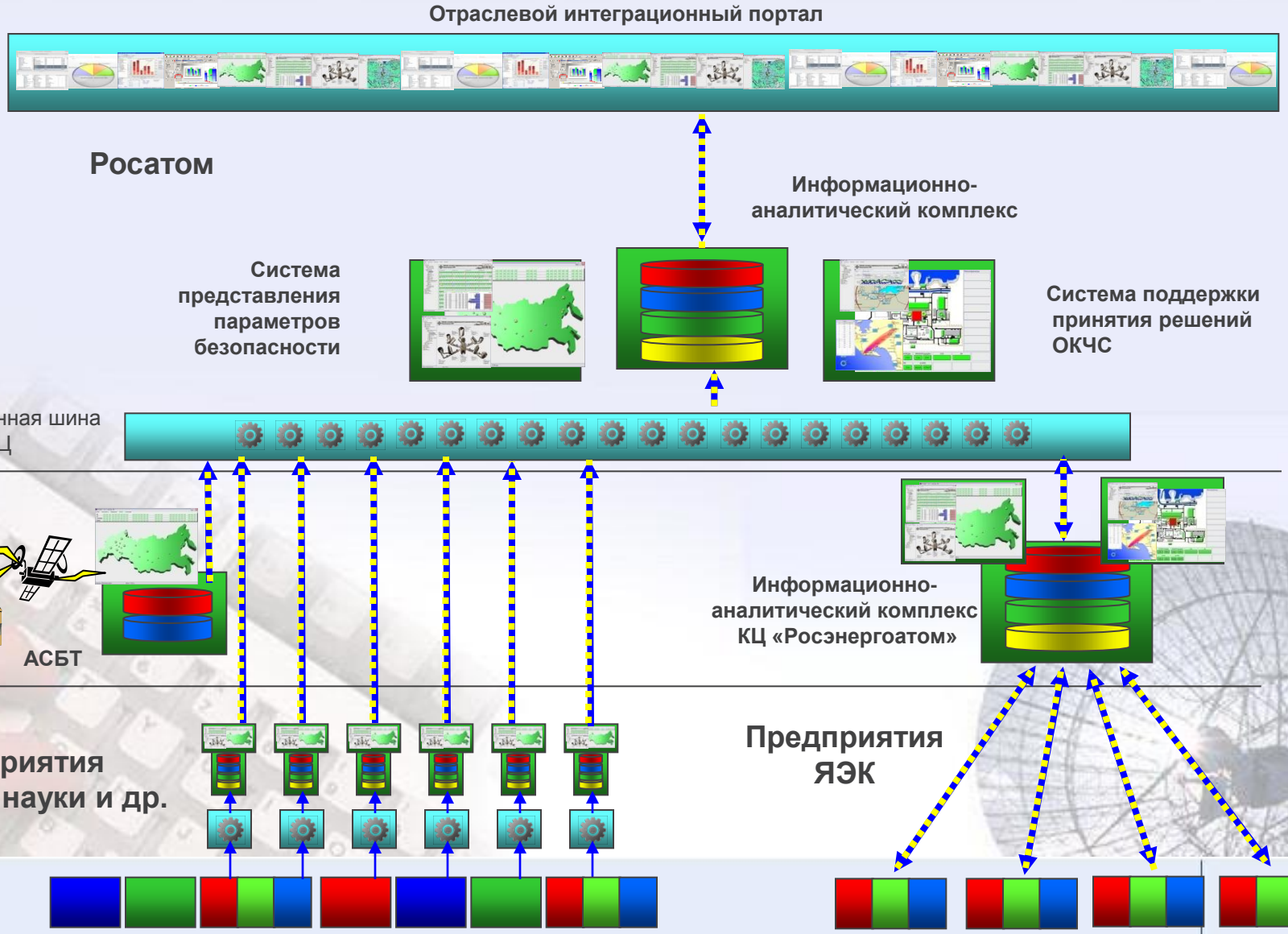
1. **Проектирование и строительство объектов использования атомной энергии.**
2. **Обеспечение функционирования объектов использования атомной энергии, включая обеспечение физической защиты.**
3. **Непрерывный мониторинг состояния объектов использования атомной энергии.**

Структура объекта оценки

1. **Технологии оперативного контроля состояния объектов использования атомной энергии оперативно-диспетчерскими службами Госкорпорации «Росатом».**
2. **Автоматизированные системы мониторинга объектов использования атомной энергии (телеметрия).**

Информационные потоки системы мониторинга объектов использования атомной энергии

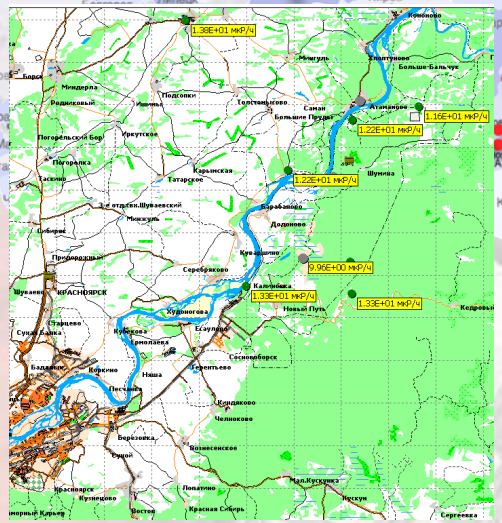
СКЦ РОСАТОМА



Особенности развития автоматизированных систем мониторинга объектов использования атомной энергии

СКЦ РОСАТОМА

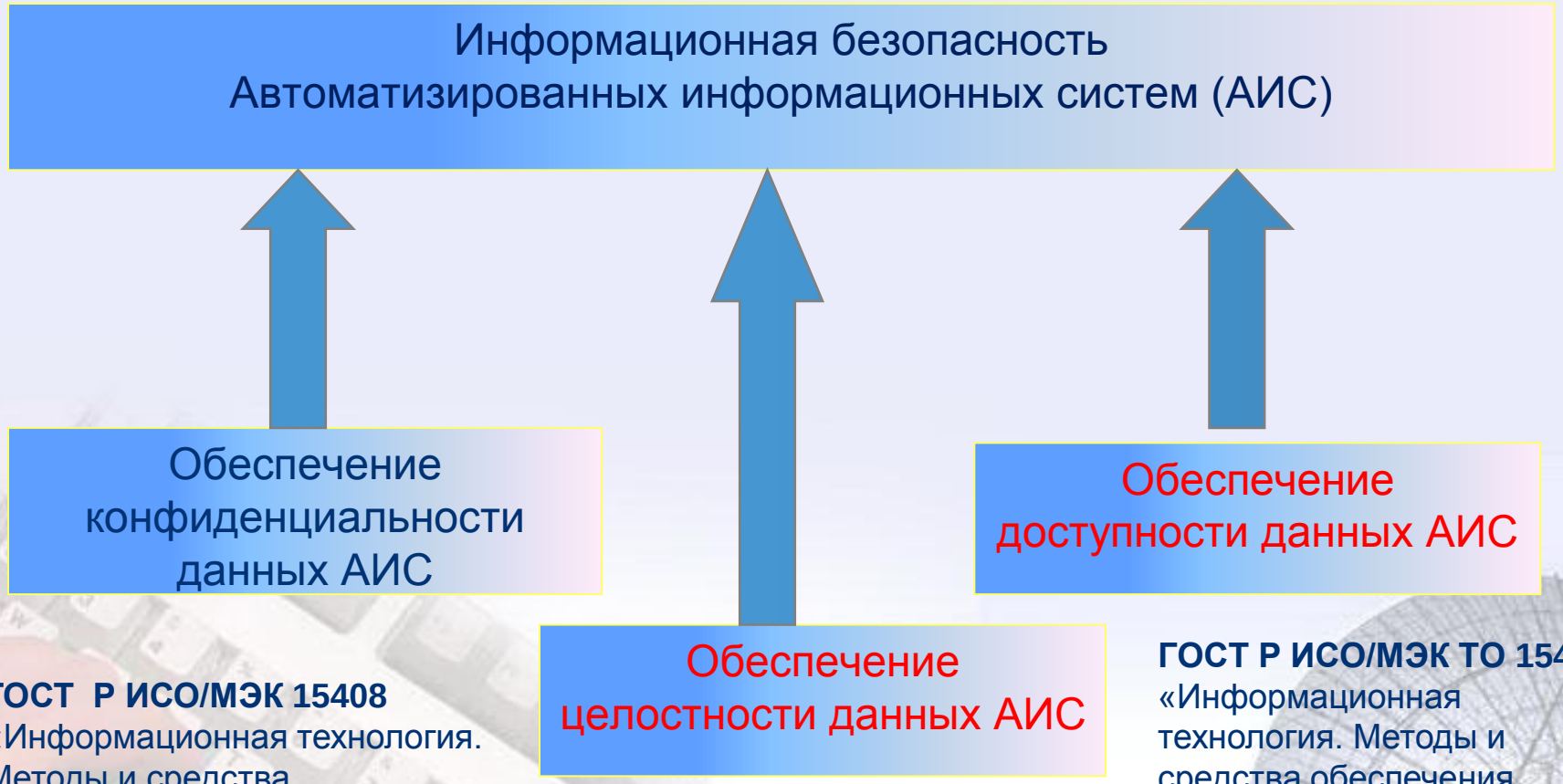
Цель: постоянный доступ уполномоченных руководителей Корпорации и экспертов к объективной информации о состоянии безопасности объектов использования ядерной энергии, выполнение законодательно закрепленных функций по информированию населения.



1. Расширение спектра и объема контролируемых параметров на существующих объектах мониторинга.
2. Интеграция с государственной системой ЕГАСМРО и системами МАГАТЭ.
3. Совершенствование средств обеспечения информационной безопасности.

www.rosatom.ru
www.russianatom.ru
www.skc.ru

Компоненты информационной безопасности АИС СКЦ Росатома



ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий».

ГОСТ Р ИСО/МЭК ТО 15446 «Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности».

Совершенствование средств доставки информации с объектов мониторинга

СКЦ РОСАТОМА

Объективные предпосылки:

- **развитие сетей беспроводной связи;**
- **«интернет вещей» - интеллектуализация и встроенные средства связи в приборы и технические средства повседневного использования.**

Прогноз развития средств доставки:

- Снижение стоимости использования коммерческих беспроводных сетей до приемлемого уровня (виртуальные каналы доставки).
- эффективность в условиях низких скоростей, отказоустойчивость, адаптивность, возможность самоорганизации.
- IPv6 как основа индивидуализации средства получения исходных данных.
- Новые типы мобильных средств измерения (измерения, обеспечивающие преобразование сведений о состоянии внешней среды в машиночитаемые данные, миниатюризация, энергосбережение).

Совершенствование средств обеспечения информационной безопасности (часть 1)

СКЦ РОСАТОМА

Объективные предпосылки:

- **переход от этапа информационного противоборства к информационной войне (warfare);**
- **использование кибероружия, направленного против объектов энергетики, в первую очередь, атомной.**

Помимо Stuxnet (Иран, Натанзе, 2010), Duqu (2011) и Flame (2012) задокументировано не менее 1500 случаев заражения в тридцати странах, с эпицентрами в России, Китае, Иране и Индии.

Современная библиотека инструментов кибераграссии включает:
средства разведки (Fanny), средства доставки (DoubleFantasy), средства контроля операционной системы (Grayfish)…

Stuxnet был разработан в рамках секретного проекта Olympic Games совместно Агентством Национальной Безопасности и Федеральным Бюро Расследований США, при содействии израильской Unit 8200 (подразделение национальной разведывательной службы).
Дэвид Сангер. «The New York Times, май 2012»

«Сегодняшний инструмент спецслужб завтра становится предметом диссертаций, а послезавтра переходит в распоряжение рядовых злоумышленников».
Брюс Шнайер.

Структура угроз объекту оценки

СКЦ РОСАТОМА

Источники угроз:
антропогенные;
технические и технологические;
природные.

Идентифицированный источник угрозы

- Уровень возможностей
- Доступные ресурсы
- Мотивация

Характеристика нападения

- Условия реализуемости нападения
- Метод нападения
- Используемые уязвимости

Атакуемый актив

Модель угроз
Модель нарушителя

Создание «периметра безопасности»

СКЦ РОСАТОМА

Реализованный ФГУП «СКЦ Росатома» комплекс технических средств обеспечения информационной безопасности информационно-коммуникационной системы мониторинга (ИКС ЯРБ) включает:

- применение межсетевых экранов (Cisco PIX Firewall) и выделение зон безопасности;
- использование протоколов безопасной передачи данных (ViPNet);
- контроль всего входящего трафика с помощью детекторов вторжений (Cisco Intrusion Detection System), разделение его с помощью виртуальных сетей (VLAN), построенных с использованием коммутаторов Cisco;
- использование корпоративной защищенной электронной почтовой системы на базе сертифицированных средств «ViPNet» для организации обмена конфиденциальной информацией между пользователями Госкорпорации «Росатом» и предприятиями отрасли;
- постоянный централизованный антивирусный мониторинг в ИКС ЯРБ и на персональных компьютерах пользователей;
- применение средств защиты информации от утечки по техническим каналам за счет различных физических полей;
- использование изолированной кабельной системы для управления средствами ИКС ЯРБ, систем электропитания и заземления, находящихся на территории Госкорпорации «Росатом».

Разработка профиля защиты и задания по безопасности объекта оценки на основе ГОСТ Р ИСО/МЭК ТО 15446

СКЦ РОСАТОМА

U. S. Government Protection Profile for Database Management Systems, version 1.3, December 2010.

- **Введение ПЗ**
- Идентификация ПЗ
- Аннотация ПЗ

2. Описание объекта оценки

3. Среда безопасности ОО
- Предположения безопасности
- Угрозы
- Политика безопасности организации

4. Цели безопасности
- Цели безопасности для ОО
- Цели безопасности для среды

5. Требования безопасности ИТ

Требования безопасности для среды ИТ

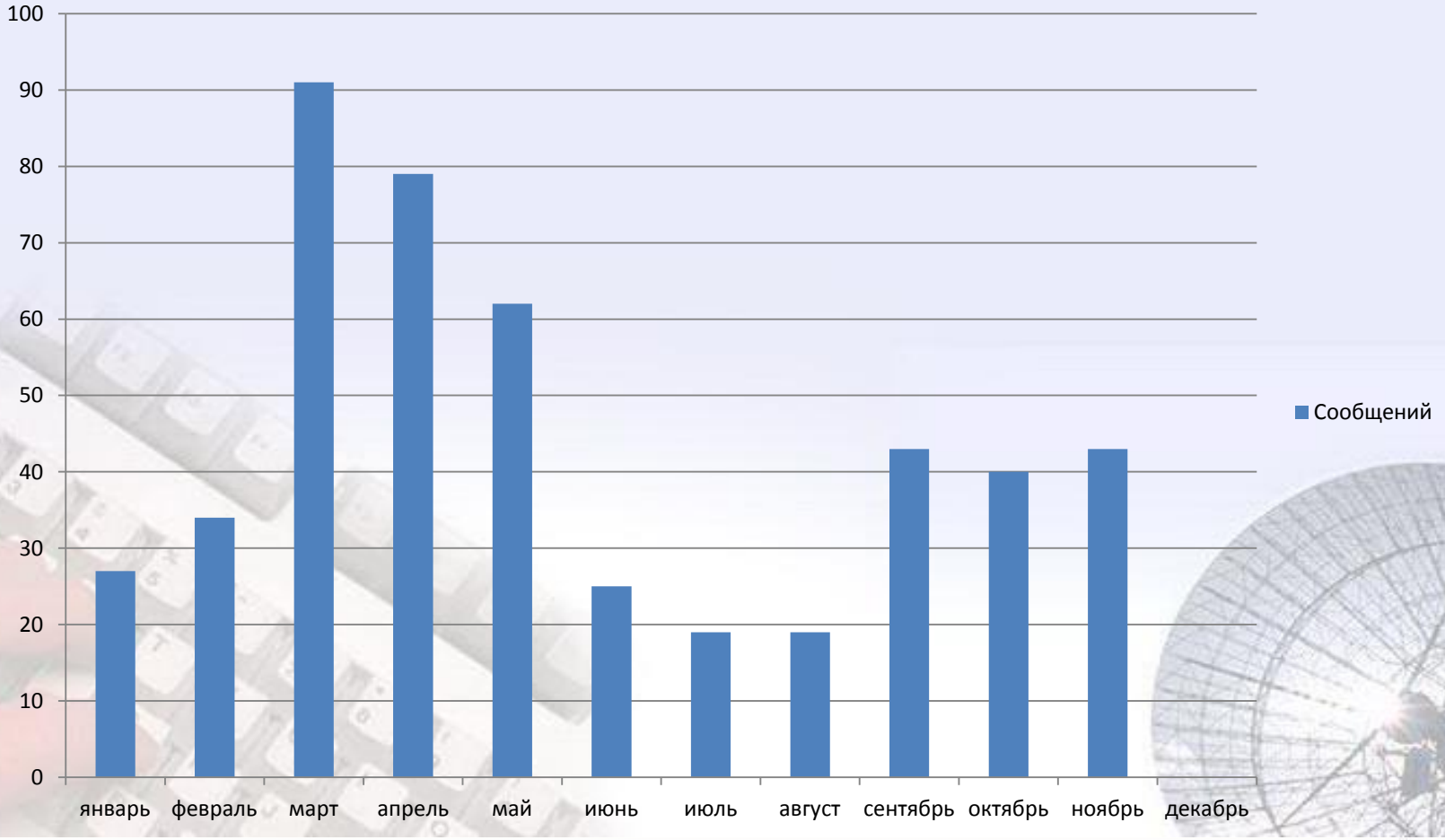
Требования безопасности для ОО
- Функциональные требования безопасности ОО
- Требования доверия к безопасности

6. Обоснование
- Обоснование целей безопасности
- Обоснование требований безопасности

Статистика попыток нарушений информационной безопасности инфраструктуры СКЦ Росатома (часть 1)

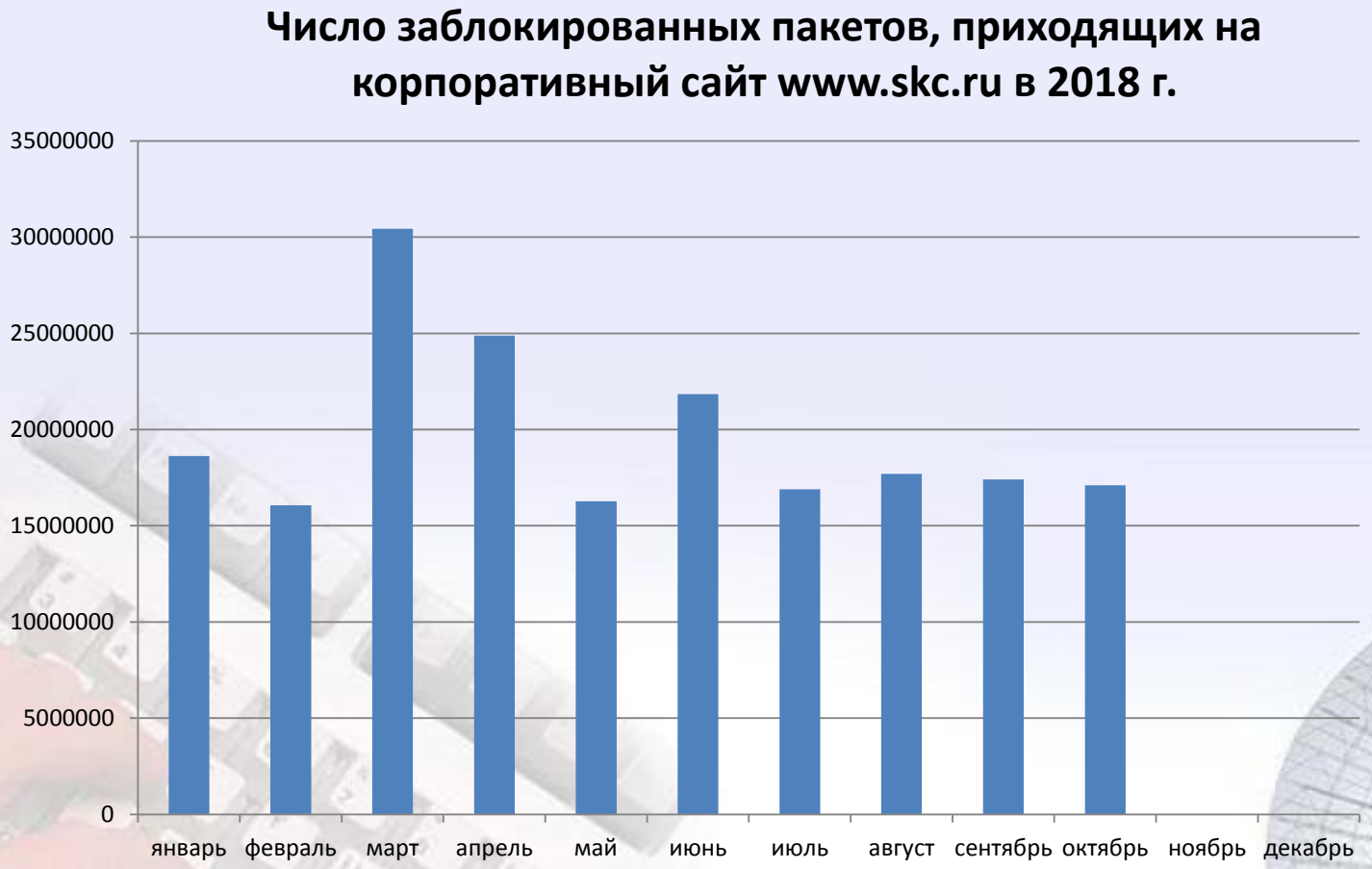
СКЦ РОСАТОМА

Число «вредоносных» сообщений, выявленных в корпоративной почте 2018 г.



Статистика попыток нарушений информационной безопасности инфраструктуры СКЦ Росатома (часть 2)

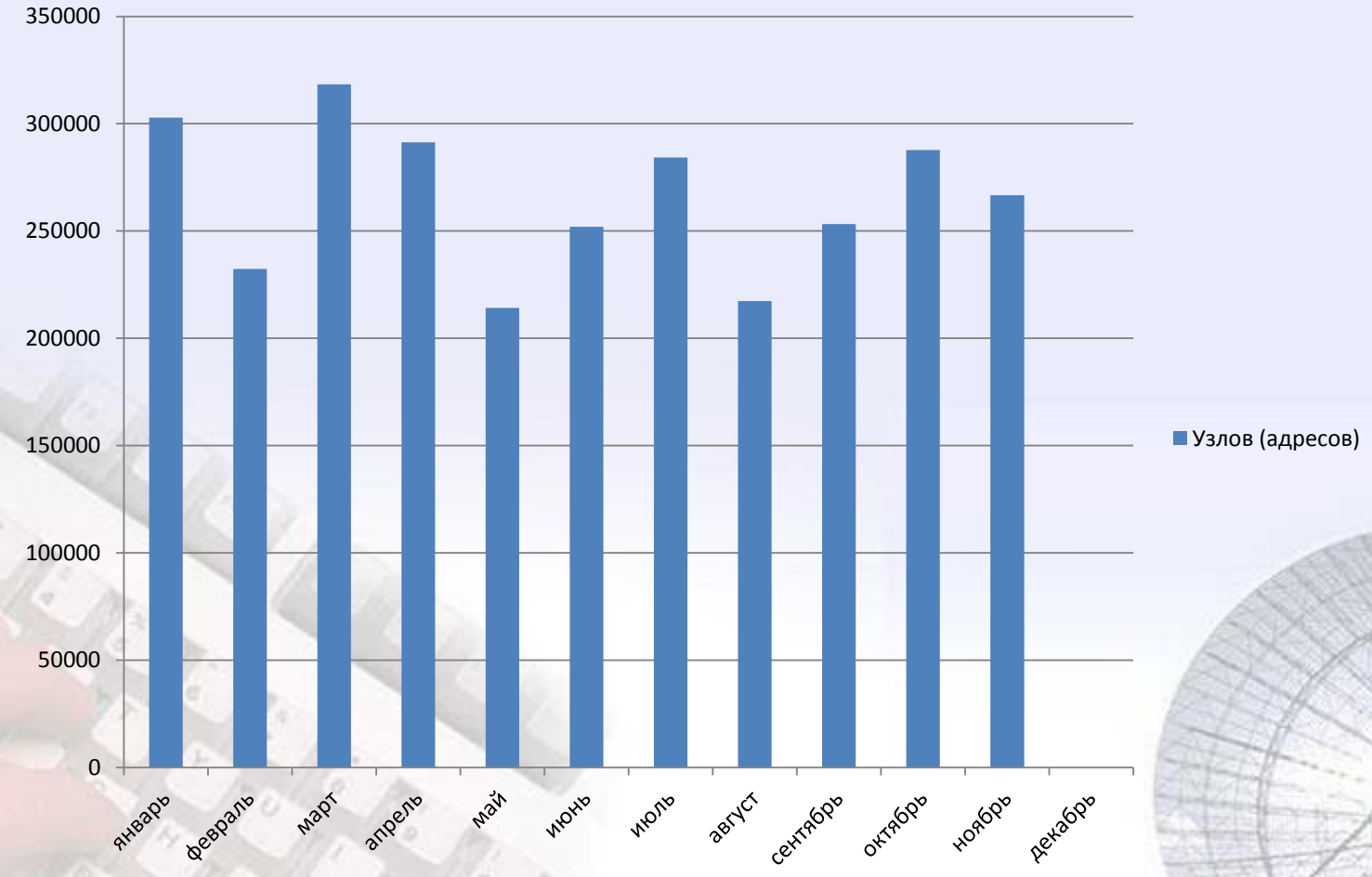
СКЦ РОСАТОМА



Статистика попыток нарушений информационной безопасности инфраструктуры СКЦ Росатома (часть 3)

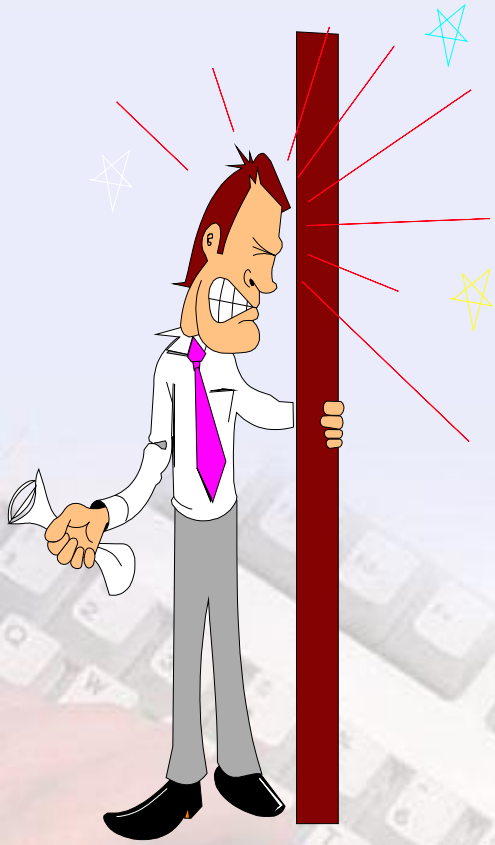
СКЦ РОСАТОМА

Число «атакующих» корпоративный сайт www.skc.ru узлов сети Интернет в 2018 г.



Направления развития средств обеспечения информационной безопасности в области мониторинга

СКЦ РОСАТОМА



Направления развития средств обеспечения информационной безопасности распределенной системы мониторинга:

- Тотальное применение криптографических средств защиты информации отечественной разработки от систем измерения до систем отображения информации с целью обеспечения конфиденциальности и целостности данных.
- Разработка и применение новых технологий обеспечения доступности информации на основе создания виртуальных каналов доставки, построенных на альтернативных системах передачи данных.

Доклад закончен.
Спасибо за внимание.

СКЦ РОСАТОМА

Смирнов Сергей Николаевич ssmirnov@skc.ru
+7(495) 933-60-40 доб. 10-05