



kaspersky



Kaspersky Industrial
Cybersecurity
Conference 2020

Константин Сахаров

Руководитель управления
информационной и компьютерной
безопасности АСУ ТП, АО «Русатом
автоматизированные системы управления»

#KasperskyICS

Чат конференции: <https://kas.pr/kicscon>




RASU
ROSATOM

Обеспечение информационной и компьютерной безопасности АСУ ТП АЭС

Константин Сахаров

- **АО РАСУ**
- **Терминология**
- **Стандарты и рекомендации**
- **Основные подходы**
- **Сертификация**
- **Инвестиционные проекты**

АО «Русатом Автоматизированные системы управления»

A decorative graphic consisting of numerous thin, white, curved lines that originate from a point on the right side of the image and fan out towards the left, creating a sense of motion and depth against the solid blue background.

Текущие проекты
25+ ЭБ АЭС

Системный интегратор и поставщик
АСУ ТП и
электрооборудования

Свыше **550** высококвалифицированных
специалистов и **350** инженеров

Свыше **2 300** работников во всем бизнесе
АСУ ТП (включая бизнес-подразделения),

Свыше **30** предприятий

Свыше **70** блоков АЭС оборудованы АСУ ТП
разработки РФ



СИСТЕМНЫЙ ИНТЕГРАТОР И ПОСТАВЩИК АСУ ТП И ЭЛЕКТРООБОРУДОВАНИЯ



RASU
ROSATOM

АО РАСУ – внедрение проектных решений на всех этапах собственными силами и экспертизой в интеграции и кооперации с зарубежными вендорами


- Системная интеграция
- Проектирование
- Управление проектами
- Управление поставщиками
- Метрология
- Сервисное сопровождение


Системы безопасности
Разработка, Производство и Тестирование


Системы НЭ и Электрооборудование
Разработка, Производство и Тестирование


- Инжиниринг
- Производство
- Тестирование
- Разработка

- Инжиниринг
- Производство
- Тестирование
- Разработка

 **Поставка компаниями Росатома**

 **Поставка другими компаниями**

 **Поставка компаниями Росатома**

 **Поставка другими компаниями**

ТЕКУЩИЕ ПРОЕКТЫ АЭС



Венгрия
Пакш-2 АЭС



Бангладеш
Руппур АЭС



Финляндия
Ханхикиви АЭС



Турция
Аккую АЭС



Индия
Кунадкулам АЭС



Египет
Эль-Дабаа АЭС

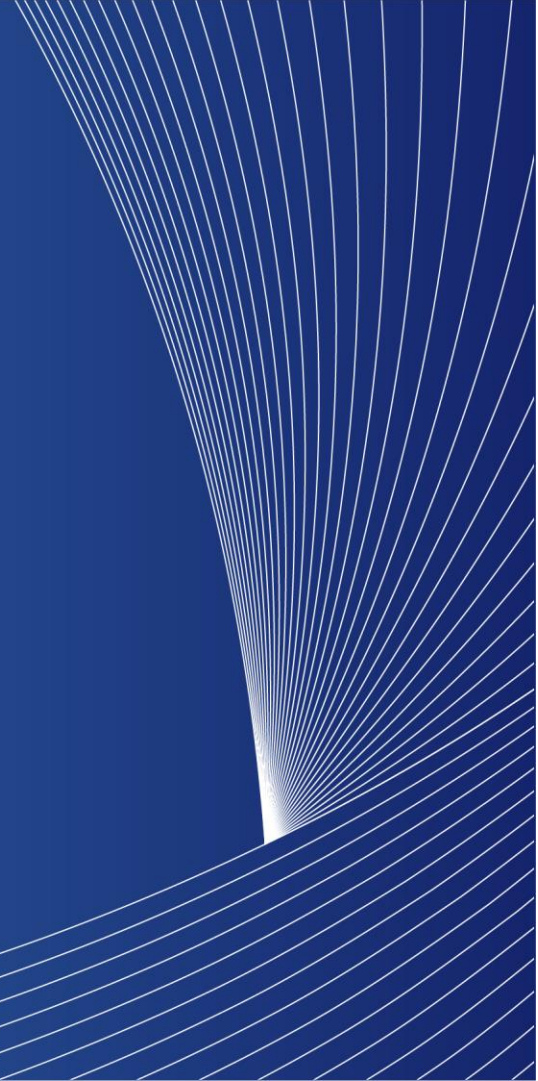
● ○ Международные активности в части КБ



IAEA



Терминология



12,5 %

- **Информационная безопасность (ISO/IEC 27000)** – сохранение **конфиденциальности, целостности и доступности** информации.

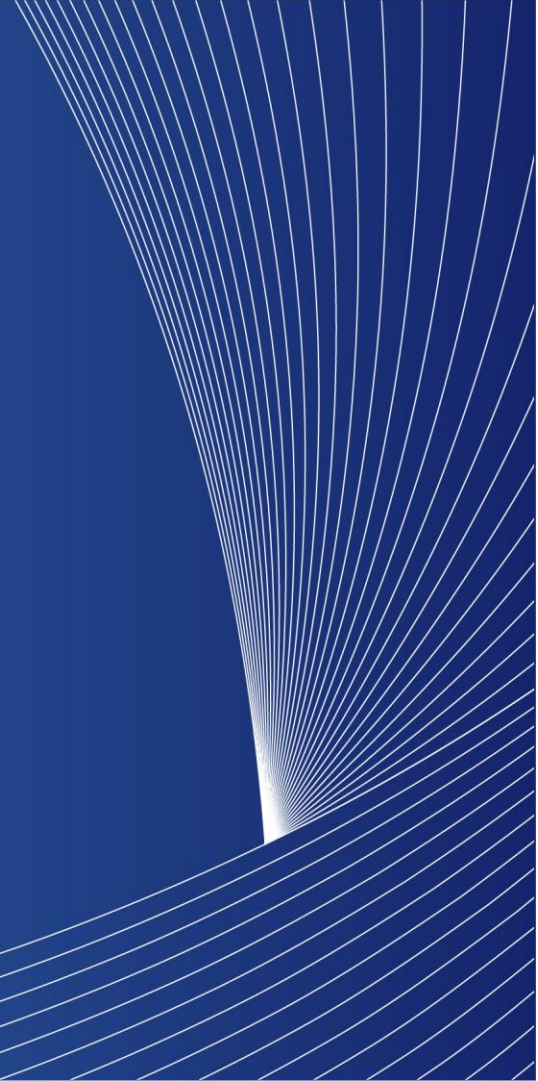
75 %

- **Кибербезопасность (IEC 62645)** – комплекс мероприятий и мер, целью которых является **предотвращение, выявление и реагирование на:**
 - злонамеренные модификации (**целостность**) функций, которые могут поставить под угрозу передачу или целостность требуемого сервиса программируемыми цифровыми **СКУ** (включая потерю управления), что может привести к аварии, небезопасной ситуации или снижению производительности;
 - злонамеренное сокрытие или предотвращение доступа к информации, данным или ресурсам (включая потерю контроля) которые могут привести к нарушению **доступности** сервисов **СКУ**, которые могут привести к аварии, небезопасной ситуации или снижению производительности;
 - злонамеренное раскрытие информации (**конфиденциальности**), которая может быть использована для выполнения злонамеренные действия, которые могут привести к аварии, небезопасной ситуации или снижению производительности.

12,5 %


- **Компьютерная безопасность (NSS 17)** – это специфический аспект информационной безопасности, относящийся к компьютерным системам, сетям и цифровым системам.

Стандарты и рекомендации



- **IAEA NSS 17 - Computer Security at Nuclear Facilities**
- **IAEA NSS 33-T - Computer Security of Instrumentation and Control Systems at Nuclear Facilities**
- **IEC/ISO 27001 - Information technology — Security techniques — Information security management systems — Requirements**
- **IEC/ISO 27002 - Information technology — Security techniques — Code of practice for information security controls**
- **IEC 62645 - Nuclear power plants - Instrumentation, control and electrical power systems - Cybersecurity requirements**
- **IEC 62859 - Nuclear power plants - Instrumentation and control systems - Requirements for coordinating safety and cybersecurity**
- **Внутренние законодательные акты и НТД**

Основные подходы к обеспечению ИИБ АСУ ТП АЭС

A decorative graphic consisting of numerous thin, white, curved lines that originate from a point on the right side of the image and fan out towards the top right corner, creating a sense of motion and depth against the solid blue background.

🎯 Основные требования КБ к ПТС



Обеспечивать целостность, доступность и, при необходимости, конфиденциальность



Не оказывать значимого негативного влияние на АСУ ТП

● Основные требования КБ к ПТС



Быть совместимыми с промышленными, физическими, пожарными, радиационными и иными мерами безопасности



Быть совместимыми с ПА средствами АСУ ТП



Риск-ориентированный и дифференцированный подход



Источники рисков



Угрозы



Вероятности

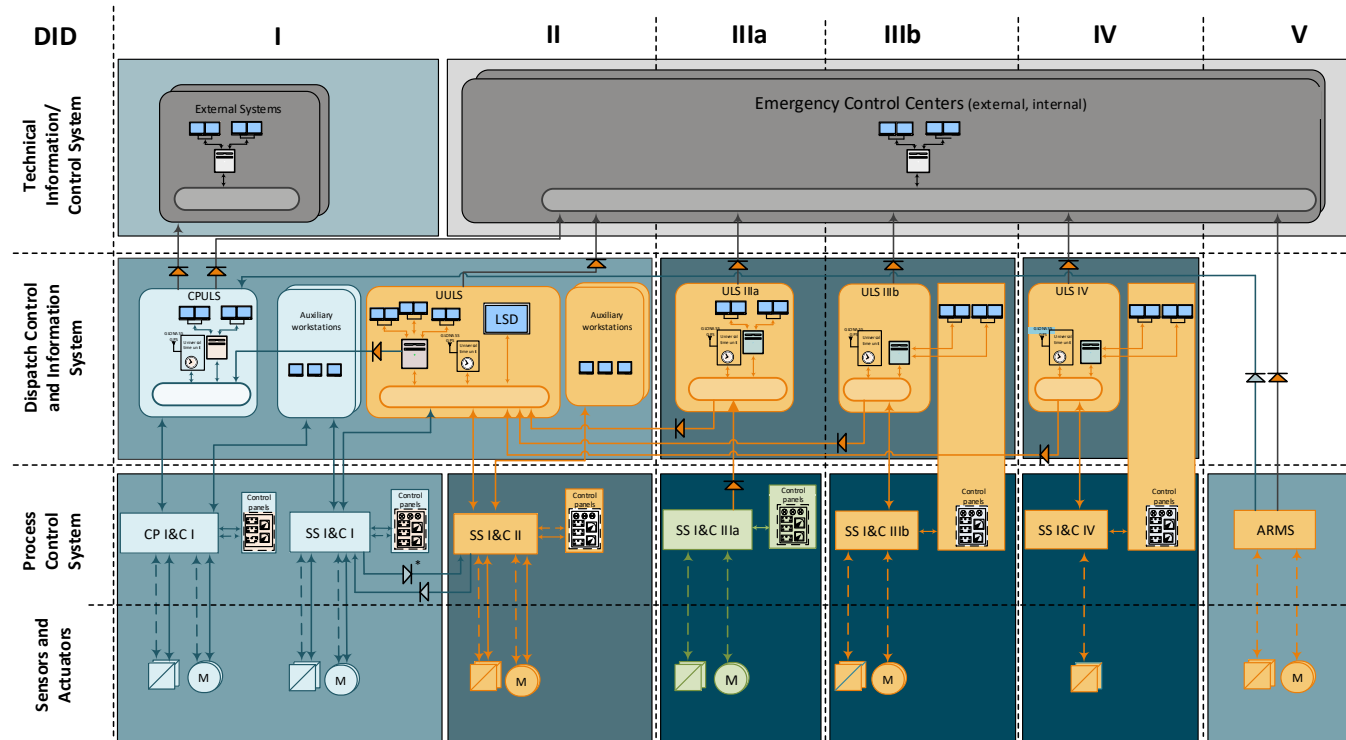
Уровень защиты

=

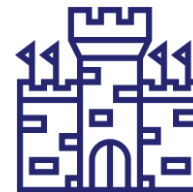
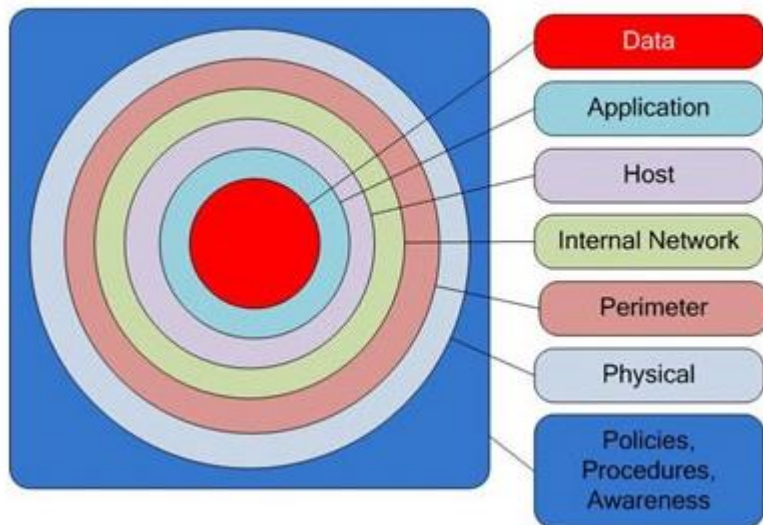
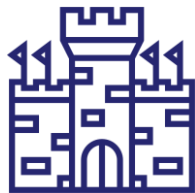
Уровень риска

Оценка риска

Зональный подход



Defense in Depth Layers





- **Физическая защита**

Рассматривается частично





- Политики, планы, программы, процедуры

Последовательный подход



- Исходные данные: ЕРС-контракт, рекомендации МАГАТЭ, стандарты МЭК
- Политика, План, Программа, Процедуры АСУ ТП
- Политика, План, Программа, Процедуры подсистем АСУ ТП



- **Защита периметра и сети**



Промышленная СОВ



МЭ



Диод Данных



- **Защита хостов, приложений и данных**

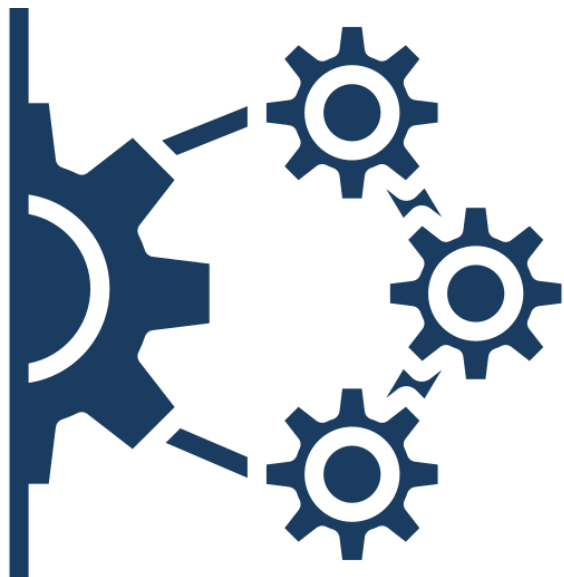


ОС



Антивирус

● Комплексный подход



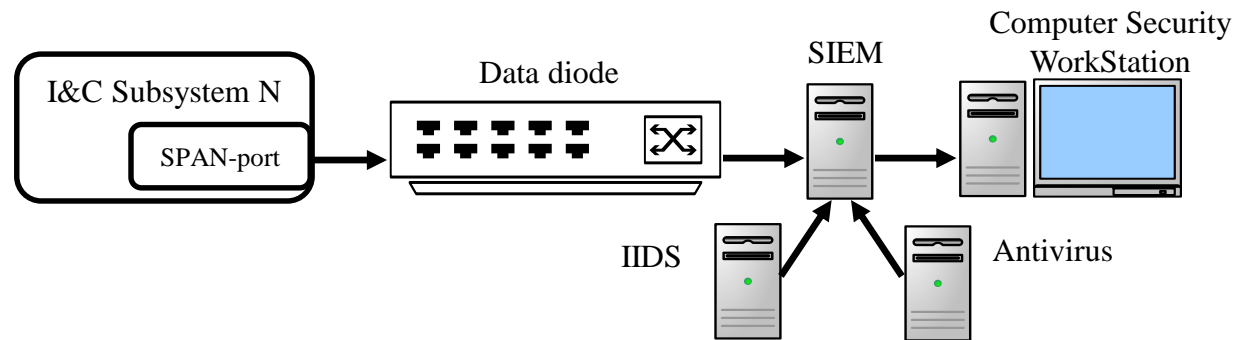
SIEM АСУ ТП



Аккумуляция и хранение логов от различных источников: сетевые устройства, приложения, ОС, СЗИ



- Исключение распространения отказов к АСУ ТП



• Разнообразие



Разные производители

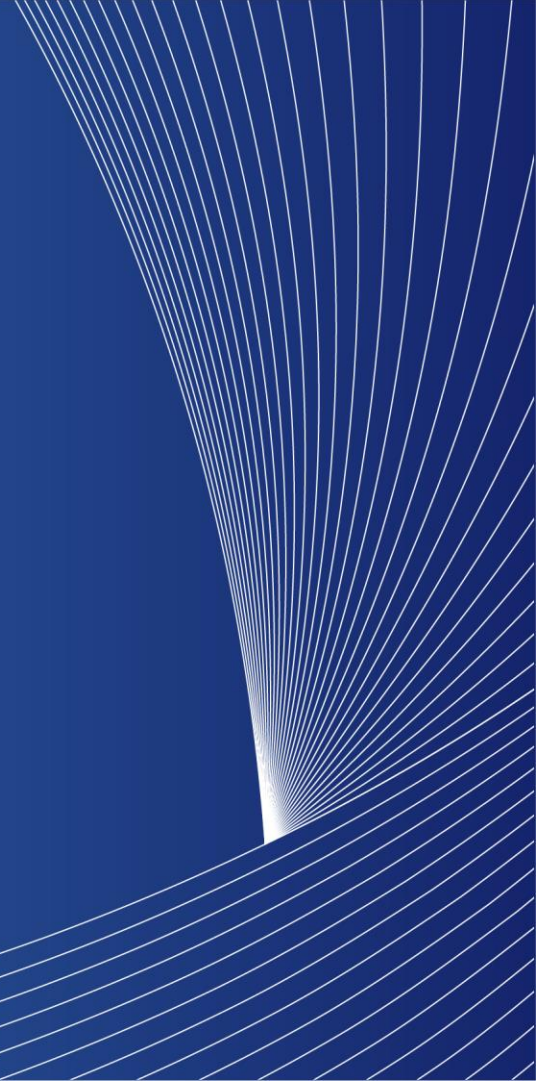


Разные принципы и алгоритмы



Разные БД угроз

Сертификация





- ФСТЭК России
- ✓ Ограниченный выбор сертифицированных СЗИ

Документы по сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации

Создано: 31 Января 2013 15:14 | Обновлено: 07 Августа 2020 15:35 | Просмотров: 514182

Государственный реестр сертифицированных средств защиты информации

Реестр / перечень / список

Оценить:  + 246  - 95

005 Государственный реестр сертифицированных средств защиты информации 212 КБ 533128

Текст для поиска

10

№ сертификата	Дата внесения в реестр	Срок действия сертификата	Наименование средства (шифр)	Наименования документов, требованиям которых соответствует средство	Схема сертификации	Испытательная лаборатория	Орган по сертификации	Заявитель	Реквизиты заявителя (индекс, адрес, телефон)	Информация об окончании срока технической поддержки, полученная от заявителя
---------------	------------------------	---------------------------	------------------------------	---	--------------------	---------------------------	-----------------------	-----------	--	--

- Common Criteria (ISO/IEC 15408)
- ✓ Сертифицированных СЗИ крайне мало

Certified Products [Statistics](#) [Download CSV](#) [Archived Certified Products](#)

The Common Criteria Recognition Arrangement covers certificates with claims of compliance against Common Criteria assurance components of either:

1. a collaborative Protection Profile (cPP), developed and maintained in accordance with CCRA Annex K, with assurance activities selected from Evaluation Assurance Levels up to and including level 4 and ALC_FLR, developed through an International Technical Community endorsed by the Management Committee; or
2. Evaluation Assurance Levels 1 through 2 and ALC_FLR.

Where a CC certificate claims compliance to Evaluation Assurance Level 3 or higher, but does not claim compliance to a collaborative Protection Profile, then for purposes of mutual recognition under the CCRA, the CC certificate should be treated as equivalent to Evaluation Assurance Level 2.

The CCDB has approved a resolution to limit the validity of mutually recognized CC certificates over time. Certificates will remain on the CPL for five years. Effective 1 June 2019, certificates with an expired validity period (that is, 5 years or more from the date of certificate issuance) will be moved to an Archive list on the CCRA portal, unless the validity period has been extended using the appropriate procedures.

[expand/collapse all categories](#)

<input type="checkbox"/> Access Control Devices and Systems – 28 Certified Products
<input type="checkbox"/> Boundary Protection Devices and Systems – 40 Certified Products
<input type="checkbox"/> Data Protection – 59 Certified Products
<input type="checkbox"/> Databases – 10 Certified Products
<input type="checkbox"/> Detection Devices and Systems – 7 Certified Products
<input type="checkbox"/> ICs, Smart Cards and Smart Card-Related Devices and Systems – 579 Certified Products

- **Сертификация платформ на соответствие IEC 62645**

IEC 62645:2019

Nuclear power plants - Instrumentation, control and electrical power systems - Cybersecurity requirements

TC 45/SC 45A | [Additional information](#)

Abstract

PREVIEW

IEC 62645:2019 establishes requirements and provides guidance for the development and management of effective computer security programmes for I&C programmable digital systems. Inherent to these requirements and guidance is the criterion that the power plant I&C programmable digital system security programme complies with the applicable country's requirements.

This document defines adequate measures for the prevention of, detection of and reaction to malicious acts by digital means (cyberattacks) on I&C programmable digital systems. This includes any unsafe situation, equipment damage or plant

[Show more »](#)

Инвестиционные проекты

A decorative graphic consisting of numerous thin, white, curved lines that originate from a single point on the right side of the image and fan out towards the left, creating a sense of motion and depth against the solid blue background.



- **Лаборатория по проверке ПО**
- **Стенд проверок КБ**
- **ПО анализа рисков**

Организация и проведение специальных испытаний для подтверждения отсутствия в ПС



Недекларированных возможностей



Уязвимостей



Программных закладок



Преднамеренных программных дефектов



Вирусов и иного вредоносного программного кода

Стенд проверок КБ



Оценка соответствия подсистем и компонентов АСУ ТП требованиям ИиКБ путем моделирования компьютерных атак на подсистемы и компоненты АСУ ТП



Оценка эффективности мер и средств защиты АСУ ТП от компьютерных атак



Моделирование и оценка последствий компьютерных атак на подсистемы и компоненты АСУ ТП



Выявление уязвимостей и недостатков механизмов защиты исследуемых подсистем АСУ ТП в программном и аппаратном обеспечении



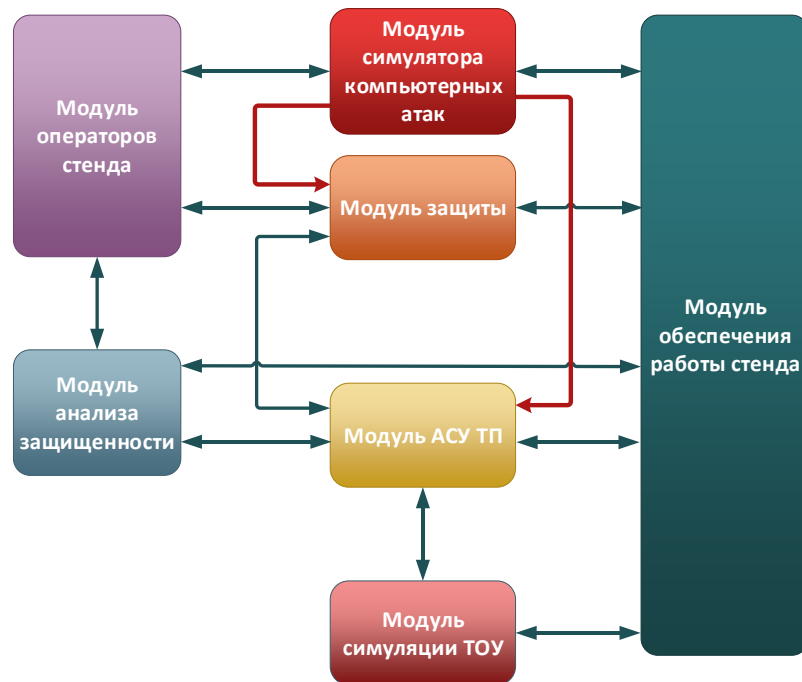
Подготовка рекомендаций по устранению выявленных уязвимостей или принятию компенсирующих мер



Разработка частной модели угроз исследуемой системы, определяющей возможные векторы несанкционированного воздействия на систему



Обучение персонала, занимающегося обслуживанием и эксплуатацией АСУ ТП, на оборудовании стенда в части обеспечения компьютерной безопасности АСУ ТП





Моделирование АСУ ТП: подсистем, компонентов, линий связи, конфигураций и настроек, уровня ущерба и т.д.



Симуляция развития компьютерных атак на смоделированную АСУ ТП



Моделирование и оценка последствий компьютерных атак на подсистемы и компоненты АСУ ТП



Оценка потенциального уровня ущерба от компьютерных атак, проведенных по различным сценариям



Минимизация уровня субъективности при оценке рисков информационной и компьютерной безопасности АСУ ТП



Оценка эффективности применения средств защиты АСУ ТП от компьютерных атак



Выявление незакрытых уязвимостей смоделированных АСУ ТП



Подготовка данных для разработки частной модели угроз смоделированной АСУ ТП

СПАСИБО

Константин Сахаров

Руководитель управления
информационной и компьютерной безопасности АСУ ТП

Tel.: +7 (495) 933-43-40, ad. 1090

Mob.: +7 (915) 198 01 37

E-mail: KVSakharov@rasu.ru

www.rasu.ru