



МЧС РОССИИ

ГЛАВНОЕ УПРАВЛЕНИЕ
МИНИСТЕРСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
ПО ДЕЛАМ ГРАЖДАНСКОЙ ОБОРОНЫ,
ЧРЕЗВЫЧАЙНЫМ СИТУАЦИЯМ И ЛИКВИДАЦИИ
ПОСЛЕДСТВИЙ СТИХИЙНЫХ БЕДСТВИЙ
ПО ПРИМОРСКОМУ КРАЮ
(Главное управление МЧС России
по Приморскому краю)

ул. Суханова, 3, г. Владивосток, 690091
Телефон/факс: 243-28-27, e-mail: gu_mchs_pk@mail.ru

31 АВГ 2015 г. № 6653-4-2

на № 45-2761 от 21.08.2015 г.

О разработке СМИС

ООО

«РН – Находканефтепродукт»

ул. Макарова, д. 19
г. Находка, 692929

Специалистами Главного управления МЧС России по Приморскому краю рассмотрено Ваше обращение о возможности согласования разработки проекта СМИС в рамках отдельного проекта для ООО «РН-Находканефтепродукт».

По данному обращению сообщая, что, рассмотрев представленную копию задания на проектирование № 7/1 от 12.11.2014 «Автоматизация технологических процессов и пожаротушения», Главное управление МЧС России по Приморскому краю согласовывает разработку проекта создания единой СМИС для ООО «РН-Находканефтепродукт» и разделы VI «Дополнительные сведения для разработки мероприятий по предупреждению чрезвычайных ситуаций природного и техногенного характера» в ранее выданных исходных данных и требованиях для разработки подраздела перечня мероприятий по гражданской обороне, мероприятий по предупреждению чрезвычайных ситуаций природного и техногенного характера (ПМ ГОЧС) (исх. № 3446-4-2 от 28.05.2014, исх. № 3447-4-2 от 28.05.2014, исх. № 3449-4-2 от 28.05.2014) излагает в следующей редакции:

«Проектом предусмотреть создание структурированной системы мониторинга и управления инженерными системами зданий и сооружений (СМИС) на территории, выделенной под строительство в составе единой СМИС на территории ООО «РН-Находканефтепродукт»».

Начальник Главного
управления
полковник внутренней службы

В.Ю. Фокин

ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АСУТП**1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ**

АВТОМАТИЗИРОВАННАЯ СИСТЕМА УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМ ПРОЦЕССОМ – система контроля, управления и защиты технологического процесса, построенная на средствах измерения, вычислительной технике и исполнительных устройствах и механизмах и предназначенная для обеспечения комплексной автоматизации технологических операций на производстве.

АДМИНИСТРАТОР БЕЗОПАСНОСТИ ИНФОРМАЦИИ – сотрудник или группа сотрудников Службы безопасности информации, осуществляющие контроль за обеспечением защиты информации в ЛВС, а также осуществляющие организацию работ по выявлению и предупреждению возможных каналов утечки информации, потенциальных возможностей осуществления НСД к защищаемой информации.

АУТЕНТИФИКАЦИЯ – проверка принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности субъекта доступа в АСУ ТП).

БАЗОВЫЙ НАБОР МЕР ЗАЩИТЫ ИНФОРМАЦИИ – минимальный набор мер защиты информации, установленный для соответствующего класса защищенности АСУ ТП.

ВЛАДЕЛЕЦ АСУТП – юридическое лицо, осуществляющие деятельность по эксплуатации АСУТП, в том числе по обработке информации, содержащейся в ее базах данных.

ВНЕШНЯЯ ИНФОРМАЦИОННАЯ СИСТЕМА – информационная система, взаимодействующая с АСУ ТП из-за пределов границ АСУ ТП.

ВНЕШНЯЯ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННАЯ СЕТЬ – информационно телекоммуникационная сеть, взаимодействующая с АСУ ТП из-за пределов границ АСУТП.

ВТОРОЙ УРОВЕНЬ – уровень, реализующий функции оперативного (диспетчерского) контроля и управления технологическими объектами, представленный программно-техническими средствами вычислительной техники, предназначенными для накопления, хранения, обработки (обобщения) и представления значительных массивов информации.

ГИПЕРВИЗОР – программа (программное обеспечение), создающая среду функционирования других программ (в том числе других гипервизоров) за счёт имитации аппаратных средств вычислительной техники, управления данными средствами и гостевыми операционными системами, функционирующими в данной среде.

ДЕМИЛИТАРИЗОВАННАЯ ЗОНА АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМ ПРОЦЕССОМ – пограничный сегмент сети автоматизированной системы управления технологическим процессом с внешними по отношению к ней сетями (также известный как защищенная подсеть), выполняющий функции «нейтральной зоны» между указанными сетями.

ДОСТУПНОСТЬ ИНФОРМАЦИИ – состояние информации, характеризующееся способностью автоматизированной системы обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия.

ЗАЩИЩЕННЫЕ ЛИНИИ СВЯЗИ – линии (каналы) связи, при передаче информации по которым обеспечивается требуемый уровень ее защищенности (конфиденциальность, целостность и (или) доступность информации). [Термины и определения настоящего документа]

ИДЕНТИФИКАТОР – уникальный признак субъекта или объекта доступа.

ИДЕНТИФИКАЦИЯ – присвоение субъектам доступа (пользователям, процессам) и объектам доступа (информационным ресурсам, устройствам) идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМ ПРОЦЕССОМ – составная часть безопасности,

отражающая влияние свойств (целостности, доступности, конфиденциальности и др.) информации, обрабатываемой и производимой автоматизированной системы управления технологическим процессом, на безопасность и надежность ее функционирования.

ИНЦИДЕНТ – появление одного или нескольких нежелательных или неожиданных событий информационной безопасности, с которыми связана значительная вероятность компрометации бизнес-операций, нарушения штатного функционирования автоматизированной системы управления технологическим процессом и создания угрозы информационной безопасности.

КОМПЕНСИРУЮЩАЯ МЕРА – мера по защите информации в автоматизированной системе управления технологическим процессом, дополнительно предпринимаемая в связи с практической невозможностью безусловно применить набор мер, формально определенных установленным классом защищенности автоматизированной системы управления технологическим процессом.

КОНТРОЛИРУЕМАЯ ЗОНА – пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, а также транспортных, технических или иных средств.

КОНФИДЕНЦИАЛЬНОСТЬ ИНФОРМАЦИИ – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

МОБИЛЬНЫЙ КОД – несамостоятельное программное обеспечение или компонент программного обеспечения (скрипты, макросы, иные компоненты) получаемые из мест распространения мобильного кода, передаваемые по сети и выполняемые на компонентах АСУ ТП (в местах использования мобильного кода) без предварительной установки (инсталляции) пользователем для расширения возможностей системного и (или) прикладного программного обеспечения.

НАРУШИТЕЛЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ – лицо, которое в результате умышленных или неумышленных действий может нанести ущерб информационным активам, в том числе информационным системам, информационным ресурсам и т.п.

НУЛЕВОЙ УРОВЕНЬ – уровень, реализующий функции получения и первичного преобразования информации о протекании технологических процессов и об оперативном состоянии оборудования, представленный такими устройствами как датчики, приводы арматуры, исполнительные механизмы, УСО и другие КИП и А (включая средства автоматики, встроенные в технологическое оборудование).

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ – реализация комплекса организационных и технических мер по защите информации и систем автоматизации от широкого спектра угроз (в отношении целостности, доступности и конфиденциальности обрабатываемой и хранящейся информации) с целью обеспечения функционирования автоматизированной системы управления технологическим процессом.

ОПЕРАТОР АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМ ПРОЦЕССОМ – работник, основную часть трудовой деятельности которого составляет процесс взаимодействия с технологическим объектом управления, осуществляемый с использованием органов управления и других технических средств автоматизированных систем управления технологическими процессами.

ПЕРВЫЙ УРОВЕНЬ – уровень, реализующий функции регулирования, противоаварийной защиты и блокировок, в аппаратном плане этот уровень представлен ПЛК.

ПЕРИМЕТР АСУ ТП – физическая и (или) логическая граница АСУ ТП (сегмента АСУ ТП), в пределах которой Владелец АСУ ТП обеспечивается защита информации в соответствии с едиными правилами и процедурами, а также контроль за реализованными мерами защиты информации.

ПОЛЬЗОВАТЕЛЬ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМ ПРОЦЕССОМ – работник (администратор (инженер) АСУ ТП, оператор АСУ ТП), который в процессе своей трудовой деятельности в рамках своих

должностных инструкций обращается к средствам вычислительной техники, применяемым в автоматизированных системах управления технологическими процессами, с запросом на выполнение работ.

ПРОГРАММНАЯ СРЕДА – совокупность программного обеспечения, используемого в АСУ ТП для решения одной или нескольких задач.

РАСПРЕДЕЛЕННАЯ СИСТЕМА УПРАВЛЕНИЯ (РСУ) – совокупность территориально и функционально распределённых подсистем с единым информационным пространством, в которой каждая подсистема может использовать параметры и результаты вычислений других подсистем.

РОЛЬ – предопределённая совокупность правил, устанавливающих допустимое взаимодействие между пользователем и АСУ ТП.

СЕГМЕНТ АСУ ТП – совокупность нескольких компонентов АСУ ТП, использующих общую (в том числе разделяемую) среду передачи и объединённых для единства решения функциональных задач.

СИСТЕМА ЗАЩИТЫ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМ ПРОЦЕССОМ – совокупность организационных и технических мер защиты, направленных на блокирование (нейтрализацию) угроз безопасности информации, реализация которых может привести к нарушению штатного режима функционирования автоматизированной системы управления технологическим процессом.

СИСТЕМНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ – программное обеспечение, предназначенное для разработки или обеспечения работы в реальном времени систем сбора, обработки, отображения и архивирования информации об объекте мониторинга или управления (SCADA - системы, специализированное ПО, необходимое для корректной работы данных систем, среды разработки и т.п.).

СОБЫТИЕ БЕЗОПАСНОСТИ (ИНФОРМАЦИОННОЙ) – идентифицированное возникновение состояния АСУ ТП (сегмента, компонента АСУ ТП), сервиса или сети, указывающее на возможное нарушение безопасности информации, или сбой средств защиты информации, или ранее неизвестную ситуацию, которая может быть значимой для безопасности информации.

СУБЪЕКТ ДОСТУПА – пользователь, процесс, выполняющие операции (действия) над объектами доступа и действия которых регламентируются правилами разграничения доступа.

ТЕХНОЛОГИИ МОБИЛЬНОГО КОДА – реализованные в программном обеспечении процессы создания и использования мобильного кода (в частности технологии Java, JavaScript, ActiveX, VBScript).

УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ – совокупность условий и факторов, определяющих потенциальную или реально существующую опасность несанкционированных и (или) непреднамеренных воздействий на технические средства и информацию, обрабатываемую в автоматизированной системе управления технологическим процессом, и способных привести к нарушению штатного режима ее функционирования.

УДАЛЕННЫЙ ДОСТУП – процесс получения доступа (через внешнюю сеть) к объектам доступа АСУ ТП из другой информационной системы (сети) или со средства вычислительной техники, не являющегося постоянно (непосредственно) соединённым физически или логически с АСУ ТП, к которой он получает доступ.

УПРАВЛЕНИЕ ДОСТУПОМ – ограничение и контроль доступа субъектов доступа к объектам доступа в АСУ ТП в соответствии с установленными правилами разграничения доступа.

УЯЗВИМОСТЬ – свойство информационной системы, обуславливающее возможность реализации угроз безопасности, обрабатываемой в ней информации.

ХОСТОВАЯ ОПЕРАЦИОННАЯ СИСТЕМА – операционная система, в среде которой функционирует гипервизор.

ЦЕЛОСТНОСТЬ ИНФОРМАЦИИ – свойство безопасности информации, при котором отсутствует любое ее изменение либо изменение субъектами доступа, имеющими на него право.

2. СОКРАЩЕНИЯ

АВЗ	–	Антивирусная защита
АНЗ	–	Контроль (анализ) защищенности информации
АРМ	–	Автоматизированное рабочее место
АСО	–	Активное сетевое оборудование
АСУ ТП	–	Автоматизированная система управления технологическим процессом
ВИ	–	Виртуальная инфраструктура
ДНС	–	Обеспечение действий в нештатных (непредвиденных) ситуациях
ЗИС	–	Защита автоматизированной системы и ее компонентов
ЗНИ	–	Защита машинных носителей информации
ЗСВ	–	Защита среды виртуализации
ИАФ	–	Идентификация и аутентификация субъектов доступа и объектов доступа
ИБП	–	Источник бесперебойного питания
МЭ	–	Межсетевой экран
ОДТ	–	Обеспечение доступности
ОПС	–	Ограничение программной среды
ОС	–	Операционная система
ОЦЛ	–	Обеспечение целостности
РСБ	–	Регистрация событий безопасности
СЗ	–	Система защиты
СОВ	–	Система обнаружения вторжений
СПО	–	Системное программное обеспечение АСУ ТП
СрЗИ	–	Средство защиты информации
УКФ	–	Управление конфигурацией автоматизированной системы управления и ее системы защиты
УПД	–	Управление доступом субъектов доступа к объектам доступа
SCADA	–	Диспетчерское управление и сбор данных.

3. ОБЩИЕ ПОЛОЖЕНИЯ

Защита информации в автоматизированной системе управления технологическими процессами является составной частью работ по созданию (модернизации) и эксплуатации АСУ ТП и должна обеспечиваться на всех стадиях ее жизненного цикла.

Принимаемые организационные и технические меры защиты информации:

–должны обеспечивать доступность обрабатываемой в автоматизированной системе управления информации (исключение неправомерного блокирования информации), ее целостность (исключение неправомерного уничтожения, модифицирования информации), а также, при необходимости, конфиденциальность (исключение неправомерного доступа, копирования, предоставления или распространения информации);

–должны соотноситься с мерами по промышленной, физической, пожарной, экологической, радиационной безопасности, иными мерами по обеспечению безопасности автоматизированной системы управления и управляемого (контролируемого) объекта и/или технологического процесса;

–не должны оказывать отрицательного влияния на штатный режим функционирования автоматизированной системы управления.

Требования к обеспечению информационной безопасности в АСУ ТП определяются в зависимости от класса защищенности автоматизированной системы управления, а также в соответствии со следующими нормативными документами:

–Приказ ФСТЭК России № 31 от 14.03.2014 г. «Об утверждении Требований 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»;

– Политика Компании «Концепция информационно-технической безопасности ПАО «НК «Роснефть» № ПЗ-11.1»;

– Положение Компании «Информационная безопасность. Автоматизированные системы управления технологическими процессами» ПАО НК Роснефть № ПЗ-11 Р-0012;

– Положение Компании «Требования к защите локальных вычислительных сетей Компании, подключаемых в единую корпоративную телекоммуникационную систему ПАО «НК «Роснефть» № ПЗ-11.01 Р-0123.

4. КЛАСС ЗАЩИЩЁННОСТИ АСУ ТП

В соответствии с положениями приказа ФСТЭК России № 31 от 14.03.2014 г. АСУ ТП присвоен класс защищённости *«указать класс защищённости АСУ ТП»*

5. ТРЕБОВАНИЯ К ТЕХНИЧЕСКИМ МЕРАМ ЗАЩИТЫ ИНФОРМАЦИИ В АСУ ТП

Настоящие требования к техническим мерам защиты информации в АСУ ТП предъявляются к комплексу программно-технических средств второго уровня АСУ ТП, обеспечивающему доступ к информации, обрабатываемой в АСУ ТП.

Базовый набор технических мер защиты информации¹ для АСУ ТП с учётом присвоенного класса защищённости (п.4.), включает:

ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ СУБЪЕКТОВ ДОСТУПА И ОБЪЕКТОВ ДОСТУПА

(ИАФ.1, ИАФ.2², ИАФ.3, ИАФ.4, ИАФ.5, ИАФ.6)

Данные меры должны быть реализованы за счёт использования встроенных в системное программное обеспечение АСУ ТП (СПО), операционную систему (ОС), BIOS механизмов защиты информации, средств антивирусной защиты (АВЗ), активного сетевого оборудования (АСО) и средств межсетевого экранирования (МЭ).

Примечание: Учётные данные, используемые в АСУ ТП и её СРЗИ, должны создаваться в соответствии с требованиями локально-нормативных документов Компании в области обеспечения защиты информации в АСУ ТП. Механизмы идентификации и аутентификации СПО, ОС, АСО, АВЗ, МЭ должны обладать следующими функциональными характеристиками:

– возможность задания произвольной длины пароля, состоящего из цифро-буквенных символов верхнего и нижнего регистра, а также специальных символов;

– возможность ограничения срока действия пароля;

– возможность запрета повторного использования пароля;

– возможность уведомления пользователя АСУ ТП о необходимости смены пароля;

– хранение паролей доступа в АСУ ТП в защищенном виде;

– ограничение неуспешных попыток входа в АСУ ТП;

– при смене пароля;

– возможность двойного подтверждения при самостоятельной смене пароля;

– возможность автоматического сброса поля ввода после каждой проверки введенного пароля.

Должна быть реализована возможность изменения паролей, создаваемых по умолчанию, в том числе к системным учетным записям.

УПРАВЛЕНИЕ ДОСТУПОМ СУБЪЕКТОВ ДОСТУПА К ОБЪЕКТАМ ДОСТУПА

(УПД.1, УПД.2, УПД.3, УПД.4, УПД.5, УПД.6, УПД.11, УПД.13, УПД.14, УПД.15, УПД.16)

Данные меры должны быть реализованы за счёт использования встроенных в СПО, ОС механизмов защиты информации, средств антивирусной защиты (АВЗ), активного сетевого оборудования (АСО) и средств межсетевого экранирования (МЭ).

Примечание: При реализации доступа работников к компонентам АСУ ТП необходимо наличие:

- возможности настройки минимально необходимых полномочий для решения производственных задач;
- возможности отключения всех дополнительных прав работников и функционала систем;
- возможности настройки права доступа на уровне модулей СПО АСУ ТП;
- возможности настройки права доступа на уровне баз данных АСУ ТП;
- возможности настройки права доступа на уровне операционных систем серверов управления и АРМ.

При предоставлении прав и привилегий по доступу к компонентам АСУ ТП:

- возможность разделять права таким образом, чтобы у одного лица не было полного контроля над всеми компонентами АСУ ТП;
- исключение неконтролируемого совершения операций в АСУ ТП другими лицами;
- возможность управления доступом на уровне ролей. При этом минимальный набор ролей на уровне СПО АСУ ТП должен включать:
- роль, реализующую функции администратора АСУ ТП, включающие внесение изменений в состав и конфигурацию АСУ ТП, установку и инициализацию модулей ПО, создание учетных записей работников и управление правами доступа;
- роль, реализующую функции оператора АСУ ТП, включающие осуществление задач по контролю и управлению технологическим процессом, без возможностей внесения изменений в состав и конфигурацию компонентов АСУ ТП.

ОГРАНИЧЕНИЕ ПРОГРАММНОЙ СРЕДЫ

(ОПС.1³, ОПС. 2², ОПС.3)

Данные меры должны быть реализованы за счёт использования встроенных в СПО и ОС механизмов защиты информации.

Примечание: Для АСУ ТП должен быть определен и документирован перечень ПО, устанавливаемого на АРМ и серверы, входящие в ее состав. В состав ПО АСУ ТП должны входить только те программные средства и модули, которые необходимы для реализации функций АСУ ТП на конкретном АРМ или сервере с учетом решаемых ими задач, а также применяемые в целях обеспечения ИБ программные средства и модули. Применяемые программные средства должны отвечать следующим условиям:

- являться официальной версией разработчика/вендора ПО;
- иметь официальное подтверждение совместимости (прикладных систем с общесистемным ПО) от разработчика/вендора, либо иметь документально подтвержденное заключение об успешных испытаниях на совместимость от поставщиков АСУ ТП;
- отвечать требованиям по лицензионной чистоте, не нарушать чьи-либо права интеллектуальной собственности;
- иметь комплект эксплуатационной документации, включая руководства пользователя (оператора) и администратора.

ЗАЩИТА МАШИННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ

(ЗНИ.1, ЗНИ.2, ЗНИ.5², ЗНИ.6³, ЗНИ.7)

Данные меры должны быть реализованы за счёт использования встроенных в ОС, BIOS механизмов защиты информации, средств антивирусной защиты (АВЗ).

Примечание: В BIOS АРМ операторов и инженерных станций АСУ ТП, серверов управления АСУ ТП должна быть запрещена загрузка операционных систем с иных носителей, кроме жесткого диска компьютеров и серверов.

При отсутствии производственной необходимости все интерфейсы и устройства ввода-вывода на съемные носители, включая порты USB, IEEE 1394, порты карт памяти, устройства чтения и записи на оптические и магнитные диски должны быть отключены, а возможность чтения/записи с/на съемные носители должна быть заблокирована с использованием механизмов защиты ОС или АВЗ.

Все факты использования съемных носителей информации, с указанием совершенных операций (чтения/записи с/на носитель) должны регистрироваться в соответствующих системных журналах.

РЕГИСТРАЦИЯ СОБЫТИЙ БЕЗОПАСНОСТИ

(РСБ.1, РСБ.3, РСБ.4, РСБ.5, РСБ.6², РСБ.7)

Данные меры должны быть реализованы за счёт использования встроенных в СПО, ОС, активное сетевое оборудование (АСО) механизмов защиты информации, АВЗ и МЭ.

Примечание: Механизмы регистрации событий СПО, ОС, АСО, АВЗ, МЭ должны обеспечивать:

- хранение журналов событий сроком не менее 1 года со дня фиксации последнего события;
- регистрацию входа/выхода пользователей, включая неуспешные попытки доступа, с указанием идентификатора пользователя, даты и времени события;
- регистрацию событий создания, удаления, изменения привилегий пользователей;
- регистрацию действий операторов АСУ ТП, администраторов АСУ ТП, по внесению изменений в конфигурацию и настройки АСУ ТП, формирование команд и операций в АСУ ТП, операции с журналами регистрации;
- регистрацию совершаемых технологических операций в АСУ ТП и параметры операций, включая дату и время совершения операции и иные параметры (например, идентификаторы оборудования, количественные характеристики операции/транзакции (объем, масса, скорость потока и т.п.), физические параметры – температура, плотность, давление и т.п.);
- регистрацию системных ошибок;
- регистрацию изменения параметров конфигурации ПО, состава компонентов АСУ ТП, установки/удаления программ и обновлений;
- регистрацию запуска/остановки событий и процессов, запуска/остановки особых режимов работы ПО и оборудования АСУ ТП;
- регистрацию доступ к объектам АСУ ТП – файлам конфигурации, файлам данных, файлам журналов регистрации.
- регистрацию доступа администраторов к активному сетевому оборудованию;
- регистрацию действия администраторов, включая внесение изменений в конфигурации активного сетевого оборудования;
- регистрацию установки обновлений программной части активного сетевого оборудования;
- регистрацию ошибок и сбоев в работе активного сетевого оборудования;
- регистрацию сетевых событий, такие как результат попытки установления соединения, результаты аутентификации, включение и отключение каналов связи и пр.
- регистрация всех действий по созданию учетных записей (идентификаторов), присвоения и изменения прав доступа к компонентам АСУ ТП в журналах событий АСУ ТП.

АНТИВИРУСНАЯ ЗАЩИТА

(АВЗ.1 , АВЗ.2)

Данные меры должны быть реализованы за счёт использования средств АВЗ и МЭ.

Примечание: Антивирусная защита:

- должна быть реализована на уровне файловой системы АРМ и серверов АСУ ТП, а также МЭ (в случае его применения);
- должны применяться средства АВЗ не ниже 5 класса защищённости по классификации ФСТЭК России;
- средства АВЗ должны поставляться исходя из количественного состава технических средств АСУ ТП, на которых предполагается их применение, с лицензиями на срок эксплуатации АСУ ТП.
- должны применяться следующие средства АВЗ по классификации ФСТЭК России:
 - а) в автоматизированных системах управления 1 класса защищённости - средства антивирусной защиты не ниже 3 класса защиты;
 - б) в автоматизированных системах управления 2 класса защищённости - средства антивирусной защиты не ниже 4 класса защиты;
 - в) в автоматизированных системах управления 3 класса защищённости - средства антивирусной защиты не ниже 5 класса защиты;
- Средства антивирусной защиты должны обладать возможностью отключения автоматического обновления и сканирования.

Для всех применяемых на АРМ и серверах АСУ ТП (коммутационные серверы, SCADA-системы, серверы приложений и баз данных) антивирусных средств обязательно официальное подтверждение поставщиком АСУ ТП и/или организацией, осуществляющей внедрение, техническую поддержку и/или сопровождение АСУ ТП, программной совместимости с СПО АСУ ТП.

СИСТЕМА ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

(COB.0³, COB.1³, COB.2³)

Данные меры должны быть реализованы за счёт использования встроенных механизмов защиты МЭ и АВЗ.

Примечание: Реализуется средствами Межсетевого экранирования. Подробные технические характеристики указаны в Разделе 6.

КОНТРОЛЬ (АНАЛИЗ) ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ

(АНЗ.2, АНЗ.4, АНЗ.5²)

Данные меры должны быть реализованы за счёт использования встроенных в СПО, ОС механизмов защиты информации, средств антивирусной защиты (АВЗ) и средств межсетевого экранирования (МЭ).

Примечание: Обновления версий и баз данных средств защиты АСУ ТП, СПО должны производиться в соответствии с соответствующими инструкциями, поставляемыми исполнителем вместе со средствами защиты.

ОБЕСПЕЧЕНИЕ ЦЕЛОСТНОСТИ

(ОЦЛ.1², ОЦЛ.3, ОЦЛ.6³, ОЦЛ.7², ОЦЛ.8²)

Данные меры должны быть реализованы за счёт использования встроенных в СПО, ОС механизмов защиты информации.

Примечание: В АСУ ТП и её СрЗИ должна быть реализована возможность контроля целостности ПО, включая их обновления, с использованием контрольных сумм, хэш-функции или электронной подписи в процессе загрузки или динамически в процессе работы АСУ ТП.

Использование автоматизированных средств контроля состава и целостности ПО, при их наличии, не должно каким-либо образом влиять на работу ПО (блокировать или останавливать работу программ, удалять файлы), только регистрировать факт нарушения с указанием названия измененного программного модуля или не вошедшего в перечень разрешенного ПО.

ОБЕСПЕЧЕНИЕ ДОСТУПНОСТИ

(ОДТ.1², ОДТ.2², ОДТ.3², ОДТ.4, ОДТ.5)

Данные меры должны быть реализованы за счёт использования встроенных в СПО, ОС механизмов защиты информации, МЭ.

Примечание: МЭ должны обладать возможностью конфигурирования в отказоустойчивом кластере. Средства защиты информации АСУ ТП должны обладать функциональной возможностью выполнения резервного копирования с сохранением резервных копий на машинные носители информации.

Резервному копированию подлежат:

– файлы и базы данных АСУ ТП - не реже одного раза в неделю; – электронные журналы регистрации событий АСУ ТП - не реже одного раза в неделю;

– конфигурационные файлы компонентов АСУ ТП и средств защиты информации АСУ ТП – при каждом внесении изменений в конфигурационные настройки АСУ ТП и её средств защиты, но не реже одного раза в месяц;

– образы системных жестких дисков АРМ и серверов АСУ ТП - не реже одного раза в месяц (неделя, в случае использования виртуальной инфраструктуры);

– должна быть обеспечена возможность просмотра / восстановления данных из резервных копий.

ЗАЩИТА СРЕДЫ ВИРТУАЛИЗАЦИИ

(ЗСВ.1, ЗСВ.2, ЗСВ.3, ЗСВ.4², ЗСВ.6², ЗСВ.7², ЗСВ.8³, ЗСВ.9, ЗСВ.10²)

Данные меры должны быть реализованы за счёт использования встроенных в СПО, ОС, механизмов защиты, АВЗ, МЭ.

Примечание: СрЗИ в АСУТП должны обеспечивать идентификацию и аутентификацию субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации, в соответствии с ИАФ.1, ИАФ.2, ИАФ.3, ИАФ.4, ИАФ.5, ИАФ.6, с учётом требований к функциональным возможностям СрЗИ в автоматизированных системах управления предъявляемыми для ИАФ.

СрЗИ в АСУТП должны обеспечивать управление доступом субъектов доступа к объектам доступа, в том числе внутри виртуальных машин, в соответствии с УПД.1, УПД.2, УПД.4, УПД.5, УПД.6, УПД.11, УПД.13, а также требованиями к функциональным возможностям СрЗИ в автоматизированных системах управления предъявляемыми для УПД.

СрЗИ в АСУТП должны обеспечивать регистрацию событий безопасности в виртуальной инфраструктуре в соответствии с РСБ.1, РСБ.3, РСБ.4 и РСБ.5, а также требованиям к функциональным возможностям СрЗИ в автоматизированных системах РСБ.

СрЗИ в АСУТП должны обеспечивать управление потоками информации между компонентами виртуальной инфраструктуры и по периметру виртуальной инфраструктуры в соответствии с УПД.3, ЗИС.3.

СрЗИ в АСУТП должны обеспечивать контроль целостности компонентов виртуальной инфраструктуры в соответствии с ОЦЛ.1.

СрЗИ в АСУТП должны обеспечивать резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры и каналов связи внутри виртуальной инфраструктуры в соответствии с ОДТ.2, ОДТ.4, ОДТ.5, а также требованиям к функциональным возможностям СрЗИ в автоматизированных системах управления предъявляемыми для ОДТ.

СрЗИ в АСУТП должны обеспечивать реализацию и управление антивирусной защитой в виртуальной инфраструктуре в соответствии с АВЗ.1, АВЗ.2.

СрЗИ в АСУТП должны обеспечивать разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей в соответствии с ЗИС.17.

В рамках одного физического хоста ВИ запрещается разворачивать более одной АСУТП.

УПРАВЛЕНИЕ ОБНОВЛЕНИЯМИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

(ОПО.0, ОПО.1, ОПО.2)

Данные меры должны быть реализованы за счёт использования встроенных в СПО, ОС механизмов защиты информации, АВЗ и МЭ.

Примечание: В комплект поставки АСУТП должны входить инструкции по обновлению ОС, СПО, средств АВЗ и средств МЭ, а также регламенты (инструкции) по установке обновлений ОС и СПО от разработчика АСУТП.

ЗАЩИТА АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ И ЕЕ КОМПОНЕНТОВ

(ЗИС.1, ЗИС.3, ЗИС.7², ЗИС.11², ЗИС.15², ЗИС.17, ЗИС.20, ЗИС.22, ЗИС.23, ЗИС.30)

Данные меры должны быть реализованы за счёт использования встроенных в СПО, ОС механизмов защиты информации, АВЗ и МЭ.

Примечание: В АСУТП и её СрЗИ должна быть реализована возможность локального, либо с использованием защищенных протоколов сетевого взаимодействия администрирования и конфигурирования компонентов сетевой инфраструктуры АСУТП. Административный доступ должен быть разрешен только с сетевых адресов, специально выделенных для этого административных консолей.

Для снижения сложности администрирования при разграничении доступа к компонентам АСУТП необходима возможность реализации доступа, основанном на ролевом подходе.

При применении в технологических сетях АСУ ТП систем беспроводной связи должно обеспечиваться:

- выделение беспроводных сетей связи в отдельный сетевой сегмент с обеспечением его защиты с использованием МЭ;
- аутентификация беспроводных устройств при доступе к беспроводной сети с использованием криптографических алгоритмов;
- шифрование данных в каналах связи беспроводной сети с использованием криптографических алгоритмов.

ОБЕСПЕЧЕНИЕ ДЕЙСТВИЙ В НЕШТАТНЫХ (НЕПРЕДВИДЕННЫХ) СИТУАЦИЯХ (ДНС.4², DNS.5)

Данные меры должны быть реализованы за счёт использования встроенных в СПО, ОС механизмов защиты информации, МЭ.

Примечание: В дополнение к указанным мерам защиты информации для обеспечения действий в нештатных (непредвиденных) ситуациях (ДНС) необходимо учитывать меры защиты информации и обязательные дополнительные функциональные возможности АСУ ТП и её СрЗИ для обеспечения доступности (ОДТ).

УПРАВЛЕНИЕ КОНФИГУРАЦИЕЙ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ И ЕЕ СИСТЕМЫ ЗАЩИТЫ (УКФ.2)

Данные меры должны быть реализованы за счёт использования встроенных в СПО, ОС механизмов защиты информации, АВЗ и МЭ.

Примечание: Встроенные механизмы защиты СПО, ОС, АВЗ и МЭ должны обладать возможностями:

- санкционирования внесения изменений в базовую конфигурацию АСУ ТП и ее системы защиты;
- регистрации действий по внесению изменений в базовую конфигурацию АСУ ТП и ее системы защиты;
- сохранения данных об изменениях базовой конфигурации АСУ ТП и ее системы защиты;
- контроль действий по внесению изменений в базовую конфигурацию АСУ ТП и ее системы защиты.

В случае невозможности использования в АСУ ТП указанных выше средств защиты информации (встроенных механизмов защиты СПО, ОС, BIOS, АСО, и АВЗ, МЭ), для обеспечения требуемого уровня безопасности с учётом присвоенного класса защищённости АСУ ТП (см. п. 4) и реализации мер защиты информации, указанных в настоящем разделе, Исполнителем должны быть предложены иные средства защиты информации, с представлением документального обоснования их применимости, либо разработаны компенсирующие меры с документальным обоснованием их возможного применения, в виде разработанной модели угроз информационной безопасности АСУ ТП.

¹ Обозначение и наименование мер защиты даны в соответствии с Приложением 2 к приказу ФСТЭК России № 31 от 14.03.2014 г.

² Мера защиты информации применяемая в автоматизированных системах управления класса защищённости К2 и К1

³ Мера защиты информации применяемая в автоматизированных системах управления класса защищённости К1

6. ТРЕБОВАНИЯ К ТЕХНИЧЕСКОМУ ОБЕСПЕЧЕНИЮ АСУ ТП И СРЕДСТВАМ ЗАЩИТЫ ИНФОРМАЦИИ (РЕКОМЕНДУЕМЫЕ)

МАШИННЫЕ НОСИТЕЛИ ИНФОРМАЦИИ

Машинные носители информации, используемые для хранения резервных копий должны удовлетворять следующим техническим характеристикам:

- иметь ёмкость не менее 1000 ГБ (1 ТБ) для резервных копий баз данных, журналов событий, образов системных дисков АРМ и серверов АСУТП;
- иметь ёмкость не менее 100 ГБ для резервных копий конфигурационных файлов СПО АСУТП, активного коммутационного оборудования, средств АВЗ и средств МЭ.

СРЕДСТВА МЕЖСЕТЕВОГО ЭКРАНИРОВАНИЯ

Средства межсетевого экранирования должны удовлетворять следующим техническим характеристикам:

- базовая конфигурация: 4 порта 10/100/1000Base-T RJ45/250Gb/220V;
- сетевые подключения: IPv4/ 1024 интерфейса или VLANs/Layer 2 (прозрачный) и Layer 3 (маршрутизации) режим;
- межсетевое экранирование (FW) и NAT;
- VPN и туннелирование;
- контроль на прикладном уровне (Application Control) на стыке корпоративной сети и сети АСУТП;
- фильтрацию URL (URL filtering)
- механизмы защиты: Firewall/Antivirus/IDS;
- должно быть предусмотрено резервирование средств МЭ на стыке корпоративной сети и сети АСУТП.

Применяемый МЭ должен выполнять следующие основные функции:

- обеспечение фильтрации входящего и исходящего сетевого трафика на сетевом, транспортном и прикладном уровнях на основе заданных правил фильтрации;
- регистрация и учет фильтруемых входящих и исходящих пакетов (данных) коммуникационных протоколов сетевого уровня с указанием атрибутов фильтруемых пакетов, времени, результата фильтрации и др.;
- идентификация и аутентификация входящих и исходящих запросов на установление соединений (протокольных блоков данных коммуникационных протоколов транспортного уровня);
- фильтрация запросов на установление соединений на основе заданных правил фильтрации;
- регистрация и учет фильтруемых входящих и исходящих запросов на установление соединений с указанием атрибутов фильтруемых пакетов, времени, результата фильтрации и др.;
- обеспечение трансляции на транспортном и прикладном уровнях (прокси) для определенных протоколов;
- регистрация и учет попыток нарушения заданных в МЭ правил фильтрации;
- идентификация и аутентификация инженера по эксплуатации СЗИ при попытке доступа к МЭ;
- регистрация и учет входа/выхода инженера по эксплуатации СЗИ в систему/из системы МЭ с указанием атрибутов субъекта, результата регистрируемого события и др.;
- контроль и анализ легитимности действий, выполняемых с административными полномочиями;
- контроль целостности программной части МЭ;
- фильтрация вредоносного ПО;
- блокирование внешних атак.

Для защиты сетевой инфраструктуры АСУ ТП от несанкционированного доступа на периметре технологической сети обязательно применение МЭ, сертифицированных по требованиям безопасности информации.

В АСУ ТП класса защищенности К1:

–МЭ не ниже 3 класса в случае взаимодействия АСУ ТП с информационно-телекоммуникационными сетями международного информационного обмена и не ниже 4 класса в случае отсутствия такого взаимодействия;

–В АСУ ТП класса защищенности К2:

–МЭ не ниже 3 класса в случае взаимодействия АСУ ТП с информационно-телекоммуникационными сетями международного информационного обмена и не ниже 4 класса в случае отсутствия такого взаимодействия;

–В АСУ ТП класса защищенности К3 применяются:

–МЭ не ниже 4 класса.

СРЕДСТВА АСО

Средства АСО, применяемые для защиты на втором уровне АСУ ТП, должны удовлетворять следующим техническим и функциональным характеристикам:

–интерфейсы:

• 10/100/1000Base-T количество портов на коммутаторе выбирается исходя из потребностей работы АСУ ТП, с учётом наличия не менее 50% свободных портов от числа использованных для возможности расширения АСУ ТП;

• 10/100/1000Base-T/SFP не менее 2 портов;

–VLAN:

• группы VLAN;

• 802.1Q Tagged VLAN;

• VLAN на основе порта;

• 802.1v Protocol VLAN;

• VLAN на основе MAC-адресов;

• VLAN Trunking;

–безопасность:

• SSH v2;

• SSL v1/v2/v3;

• Port Security;

• привязка IP-MAC-Port;

• защита от широковещательного/многоадресного/одноадресного шторма;

• сегментация трафика.

ИБП

Все активное серверное и сетевое оборудование должно обеспечиваться источниками бесперебойного питания (ИБП). ИБП должны обладать следующими техническими и функциональными характеристиками:

–выходное напряжение – 220 В±10% переменного тока;

–в случае сбоя постоянного источника электропитания должен обеспечить работоспособность технических средств защиты АСУ ТП по времени не менее 20 минут;

–должна быть предусмотрена предупредительная сигнализация о необходимости замены аккумулятора;

–должна быть предусмотрена визуальная и звуковая сигнализация нештатного состояния;

–должен быть предусмотрен механизм автоматического включения зарядного устройства ИБП при восстановлении подачи электроснабжения;

–должна быть предусмотрена возможность установки, при необходимости, дополнительных аккумуляторов;

–должна быть предусмотрена возможность контроля и управления ИБП через ЛВС с использованием стандартного протокола SNMP;

При выборе средств МЭ, средств активного сетевого оборудования и АВЗ следует учитывать рекомендованные разработчиками АСУ ТП (обязательное требование) технические и программные средства защиты, а также средства защиты, которые применяются в Обществе (рекомендательное требование).

Программно-технические средства защиты информации в АСУТП должны обладать следующими возможностями:

–Отключение всех служб и сервисов на АРМ и серверах управления АСУ ТП, не используемых в процессе эксплуатации и сопровождения АСУ ТП (при наличии технической возможности). При необходимости данные службы, сервисы и функции должны иметь возможность включения на определенный период времени в соответствии с требованиями по управлению конфигурацией АСУ ТП;

–Все коммуникационные порты, порты ввода-вывода и интерфейсы на оборудовании АСУ ТП, включая АРМ, серверы управления, коммуникационное оборудование, не используемые в процессе эксплуатации и сопровождения АСУ ТП, должны иметь возможность отключения или блокировки;

–В BIOS АРМ операторов и инженерных станций АСУ ТП, серверов управления АСУ ТП должна быть возможность запрета загрузки операционных систем с иных носителей, кроме жесткого диска компьютеров и серверов;

–Конфигурация параметров АСУ ТП должна быть документирована. Эксплуатационная документация на АСУ ТП и её средства защиты, а также инструкции, которые поставляются вместе с техническими средствами АСУ ТП, должны содержать перечень и эталонные значения конфигурационных параметров компонентов АСУ ТП, в том числе технических защитных мер.