РОСАТОМ

ГОСУДАРСТВЕННАЯ КОРПОРАЦИЯ ПО АТОМНОЙ ЭНЕРГИИ «РОСАТОМ»

Подход АО «РАСУ» к обеспечению информационной и компьютерной безопасности (кибербезопасности) АСУ ТП АЭС

А.Н. Лукашкин

Начальник отдела информационной и компьютерной безопасности
АО «Русатом Автоматизированные системы управления»

XXII Международный форум «Технологии безопасности»
Москва, 13-15 февраля 2018 года

Обеспечение комплексной безопасности и защищенности объектов промышленности, нефтегаза и энергетики

Методологические основы обеспечения информационной и компьютерной безопасности (кибербезопасности) АСУ ТП, создаваемых для АЭС российской юрисдикции

Во исполнение п.3 ***«Комплексного плана мероприятий по обеспечению информационной и компьютерной безопасности (кибербезопасности) АСУ ТП АЭС на 2017-2020 гг.»****, утвержденного приказом Госкорпорации «Росатом» от 29 июня 2017 года № 1/590-П «Об утверждении Комплексного плана мероприятий по обеспечению информационной и компьютерной безопасности АСУ ТП АЭС на 2017–2020 гг.», в истекшем году (2017 г.) силами АО «РАСУ», в рамках отведенных полномочий, был разработан и введен в действие документ концептуального уровня со следующим титульным наименованием –* ***«Методологические основы по созданию АСУ ТП в части обеспечения информационной и компьютерной безопасности (кибербезопасности) АСУ ТП АЭС. Редакция 1.0»*** *(далее – «Методологические основы …»).*

Назначение и цели «Методологических основ…»*:*

разрабатываемый документ ***предназначен*** *для документальной фиксации достигнутого уровня методологических и концептуальных воззрений по созданию АСУ ТП в защищенном исполнении для АЭС российской юрисдикции на основе действующих нормативных правовых актов Российской Федерации и национальных нормативно-технических и нормативно методических документов, регламентирующих правоотношения и устанавливающих технические и организационные требования по обеспечению информационной безопасности для объектов критической информационной инфраструктуры Российской Федерации;*

целью *разработки документа является изложение методологических основ практической направленности относительно: вербальной модели предметной области информационной и компьютерной безопасности (кибербезопасности) АСУ ТП АЭС, ключевых участников отношений в предметной области, целевой и ролевой направленности деятельности субъектов отношений в рамках предметной области, а также концептуальные положения касаемо формирования требований к защите информации в АСУ ТП АЭС и концептуальные положения касаемо создания АСУ ТП АЭС как автоматизированной системы в защищенном исполнении (АС ЗИ).*

Базовые документы, использованные при разработке «Методологических основ…»

Федеральные законы:

- от 21 ноября 1995 года № 170-ФЗ «Об использовании атомной энергии»;
- от 27 декабря 2002 года № 184-ФЗ «О техническом регулировании»;
- от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- от 28 декабря 2010 года № 390-ФЗ «О безопасности»;
- от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

Доктринальные документы:

- «Доктрина информационной безопасности Российской Федерации», утвержденная Президентом Российской Федерации 5 декабря 2016 года № 646;
- «Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы», утвержденная Указом Президента Российской Федерации от 9 мая 2017 года № 203;
- «Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными технологическими процессами критически важных объектов инфраструктуры Российской Федерации», утвержденные Президентом Российской Федерации 3 февраля 2012 года № 803;
- «Программа «Цифровая экономика Российской Федерации», утвержденная распоряжением Правительства Российской Федерации от 28 июля 2017 года № 1632-р.

Федеральные нормы и правила в области использования атомной энергии:

- «Общие положения обеспечения безопасности атомных станций» (НП-001-15);
- «Требования к управляющим системам, важным для безопасности атомных станций» (НП-026-16);
- «Положение о порядке расследования и учета нарушений в работе атомных станций» (НП-004-08);
- «Требования к системам физической защиты ядерных материалов, ядерных установок и пунктов хранения ядерных Материалов» (НП-083-15);

«Требования к программам обеспечения качества для объектов использования атомной энергии» (НП-090-11)

Документы государственных регуляторов, уполномоченных в области защиты информации:

- «Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды», утвержденные приказом ФСТЭК России от 14 марта 2014 года № 31 «Об утверждении Требований к обеспечению защиты информации …» (Зарегистрировано в Минюсте России, Рег. № 32919 от 30 июня 2014 года);
- «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)» (с изменениями) // Гостекомиссия России, М.: 2001;

Базовые документы, использованные при разработке «Методологических основ…» (продолжение)

Документы МАГАТЭ:

- «Технические руководящие материалы. Компьютерная безопасность на ядерных установках. Справочное руководство» // МАГАТЭ, ВЕНА, 2012. – Серия изданий МАГАТЭ по физической ядерной безопасности, № 17;
- Security of nuclear information. – VIENNA: INTERNATIONAL ATOMIC ENERGY AGENCY (IAEA), 2015. – IAEA nuclear security series No. 23-G;
- Design of instrumentation and control systems for nuclear power plants: specific safety guide. – VIENNA: INTERNATIONAL ATOMIC ENERGY AGENCY (IAEA), 2016. – IAEA safety standards series, No. SSG-39.

Национальные стандарты:

- ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования;
- ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения;
- ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения;
- ГОСТ Р 56546-2015 Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем;
- ГОСТ Р 56939-2016 Защита информации. Разработка безопасного программного обеспечения. Общие требования;
- ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель;
- ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности;
- ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности;
- ГОСТ Р МЭК 61226-2011 Атомные станции. Системы контроля и управления, важные для безопасности. Классификация функций контроля и управления;
- ГОСТ Р МЭК 60880–2011 Атомные электростанции. Системы контроля и управления, важные для безопасности. Программное обеспечение компьютерных систем, выполняющих функции категории А;
- ГОСТ Р МЭК 62138–2011 Атомные электростанции. Системы контроля и управления, важные для безопасности. Программное обеспечение компьютерных систем, выполняющих функции категории В и С;
- ГОСТ Р 56205-2014 Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели.

Базовые документы, использованные при разработке «Методологических основ…» (окончание)

Документы организаций, подведомственных Госкорпорации «РОСАТОМ»:

- «Общие положения по обеспечению безопасности информации автоматизированных систем контроля и управления технологическими процессами на АЭС. ОП 1.5.2.01.999.0202–2014 (в редакции Изменений № 1)», введенные в действие приказом ОАО «Концерн Росэнергоатом» от 30 января 2014 года № 9/77–П «О введении в действие …» (с изменениями № 1 к ОП 1.5.2.01.999.0202–2014, введенными в действие приказом ОАО «Концерна Росэнергоатом» от 25 апреля 2016 года № 9/496–П);
- «Порядок обеспечения информационной безопасности при создании и вводе в действие АСУ ТП. ПОР-УЖЦАСУ.39», введенный в действие приказом АО «РАСУ» от 23 марта 2017 года № 341/111-П;
- «Руководство по информационной и компьютерной безопасности при создании АСУ ТП. РК-УЖЦАСУ.01», введен в действие приказом АО «РАСУ» № 341/199-П от 24.05.2017.

Базовый посыл и смысловое построение «Методологических основ…»

В качестве **базового посыла** была использована **концептуальная идея**, состоящая в том, что минимизация остаточных рисков нарушения безопасности (целостности и доступности, а в случае необходимости и конфиденциальности) критически важной (значимой) информации (КВ(З)И), обрабатываемой средствами автоматизации, входящими в состав компонент (подсистем) АСУ ТП АЭС, может быть достигнута **только при условии создания АСУ ТП АЭС** и последующего её ввода в действие на АЭС для эксплуатации, как автоматизированной системы (компьютеризированной информационно-управляющей системы, или иначе – информационно-управляющей системы с широким применением цифровой техники) в **защищенном исполнении (АС ЗИ).**

Разработанные **«Методологические основы …»** относятся к корпусу методологических документов практической направленности в конкретной предметной области приложения и содержат, в том числе:

- ***вербальную модель*** *предметной области приложения*;
- *описание* ***ключевых участников*** *отношений в предметной области приложения;*
- *описание* ***целевой и ролевой направленности*** *деятельности субъектов отношений в рамках предметной области приложения.*

Основные объекты предметной области информационной и компьютерной безопасности (кибербезопасности) АСУ ТП АЭС

Основными объектами предметной области информационной и компьютерной безопасности (кибербезопасности) АСУ ТП АЭС являются:

- *собственно, **АСУ ТП**, являющиеся элементами сооружаемой (или модернизируемой) **АЭС**, состоящие из компьютеризированных и не компьютеризированных компонент (подсистем) различной целевой и функциональной направленности;*
- ***информация**, обрабатываемая компонентами (подсистемами) АСУ ТП и их составными элементами в автоматизированном и автоматическом режимах, для целей обеспечения функции нормальной эксплуатации АЭС, а также для целей обеспечения управления АЭС в условиях проектных и запроектных аварий;*
- *компьютеризированные и не компьютеризированные **компоненты (подсистемы)**, используемые для обработки информации;*
- *эвентуальные **угрозы безопасности информации**, обрабатываемой компонентами (подсистемами) АСУ ТП, а также эвентуальные угрозы компонентам (подсистемам) АСУ ТП и их составных элементов, применяемым (используемым) при обработке информации;*
- *эвентуальные **нарушители безопасности информации**, обрабатываемой компонентами (подсистемами) АСУ ТП и их составными элементами;*
- *системы защиты информации (СиЗИ).*

АСУ ТП АЭС, как объект предметной области информационной и компьютерной безопасности (кибербезопасности)

АСУ ТП в составе АЭС предназначена для:

- ***управления*** *всеми технологическими объектами АЭС;*
- ***контроля*** *технологических объектов управления (ТОУ) и автоматизированного ведения режимов, защиты оборудования, автоматического регулирования параметров ТОУ;*
- ***диагностики*** *основного оборудования;*
- ***информационного обеспечения*** *персонала, а целью создания всякой АСУ ТП является выполнение* ***контроля и управления*** *технологическими процессами и оборудованием для обеспечения:*
  - *ядерной и радиационной безопасности;*
  - *надежности выработки электроэнергии;*
  - *экономичности производственных процессов.*

Типовая АСУ ТП АЭС*, как правило, представима следующей* ***трёхуровневой*** *логической структурой:*

уровень ***операторского*** *(диспетчерского) управления (верхний уровень);*

уровень ***автоматического*** *управления (средний уровень);*

уровень ***ввода (вывода) данных****,* ***исполнительных устройств*** *(нижний (полевой) уровень).*

АСУ ТП АЭС, как объект предметной области информационной и компьютерной безопасности (кибербезопасности) (продолжение)

Состав систем и подсистем типовой АСУ ТП АЭС определяется требованиями Федеральных норм и правил НП-001-15 и НП-026-16 и **различаются по**:

- **назначению:**
  - *системы и элементы нормальной эксплуатации;*
  - *системы и элементы безопасности;*
  - *системы и элементы специальных технических средств для управления запроектными авариями;*
- **влиянию на безопасность:**
  - *важные для безопасности;*
  - *остальные, не влияющие на безопасность.*

*На каждом энергоблоке блоке АЭС для управления технологическим оборудованием систем нормальной эксплуатации (**СНЭ**) и систем безопасности (**СБ**) **предусматриваются**:*

- *блочный пункт управления (**БПУ**);*
- *резервный пункт управления (**РПУ**);*
- *управляющие системы нормальной эксплуатации (**УСНЭ**);*
- *управляющие системы безопасности (**УСБ**);*
- *система информационной поддержки оператора (**СИПО**);*
- *автономные средства регистрации и хранения информации (**АСРиХИ**).*

*Согласно НП-026-16 для каждого энергоблока АЭС предусматриваются следующие управляющие системы важные для безопаснсти (**УСВБ**):*

- *управляющие системы нормальной эксплуатации, важные для безопасности (**УСНЭ ВБ**);*
- *управляющие системы безопасности (**УСБ**);*
- *управляющие системы, относящиеся к важным для безопасности специальным техническим средствам для управления запроектными авариями.*

Требование гарантированного и высоконадежного обеспечения глубокоэшелонированной защиты АЭС – базовый принцип формирования архитектуры типовой АСУ ТП АЭС

В соответствии с требованиями Федеральных нормы и правила в области использования атомной энергии НП-001-15 безопасность АЭС должна обеспечиваться за счет последовательной реализации глубокоэшелонированной защиты (ГЭЗ), предусматривающей 5 уровней.

Уровни ГЭЗ	Подсистема АСУ ТП АЭС	Главная функция
Уровень 1 (I)	УСНЭ (СКУ НЭ)	Устранение отклонений от заданного режима работы
Уровень 2 (II)	УСНЭ ВБ (СКУ НЭВБ)	Предотвращение развития отклонений от нормальной эксплуатации в проектные аварии
Уровень 3 (III)	УСБ (СКУ СБ)	Предотвращение развития проектных аварий в запроектные аварии
Уровень 4 (IV)	СКУ запроектных аварий	Управление запроектными авариями
Уровень 5 (V)	Пост аварийные СКУ	Послеаварийные организационные и технические меры

Требования НП-026-16 по обеспечению информационной и компьютерной безопасности (кибербезопасности)

*Установлены следующие **требования к структуре типовой АСУ ТП АЭС**:*

- *в составе УСВБ, должны предусматриваться системы, обеспечивающие представление персоналу АЭС достоверной информации о состоянии систем и элементов АЭС, важных для безопасности;*
- *перечень параметров АЭС, контролируемых с БПУ, должен быть достаточным для предоставления персоналу АЭС однозначной информации о соблюдении пределов безопасной эксплуатации АЭС, о возникновении условий введения в действие СБ, а также об автоматическом срабатывании и функционировании систем безопасности;*
- *обмен информацией между УСВБ и СНЭ, не влияющими на безопасность, должен осуществляться в одностороннем режиме (от УСВБ в СНЭ, не влияющие на безопасность) через шлюзовые устройства из состава УСВБ;*
- *на АЭС должна быть обеспечена защищенность от несанкционированного доступа (НСД) к элементам УСВБ, включая линии связи и данные;*
- *объектами, в отношении которых должна обеспечиваться защищенность от НСД, являются:*
- *средства, с помощью которых производится изменение уставок защит, блокировок, предупредительной и аварийной сигнализации, задание настроек регуляторов;*
- *коммутационные элементы для подключения внешних по отношению к УСВБ цепей;*
- *сменные составные части, расположенные внутри элементов УСВБ;*
- *органы ручного управления (например, выключатели электроснабжения, переключатели режимов работы, средства вывода из работы каналов УСВБ и другие);*
- *средства ручного ввода и вывода данных (например, клавиатура);*
- *носители и программное обеспечение (ПО) на носителях;*
- *для УСВБ, участвующей в выполнении управляющих или информационных функций категории А или В, должны быть предусмотрены меры по предотвращению НСД внутрь составных частей УСВБ, по обеспечению защищенности от изменения программ и данных, в том числе со стороны смежных систем, а также немедленное оповещение персонала АЭС о НСД. Проектом АЭС должны быть предусмотрены технические и административные меры ограничения доступа к элементам УСВБ.*

Информация, обрабатываемая в АСУ ТП АЭС, как объект предметной области информационной и компьютерной безопасности (кибербезопасности)

*Информация, обрабатываемая автоматически и автоматизировано, в АСУ ТП АЭС, посредством технических, программно-технических и программных средств, входящих в состав её компонент (подсистем, ТК, ПК, ПТК) подразделяется на осведомляющую информацию (**ОИ**) и управляющую информацию (**УИ**).*

***К ОИ относится**:*

- *сигналы, характеризующие измеряемые и вычисляемые параметры;*
- *отображаемые данные о состоянии технологического процесса, на основе которых принимаются решения по управлению оборудованием и системами;*
- *учетная информация о регистрации событий.*

***К УИ относится**:*

- ***управляющая информация**, обеспечивающая управление технологическим процессом (команды, сигналы, управляющие сигналы);*
- ***программно-техническая информация** (конфигурационные файлы, резервные копии программного обеспечения, дистрибутивы, настройки программного обеспечения, обеспечивающие требуемые режимы функционирования АСУ ТП, а также программно-техническая документация);*
- ***аутентификационные и идентификационные данные** персонала АСУ ТП (идентификационная информация).*

*ОИ и УИ, обрабатываемая компонентами (подсистемами) АСУ ТП, разделяется на **два следующих вида**: критически важную (значимую) информацию **(КВ(З)И)** и не являющуюся таковой (не КВ(З)И).*

Информация, обрабатываемая в АСУ ТП АЭС, как объект предметной области информационной и компьютерной безопасности (кибербезопасности) (продолжение)

Защита КВ(З)И понимается деятельность, направленная на предотвращение:

- *несанкционированных воздействий на информацию;*
- *непреднамеренных воздействий на информацию;*
- *утечки информации (для КВ(З)И категорированной как конфиденциальной).*

***Виды защиты**:*

- ***техническая защита информации** (обеспечение не криптографическими методами защиты информации, с применением технических (аппаратных), программных и программно-технических (программно-аппаратных) средств);*
- ***криптографическая защита информации** (защита информации с помощью её криптографического преобразования);*
- ***физическая защита информации** (защита информации путем применения организационных мер и мероприятий, а также совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту (средству) обработки информации).*

*Посредством комплексного применения мер защиты КВ(З)И в АСУ ТП обеспечивается её **доступность** (availability), **целостность** (integrity), а также **конфиденциальность** (confidentiality), для той части КВ(З)И, каковая категорирована как конфиденциальная.*

***Защита КВ(З)И**, обрабатываемой в АСУ ТП АЭС должна быть:*

- *гарантируемой;*
- *комплексной;*
- *целенаправленной;*
- *управляемой;*

Обработка КВ(З)И в АСУ ТП АЭС осуществляется автоматически и автоматизировано посредством использования, в том числе, компьютеризированных технических (аппаратных), программно-технических (программно-аппаратных) и программных средств, входящих в состав комплекса средств автоматизации (КСА) АСУ ТП АЭС, каковые со организованны в виде функциональных совокупностей программных, технических и программно-технических комплексов (ТК, ПК и ПТК), исходя из их целевого назначения в составе АСУ ТП АЭС.

От полноты и достоверности, а также своевременности поступления ОИ и УИ напрямую зависит ***качество управления нормальной эксплуатацией*** *АЭС оперативным персоналом АСУ ТП АЭС.*

В качестве ***предельного*** *принимается случай реализации на основе неполной и/или недостоверной информации и/или отсутствия необходимой информации ошибочных решений и действий оперативного персонала, вследствие которых может произойти (или быть инициирована) авария на АЭС (как проектная, так и запроектная)*

Следствием несанкционированных и/или непреднамеренных физических, информационных, энергоинформационных или иных воздействий на элементы ТК, ПК и ПТК, эксплуатируемых в составе КСА АСУ ТП АЭС, а также наличие у элементов ТК, ПК и ПТК изначально не предусмотренных атрибутивных и/или функционально-кибернетических свойств (или качеств), может явится ***нарушение доступности и целостности****, обрабатываемой в АСУ ТП АЭС КВ(З)И, а также* ***конфиденциальности КВ(З)И****, для той части, которая категорирована как конфиденциальная.*

Принимается, что:

***при эксплуатации** ТК, ПК и ПТК, предназначенных для обработки КВ(З)И, должны быть обеспечены их целостность (integrity), доступность (availability), подотчетность (accountability), подлинность (authenticity), а также конфиденциальность (confidentiality) по компонентам, входящих в состав технических средств защиты информации (ТСЗИ) и средств криптографической защиты информации (СКЗИ);*

***при создании (проектировании и разработке)** ТК, ПК и ПТК, предназначенных для обработки КВ(З)И, должны быть обеспечены минимально возможные риски случайных и/или преднамеренных воздействий на создаваемые элементы ТК, ПК и ПТК, со стороны их создателей (проектировщиков, разработчиков) и/или применяемых ими инструментальных средств проектирования (разработки), в результате которых у элементов ТК, ПК и ПТК могут появиться изначально не предусмотренные атрибутивные и/или функционально-кибернетические свойства (или качества), обусловливающие ситуационные условия для нарушения целостности, доступности и конфиденциальности КВ(З)И, а также порождающие скрытые каналы для различных негативных воздействий на КВ(З)И;*

***в рамках создания** ТК, ПК и ПТК, предназначенных для обработки КВ(З)И, должна быть предусмотрена и реализована процедура специальных лабораторных отработочных испытаний и камерального контроля отсутствия в составе элементов ТК, ПК и ПТК аппаратных, аппаратно-программных и программных закладок и/или недекларированных возможностей, имеющих целью создавать реальные или потенциально возможные действия по нарушению целостности, доступности и конфиденциальности КВ(З)И;*

при создании (проектировании и разработке) ТК, ПК и ПТК должна быть обеспечена конфиденциальность относительно реализуемых в составе АСУ ТП АЭС технических и организационных решений по защите КВ(З)И, защите ТК, ПК и ПТК, предназначенных для обработки КВ(З)И, а также защите самих ТСЗИ и СКЗИ.

Система защиты информации (СиЗИ) в составе АСУ ТП АЭС

Проектируемая и разрабатываемая СиЗИ, для АСУ ТП АЭС, создаваемой в защищенном исполнении, определяется как совокупность организационных мероприятий, технических, программных и программно-технических средств защиты информации и средств контроля эффективности защиты информации, предназначенных для предотвращения несанкционированного доступа к защищаемой КВ(З)И, обрабатываемой в подсистемах (компонентах) АСУ ТП АЭС, а также для предотвращения реализации угроз безопасности КВ(З)И, нарушающий свойства её безопасности (доступности, целостности и конфиденциальности, для части КВ(З)И, категорированной как конфиденциальной).

При производстве проектных работ создаваемая СиЗИ для АСУ ТП АЭС рассматривается в статусе обязательного элемента системы технических и организационных мер глубокоэшелонированной защиты АЭС, относимого одновременно ко 2-му и 3-му уровню мер глубокоэшелонированной защиты в соответствии с НП-001-15.

При проектировании и разработке СиЗИ АСУ ТП АЭС используются:

- *Контрактные требования головного Заказчика АСУ ТП АЭС (АО «Концерн Росэнергоатом» и/или его филиалов);*
- *Федеральные нормы и правила в области использования атомной энергии (НП-001-15, НП-026-16, НП-004-08, НП-083-15, НП-090-11);*
- *Требования и рекомендации национальных стандартов и методических документов по защите информации, в том числе «Требования…» утвержденные приказом ФСТЭК России от 14 марта 2014 года № 31;*
- *Документы МАГАТЭ по обеспечению компьютерной безопасности;*
- *«Общие положения по обеспечению безопасности информации автоматизированных систем контроля и управления технологическими процессами на АЭС. ОП 1.5.2.01.999.0202–2014», АО «Концерн Росэнергоатом»;*
- *«Модели угроз безопасности КВ(З)И АСУ ТП АЭС» предоставляемые головным Заказчиком и/или его филиалами;*
- *Стандарты МЭК и иные международные или национальные НТД по кибербезопасности, если это специально оговорено контрактными требованиями головного Заказчика АСУ ТП АЭС.*

Система защиты информации (СиЗИ) в составе АСУ ТП АЭС (продолжение)

*Для подсистем (компонент) АСУ ТП АЭС, отнесенных к соответствующим **классам защищенности** (классам кибербезопасности) применяются **сертифицированные** СрЗИ (средства вычислительной техники, системы обнаружения вторжений, средства антивирусной защиты, средства доверенной загрузки, средства контроля съемных носителей информации, межсетевые экраны, шлюзы однонаправленной передачи данных и др.) в соответствии с п. А.2 Приложения А. «Общих положений …» ОП 1.5.2.01.999.0202–2014.*

*Принимается, что **базовые наборы мер защиты** (технических и организационных), каковые должны быть реализованы в рамках проектируемой и разрабатываемой СиЗИ АСУ ТП АЭС, для различных классов кибербезопасности (классов защищенности) подсистем (компонент) АСУ ТП АЭС, выбираются из таблицы А.1 Приложения А. «Общих положений …» ОП 1.5.2.01.999.0202–2014.*

*Для конкретной подсистемы (компоненте) АСУ ТП АЭС должен быть, как минимум, **реализован** в СиЗИ АСУ ТП АЭС **адаптированный базовый набор мер защиты** КВ(З)И, соответствующий установленному классу защищенности (классу кибербезопасности) этой подсистемы (компоненты) АСУ ТП АЭС.*

*При **невозможности реализации** в СиЗИ АСУ ТП АЭС отдельных выбранных мер защиты КВ(З)И на этапах адаптации базового набора мер защиты КВ(З)И или уточнения адаптированного базового набора мер защиты КВ(З)И могут разрабатываться **иные (компенсирующие) меры защиты** КВ(З)И, обеспечивающие адекватное блокирование (нейтрализацию) **актуальных угроз** нарушения безопасности КВ(З)И, обрабатываемой в конкретной подсистеме (компоненте) АСУ ТП АЭС.*

*СиЗИ для АСУ ТП АЭС, создаваемой в **защищенном исполнении**, проектируется и разрабатывается как система, имеющая в своём составе, в том числе, ниже перечисленные **подсистемы** защиты информации:*

систему защиты информации от несанкционированного доступа (СиЗИ НСД);

систему антивирусной защиты (САВЗ);

систему обнаружения вторжений (СОВ);

систему защиты информации от утечки по техническим каналам (СиЗИ УТК), для той части информации, которая категорирована как конфиденциальная.

РОСАТОМ

ГОСУДАРСТВЕННАЯ КОРПОРАЦИЯ ПО АТОМНОЙ ЭНЕРГИИ «РОСАТОМ»

Спасибо за внимание!

А.Н. Лукашкин

Начальник отдела информационной и компьютерной безопасности АО «Русатом Автоматизированные системы управления»