Kaspersky Industrial Cybersecurity Conference

Практические аспекты обеспечения информационной безопасности подсистем АСУ ТП АЭС

Сахаров Константин Валерьевич
АО «РАСУ»

kaspersky

Деятельность в области обеспечения ИБ АСУ ТП

Зарубежные проекты

- Венгрия, Пакш-2
- Турция, Аккую
- Египет, Эль-Дабаа
- Бангладеш, Руппур

Проекты РФ

- Калининская АЭС
- Ростовская АЭС
- Курская АЭС-2
- Нововоронежская АЭС
- Белоярская АЭС

- Проектирование систем обеспечения информационной безопасности АСУ ТП
- Разработка документации: модели угроз, ТЗ, ТП, РД, ЭД в части ИБ
- Настройка оборудования АСУ ТП по требованиям ИБ
- Проведение испытаний подсистем АСУ ТП на соответствие требованиям ИБ

- Анализ уязвимостей в АСУ ТП и тестирование на проникновение
- Проведение аудитов поставщиков части реализации процессов безопасной разработки ППО
- Проверка ППО на соответствие требованиям ИБ (проведение статического, динамического тестирования, фаззинг-тестирования, тестирование на проникновение)

WANO

IAEA

IEC INTERNATIONAL ELECTROTECHNICAL COMMISSION

ROSATOM

- Разработка руководств и рекомендаций по компьютерной безопасности
- Участие в рабочих группах по компьютерной безопасности

- ТК 362 «Защита информации»
- ТК 45 «Ядерное приборостроение»
- Совет по информационной безопасности в Госкорпорации «Росатом» и ее организациях

The content of this presentation is for discussion purposes only, shall not be considered as an offer and doesn't lead to any obligations to RASU and its affiliated companies. RASU disclaims all responsibility for any and all mistakes, quality and completeness of the information.
© Intellectual property of JSC RASU. Copies shall include the reference

Требования законодательства к обеспечению ИБ (ИКБ)

Законодательство Российской Федерации

АСУ ТП АЭС в контуре Российской Федерации

- Федеральные законы
- Постановления Правительства
- Приказы, методические документы ФСТЭК и ФСБ России
- Приказы, распоряжения, ЕОМУ ГК «Росатом»
- Приказы, распоряжения, СТО АО «Концерн Росэнергоатом»

Международное законодательство

АСУ ТП АЭС в международном сегменте

- Nuclear Security Fundamentals
- Recommendations
- Implementing Guides
- Technical Guidance
- Локальные законы, нормативные правовые акты, стандарты страны

Ключевые НТД, влияющие на реализацию мер ИБ (ИКБ)

- **МУ-УИТ.09.00.07.** Единые отраслевые методические указания по категорированию объектов
- **Приказ ФСТЭК России от 25.12.2017 №239.** Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры
- **МР 1.1.4.04.1780-2021.** Оценка соответствия требованиям по безопасности информации
- **Стандарты и методические документы по разработке безопасного программного обеспечения**
- **IEC 62645:2014.** Nuclear power plants - Instrumentation and control systems - Requirements for security programmes for computer-based systems
- **IEC 62645:2019.** Nuclear power plants - Instrumentation, control and electrical power systems - Cybersecurity requirements
- **IAEA NSS 17-T.** Computer Security at Nuclear Facilities
- **IAEA NSS 33-T.** Computer Security of Instrumentation and Control Systems at Nuclear Facilities

Типовые организационно-технические меры по обеспечению информационной и компьютерной безопасности АСУ ТП АЭС

The content of this presentation is for discussion purposes only, shall not be considered as an offer and doesn't lead to any obligations to RASU and its affiliated companies. RASU disclaims all responsibility for any and all mistakes, quality and completeness of the information.
© Intellectual property of JSC RASU. Copies shall include the reference

Ограничения при реализации мер ИБ (ИКБ)

Модернизация подсистем АСУ ТП АЭС

Изготовления и поставка подсистем АСУ ТП на новый блок

Общие ограничения

- приоритет ядерной безопасности
- отсутствие значимого негативного влияние на технологические процессы АСУ ТП
- разная трактовка требований к реализации мер обеспечения ИБ (ИКБ)
- проприетарные протоколы передачи данных
- серийно выпускаемые КТС (при включение в состав шкафа дополнительного технического средства, например, межсетевого экрана или диода данных, требуется проведение полного комплекса испытаний)
- стоимость внедрения решений
- ограниченный выбор средств защиты информации, ограниченный функционал

ограничение по срокам модернизации и, следовательно, на срок проведения оценки влияния на технологический процесс встроенных и наложенных СЗИ

отсутствие реализованных мер обеспечения информационной безопасности в смежных/взаимодействующих подсистемах АСУ ТП

невозможность внедрения полноценной СОИБ без комплексной модернизации АСУ ТП

The content of this presentation is for discussion purposes only, shall not be considered as an offer and doesn't lead to any obligations to RASU and its affiliated companies. RASU disclaims all responsibility for any and all mistakes, quality and completeness of the information.
© Intellectual property of JSC RASU. Copies shall include the reference

Этапы реализации мер обеспечения ИБ (ИКБ)

Этапы создания АС

ТЗ

Требования к обеспечению ИБ подсистемы АСУ ТП

- Модель угроз безопасности информации, включая модель нарушителя
- Политика информационной безопасности
(аналог ЧТЗ на подсистему информационной безопасности)

Техноарабочий проект

Организационные и технические меры ИБ Проектирование

- План информационной безопасности
- Процедуры реализации мер информационной безопасности
- Эксплуатационная документация на подсистему информационной безопасности
- Инструкции по установке и настройке средств защиты информации
- Руководство администратора информационной безопасности

Подсистема информационной безопасности представляет из себя совокупность организационных и технических мер по обеспечению ИБ, принятых в соответствии с присвоенной подсистеме АСУ ТП категорией значимости

Ввод в действие

Организационные и технические меры ИБ Внедрение

- Установка и настройка средств защиты информации
- Разработка/доработка организационно-распорядительной документации
- Предварительные испытания подсистемы информационной безопасности
- Анализ уязвимостей и тестирование на проникновение подсистемы АСУ ТП
- Опытная эксплуатация
- Приемочные испытания подсистемы информационной безопасности

Под **ОРД** понимается комплект документов, регламентирующих правила и процедуры реализации организационных и технических мер ИБ, распределение функций и определение порядка взаимодействия подразделений и должностных лиц эксплуатирующей организации на этапах эксплуатации и вывода из эксплуатации подсистемы АСУ ТП, обеспечивающее четкое разделение их полномочий и ответственности

Ввод в промышленную эксплуатацию подсистемы АСУ ТП

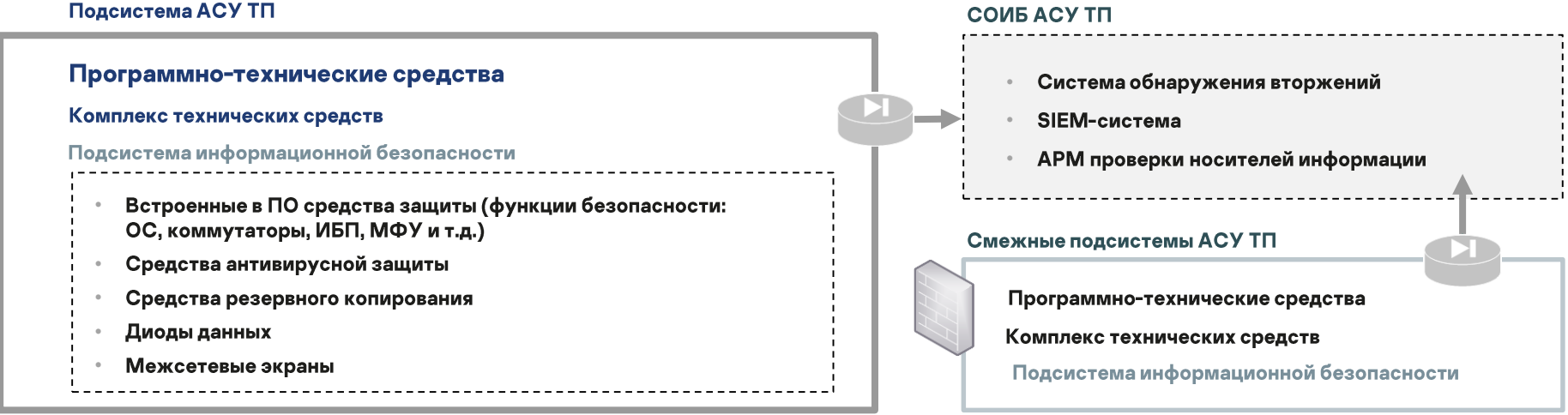
* под средствами защиты понимаются и наложенные и встроенные в общесистемное и прикладное программное обеспечение средства защиты

** внедрение организационных мер обеспечения ИБ (ИКБ) осуществляется эксплуатирующей организацией

The content of this presentation is for discussion purposes only, shall not be considered as an offer and doesn't lead to any obligations to RASU and its affiliated companies. RASU disclaims all responsibility for any and all mistakes, quality and completeness of the information.
© Intellectual property of JSC RASU. Copies shall include the reference

Подсистема информационной безопасности (1/3)

Вариант №1



- В зависимости от категории значимости, присвоенной подсистеме АСУ ТП, проектируется расположение межсетевого экрана.
- В состав СОИБ АСУ ТП входит средство анализа защищенности подсистем АСУ ТП
- В состав СОИБ АСУ ТП также входят портативные средства антивирусной защиты для проведения периодической антивирусной проверки в подсистемах АСУ ТП, в которых по объективным причинам невозможна установка «стационарного» средства антивирусной защиты

The content of this presentation is for discussion purposes only, shall not be considered as an offer and doesn't lead to any obligations to RASU and its affiliated companies. RASU disclaims all responsibility for any and all mistakes, quality and completeness of the information.
© Intellectual property of JSC RASU. Copies shall include the reference

Подсистема информационной безопасности (2/3)

Вариант №2

Подсистема АСУ ТП

Программно-технические средства

Комплекс технических средств

Подсистема информационной безопасности

- **Встроенные в ПО средства защиты (функции безопасности: ОС, коммутаторы, ИБП, МФУ и т.д.)**
- **Средства антивирусной защиты**
- **Средства резервного копирования**
- **Диоды данных (опционально)**
- **Межсетевые экраны**

Смежные подсистемы АСУ ТП

Программно-технические средства

Комплекс технических средств

Отсутствует подсистема информационной безопасности

- В зависимости от категории значимости, присвоенной подсистеме АСУ ТП, проектируется расположение межсетевого экрана.
- В зависимости от влияния на технологический процесс возможна установка на границе подсистемы АСУ ТП диода данных, например, для передачи данных в ЛВС.

Комплекс компенсирующих мероприятий

The content of this presentation is for discussion purposes only, shall not be considered as an offer and doesn't lead to any obligations to RASU and its affiliated companies. RASU disclaims all responsibility for any and all mistakes, quality and completeness of the information.
© Intellectual property of JSC RASU. Copies shall include the reference

Подсистема информационной безопасности (3/3)

Вариант №3

Подсистема АСУ ТП

Программно-технические средства

Комплекс технических средств

Подсистема информационной безопасности

- **Встроенные в ПО средства защиты (функции безопасности: ОС, коммутаторы, ИБП, МФУ и т.д.)**
- **Средства антивирусной защиты**
- **Средства резервного копирования**
- **Диоды данных (опционально)**
- **Межсетевые экраны**

Смежные подсистемы АСУ ТП

Программно-технические средства

Комплекс технических средств

Подсистема информационной безопасности

- **Встроенные в ПО СЗИ (функции безопасности: ОС, коммутаторы, ИБП, МФУ и т.д.)**
- **Средства антивирусной защиты**
- **Средства резервного копирования**
- **Диоды данных (опционально)**
- **Межсетевые экраны**

- В зависимости от категории значимости, присвоенной подсистеме АСУ ТП, проектируется расположение межсетевого экрана.
- В зависимости от влияния на технологический процесс возможна установка на границе подсистемы АСУ ТП диода данных, например, для передачи данных в ЛВС.

The content of this presentation is for discussion purposes only, shall not be considered as an offer and doesn't lead to any obligations to RASU and its affiliated companies. RASU disclaims all responsibility for any and all mistakes, quality and completeness of the information.
© Intellectual property of JSC RASU. Copies shall include the reference

Возникающие проблемы при реализации мер ИБ (ИКБ)
Базовые технические проблемы

Влияние средств антивирусной защиты на технологический процесс
Влияние обновлений средств антивирусной защиты и базы сигнатур

- Большая часть САВЗ работает в активном режиме на удаление или лечение и могут принять «технологический» файл за вредоносный
- У ряда САВЗ отсутствует автоматическая процедура обновления баз признаков вредоносного ПО

Невозможность установки аппаратного межсетевого экрана

Для серийно выпускаемых ПТС включение любого дополнительного технического средства ведет к новой разработке, РКД, полному циклу испытаний и постановки на серийное производство

Отсутствие встроенных средств защиты информации в прикладном ПО
Влияние настроек безопасности в ОС на функционирование прикладного программного обеспечения

Изменения настроек безопасности (парольной защиты, мандатного контроля целостности и тд) операционной системы может оказывать влияние на функционирование прикладного программного ПО

Необходимость получения сообщений о доставке при функционировании программного обеспечения подсистемы АСУ ТП

Для связи смежных подсистем АСУ ТП при передаче данных зачастую требуется подтверждение получения данных, что невозможно при односторонней передаче через диоды. Также и с функционированием SIEM системы, когда агенты размещаются в подсистемах АСУ ТП и передают данные в СОИБ

The content of this presentation is for discussion purposes only, shall not be considered as an offer and doesn't lead to any obligations to RASU and its affiliated companies. RASU disclaims all responsibility for any and all mistakes, quality and completeness of the information.
© Intellectual property of JSC RASU. Copies shall include the reference

Пути реализации мер обеспечения ИБ (ИКБ) при базовых технических проблемах

Использование САВЗ без активного модуля защиты «Тонкая» настройка САВЗ по каждому из сценариев выполнения Тестовый стенд/отдельный АРМ для проверки влияния обновлений

- Дополнительное тестирование САВЗ с каждой подсистемой при проведении настройки и предварительных испытаний
- Ведется работа с вендором по разработке портативного САВЗ для Linux и полная поддержка продукта со стороны вендора
- Разработана процедура обновления САВЗ, не поддерживающего автоматическое обновление без сети Интернет

Невозможность установки аппаратного межсетевого экрана

- Установка аппаратных МЭ в смежных подсистемах (в которых отсутствуют серийно выпускаемые ПТС)
- Настройка iptables в ОС семейства Linux
- Тестирование МЭ на влияние на технологический процесс и включение в конструктив обновленных ПТС – работа с Разработчиком ПТС

Отсутствие встроенных средств защиты информации в прикладном ПО Влияние настроек безопасности в ОС на функционирование прикладного программного обеспечения

- Установка требований по наличию ВСЗИ в прикладном ПО – взаимодействие с разработчиками прикладного ПО АСУ ТП
- Дополнительное тестирование прикладного ПО при настроенных функциях безопасности ОС на этапе предварительных испытаний

The content of this presentation is for discussion purposes only, shall not be considered as an offer and doesn't lead to any obligations to RASU and its affiliated companies. RASU disclaims all responsibility for any and all mistakes, quality and completeness of the information.
© Intellectual property of JSC RASU. Copies shall include the reference

Испытания подсистемы безопасности (1/2)

Предварительные испытания

Предварительные испытания подсистемы безопасности на соответствие ИБ включают:

- проверку работоспособности отдельных средств защиты информации и подсистемы безопасности в целом;
- предварительную оценку выполнения требований информационной безопасности, изложенных в Политике ИБ;
- оценку влияния подсистемы безопасности на функционирование подсистемы АСУ ТП АЭС при проектных режимах её работы, установленных проектной документацией;
- принятие решения о возможности опытной эксплуатации подсистемы безопасности при проведении опытной эксплуатации подсистемы АСУ ТП АЭС

Анализ уязвимостей и тестирование на проникновение

- Моделируются условия**, соответствующие возможностям нарушителей, определенным в модели угроз безопасности информации**

Опытная эксплуатация

- Опытную эксплуатацию подсистемы безопасности проводят с целью обнаружения и устранения ошибок, готовности пользователей и персонала к работе в условиях функционирования подсистемы безопасности, определения фактической эффективности подсистемы безопасности, корректировки (при необходимости) документации.
- Опытная эксплуатация подсистемы безопасности всегда совмещена с опытной эксплуатацией подсистемы АСУ ТП АЭС

Приемочные испытания

- В ходе приемочных испытаний подсистемы безопасности проводится комплекс технических мероприятий (испытаний), в результате которых подтверждается соответствие подсистемы безопасности подсистемы АСУ ТП АЭС требованиям Политики ИБ на подсистему АСУ ТП АЭС.

Нормативная база: ГОСТ Р 59792-2021; приказ ФСТЭК России от 25.12.2017 №239; МР 1.1.4.04.1780-2021

Испытания подсистемы безопасности должны коррелироваться с испытаниями подсистемы АСУ ТП АЭС. Формат и вид испытаний для каждой подсистемы и в зависимости от проекта может уточняться

The content of this presentation is for discussion purposes only, shall not be considered as an offer and doesn't lead to any obligations to RASU and its affiliated companies. RASU disclaims all responsibility for any and all mistakes, quality and completeness of the information.
© Intellectual property of JSC RASU. Copies shall include the reference

Испытания подсистемы безопасности (2/2)

Все программы и методики испытаний согласовываются с Изготовителем, Заказчиком, эксплуатирующей организацией

На этапе предварительных испытаний проводится аудит внедрения процессов разработки безопасного программного обеспечения у Изготовителя ПТС (в случае самостоятельной разработки ПО)

Испытания проводятся только по утвержденным ПМИ и с участием Изготовителя, Заказчика и эксплуатирующей организацией

Ввод в действие подсистемы АСУ ТП АЭС осуществляется при положительном заключении (выводе) о соответствии подсистемы АСУ ТП АЭС требованиям ИБ, изложенным в Политике ИБ на подсистему АСУ ТП АЭС

Вид (наименование) испытаний на соответствие требованиям информационной безопасности может изменяться в зависимости от подсистемы АСУ ТП АЭС, но сохраняется последовательность:

- Предварительные испытания
- Приемочные испытания

Предварительные испытания могут проводиться либо на площадке завода-изготовителя, либо на полигоне АО «РАСУ»
Приемочные испытания рекомендуется проводить на площадке АЭС ввиду наличия рисков внесения изменений в конфигурацию подсистемы при проведении ПНР

The content of this presentation is for discussion purposes only, shall not be considered as an offer and doesn't lead to any obligations to RASU and its affiliated companies. RASU disclaims all responsibility for any and all mistakes, quality and completeness of the information.
© Intellectual property of JSC RASU. Copies shall include the reference

Аудит поставщиков в части реализации процессов разработки безопасного ПО

Программные и программно-технические средства защиты информации

Компоненты системы обеспечения информационной безопасности АСУ ТП

Приказ ФСТЭК России от 25.12.2017 №239, п.29.3:

Методика оценки поставщиков
Критерии

- наличие руководства по РБПО;
- проведение анализа угроз ИБ для ПО;
- наличие описания структуры ПО на уровне подсистем и сопоставления функций и интерфейсов ПО, с его подсистемами (для ЗО КИИ 1 кат.)

- проведение статического анализа исходного кода программы;
- проведение фаззинг-тестирования программы;
- проведение динамического анализа кода программы (для ЗО КИИ 1 кат.)

- наличие процедур отслеживания и исправления обнаруженных ошибок и уязвимостей ПО;
- определение способов и сроков доведения до пользователей информации об уязвимостях ПО, о компенсирующих мерах по ЗИ или ограничениях по применению ПО, способов получения пользователями ПО его обновлений, проверки их целостности и подлинности;
- наличие процедур информирования пользователя об окончании производства и (или) поддержки ПО (для ЗО КИИ 1 кат.).

АУДИТ ПОСТАВЩИКОВ

- Экспертиза документации
- Оценка полноты и достаточности проводимых испытаний ПО
- Выездная экспертиза реализуемых процедур тестирования ПО
- Проверка наличия процессов технической поддержки ПО

Приказ ФСТЭК России от 25.12.2017 №239, п.29.4:

The content of this presentation is for discussion purposes only, shall not be considered as an offer and doesn't lead to any obligations to RASU and its affiliated companies. RASU disclaims all responsibility for any and all mistakes, quality and completeness of the information.
© Intellectual property of JSC RASU. Copies shall include the reference

Thank you!

Практические аспекты обеспечения информационной безопасности подсистем АСУ ТП АЭС

Сахаров Константин Валерьевич **АО «РАСУ»** **rasu.ru**

kaspersky