

ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АСУТП

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Автоматизированная система управления технологическим процессом (АСУ ТП) — комплекс программных и технических средств, предназначенных для контроля и управления технологическим оборудованием и связанными с ним процессами.

Идентификация — присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Аутентификация — проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности.

Персональная учетная запись — уникальный идентификатор, закрепленный за конкретным физическим лицом, исключающий коллективное использование одних и тех же реквизитов доступа.

Программируемый логический контроллер (ПЛК) — микропроцессорное устройство, предназначенное для сбора данных, логической обработки и управления исполнительными механизмами на технологическом уровне.

Межсетевой экран (МЭ) — средство защиты, осуществляющее контроль и фильтрацию сетевого трафика в соответствии с заданными правилами безопасности.

Целостность информации — состояние информации, при котором отсутствует любое ее несанкционированное изменение.

Доступность информации — состояние информации, при котором субъекты, имеющие права доступа, могут беспрепятственно получать и использовать её.

Контролируемая зона — пространство, в котором исключено неконтролируемое пребывание лиц, не имеющих допуска.

Нештатная ситуация — отклонение в работе АСУ ТП от нормального режима, вызванное техническим сбоем, ошибкой персонала или внешним воздействием.

Регламент (инструкция) — организационный документ, устанавливающий обязательный порядок выполнения действий по обеспечению безопасности и эксплуатации системы.

2. СОКРАЩЕНИЯ

АВЗ — антивирусная защита;
АРМ — автоматизированное рабочее место;
АСО — Активное сетевое оборудование;
АСУ ТП — автоматизированная система управления технологическим процессом;
АУД — аудит безопасности;
БД — база данных;
ДНС — обеспечение действий в нештатных ситуациях;
ЗНИ — защита машинных носителей информации;
ЗИС — защита сетевого взаимодействия;
ЗТС — защита технических средств и систем;
ИАФ — идентификация и аутентификация;
ИНЦ — реагирование на компьютерные инциденты;
МЭ — межсетевой экран;
ОДТ — обеспечение доступности;
ОПО — управление обновлениями программного обеспечения;
ОС — операционная система;
ОЦЛ — обеспечение целостности;
ПЛК — программируемый логический контроллер;
ПЛН — планирование мероприятий по обеспечению защиты информации;
ПО — программное обеспечение;
СПО — системное программное обеспечение;
ТЗ — техническое задание;
УКФ — управление конфигурацией;
УПД — управление доступом;
ФСТЭК России — Федеральная служба по техническому и экспортному контролю;
DMZ — демилитаризованная зона;
UTM — универсальный шлюз безопасности;
VPN — виртуальная частная сеть.

3. ОБЩИЕ ПОЛОЖЕНИЯ

Защита информации в АСУ ТП является составной частью работ по созданию (модернизации) и эксплуатации системы и обеспечивается на всех стадиях ее жизненного цикла.

Принимаемые организационные и технические меры защиты информации:

- должны обеспечивать доступность и целостность обрабатываемой информации, а также ее конфиденциальность (в случаях, установленных проектной документацией);
- должны быть интегрированы с мерами по промышленной, физической и пожарной безопасности и не должны препятствовать выполнению требований по обеспечению безопасности технологического процесса;
- не должны оказывать отрицательного влияния на штатный режим функционирования, надежность и отказоустойчивость АСУ ТП.

Требования к обеспечению защиты информации определяются в соответствии со следующими нормативными документами:

- Приказ ФСТЭК России от 14 марта 2014 г. № 31 «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».

4. ТРЕБОВАНИЯ К МЕРАМ ЗАЩИТЫ ИНФОРМАЦИИ В АСУ ТП

Настоящие требования предъявляются к комплексу программно-технических средств всех уровней АСУ ТП, а также к организационному обеспечению процессов эксплуатации системы.

Набор мер защиты информации для АСУ ТП с учётом присвоенного класса защищённости «3» включает:

ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ СУБЪЕКТОВ ДОСТУПА И ОБЪЕКТОВ ДОСТУПА

(ИАФ.0, ИАФ.1, ИАФ.2, ИАФ.3, ИАФ.4, ИАФ.5, ИАФ.7)

Должен быть реализован комплекс мер, обеспечивающий строгое разграничение доступа к компонентам АСУ ТП за счет:

1. Документальное оформление (ИАФ.0): Разработка регламента (политики), определяющего правила назначения прав, требования к сложности паролей и порядок действий при компрометации учетных записей.
2. Идентификация и аутентификация пользователей, управление их идентификаторами и средствами аутентификации (ИАФ.1, ИАФ.3, ИАФ.4): Обеспечения реализации создания персональных учетных записей для каждого пользователя и процесса с использованием отечественного сертифицированного программного обеспечения (в том числе служб каталогов и систем управления доступом, включенных в реестр российского ПО) или сертифицированных встроенных механизмов защиты СПО. Использование общих (групповых) учетных записей не допускается. Механизмы должны поддерживать блокировку при переборе паролей и контроль срока их действия.
3. Контроля оборудования (ИАФ.2): Технического ограничения возможности подключения к сети АСУ ТП сторонних устройств (привязка по MAC-адресам, использование сертификатов или блокировка неиспользуемых портов).
4. Безопасного внешнего доступа (ИАФ.5): Обеспечения однозначной идентификации внешних пользователей и ограничения удаленного доступа к компонентам АСУ ТП только для авторизованных лиц.
5. Криптографической защиты (ИАФ.7): Использования защищенных протоколов передачи данных, исключающих передачу аутентификационной информации в открытом виде внутри промышленного сегмента и за его пределами.

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

УПРАВЛЕНИЕ ДОСТУПОМ

(УПД.0, УПД.1, УПД.2, УПД.4, УПД.5, УПД.6, УПД.10, УПД.11, УПД. 13, УПД. 14)

Должен быть реализован комплекс мер, для системы управления доступом, исключающих несанкционированные действия пользователей и внешних систем в контуре АСУ ТП:

1. Документальное оформление (УПД.0): Разработка политики управления доступом, определяющей роли, права и обязанности персонала, а также процедуры пересмотра прав доступа.
2. Управление полномочиями и ролями (УПД.1, УПД.2, УПД.4, УПД.5):
Использования отечественного сертифицированного ПО (служб каталогов, систем управления доступом) для создания учетных записей (УПД.1) и реализации ролевой модели доступа. Права должны назначаться исходя из принципа «минимально необходимых привилегий» (УПД.5) для каждой роли (УПД.4), обеспечивая физическое и логическое разграничение доступа к ресурсам (УПД.2).
3. Контроль сеансов и попыток доступа (УПД.6, УПД.10, УПД.11): Настройки механизмов блокировки доступа при превышении заданного числа неуспешных попыток входа (УПД.6), автоматического блокирования сеанса при неактивности пользователя (УПД.10) и жесткого ограничения перечня разрешенных действий в системе до момента успешного прохождения аутентификации (УПД.11).
4. Безопасное взаимодействие (УПД.13, УПД.14): Применения межсетевых экранов и криптографических шлюзов на базе отечественного сертифицированного ПО для реализации защищенного удаленного доступа (УПД.13), а также механизмов фильтрации и контроля трафика при взаимодействии с внешними информационными системами (УПД.14).

Примечание: должен быть реализован регламент управления доступом и актуальная матрица доступа, описывающая права каждой роли (администратор, инженер, оператор) ко всем компонентам АСУ ТП

ЗАЩИТА МАШИННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ

(ЗНИ.0, ЗНИ.1, ЗНИ.2, ЗНИ.5, ЗНИ.7, ЗНИ.8)

В проекте должны быть предусмотрены технические средства и организационные процедуры, обеспечивающие защиту информации на съемных носителях и контроль интерфейсов ввода-вывода. Указанные меры реализуются путем применения:

1. Разработка политики защиты машинных носителей информации (ЗНИ.0): создание регламента, определяющего зоны ответственности, правила использования носителей в АСУ ТП и порядок действий персонала.
2. Учет машинных носителей информации (ЗНИ.1): разработка форм реестров (журналов) и порядка присвоения уникальных идентификаторов (маркировки) для обеспечения прослеживаемости носителей.
3. Управление физическим доступом к машинным носителям информации (ЗНИ.2): определение требований к местам безопасного хранения (сейфам, шкафам) и разработка процедур контроля доступа к ним в нерабочее время.
4. Контроль использования интерфейсов ввода (вывода) и подключения машинных носителей информации (ЗНИ.5, ЗНИ.7): внедрение и настройка отечественного сертифицированного ПО для программного управления портами, а также физическое ограничение (блокировка) доступа к неиспользуемым интерфейсам на уровне аппаратного обеспечения (BIOS/UEFI, опломбирование портов или установка механических блокираторов).
5. Уничтожение (стирание) информации на машинных носителях информации (ЗНИ.8): поставка и настройка отечественного сертифицированного ПО для гарантированного удаления данных, а также разработка инструкции по выводу носителей из эксплуатации.

Примечание: должны быть реализованы утвержденные формы журналов учета машинных носителей, инструкции по маркировке носителей и регламент гарантированного уничтожения информации».

АУДИТ БЕЗОПАСНОСТИ

(АУД.0, АУД.1, АУД.2, АУД.3, АУД.4, АУД.6, АУД.7, АУД.8, АУД.10)

В проекте должны быть предусмотрены инструменты и процедуры непрерывного контроля состояния защиты, регистрации событий и оперативного реагирования на инциденты в АСУ ТП.

Указанные меры реализуются путем применения:

1. Разработка политики аудита безопасности и проведение внутренних аудитов (АУД.0, АУД.10): разработка регламентов, определяющих перечень регистрируемых событий, периодичность их анализа, а также порядок проведения плановых внутренних проверок состояния защищенности системы.
2. Инвентаризация информационных ресурсов (АУД.1): создание и настройка автоматизированных механизмов учета всех компонентов АСУ ТП (ПЛК, АРМ, серверы, сетевое оборудование) с фиксацией их характеристик и мест установки.
3. Анализ уязвимостей и их устранение (АУД.2): использование отечественного сертифицированного ПО для поиска уязвимостей в программном обеспечении и конфигурациях оборудования, а также разработка регламента по их устранению и установке обновлений безопасности.
4. Реагирование на сбои при регистрации событий безопасности (АУД.8): настройка механизмов оповещения администраторов в случае невозможности записи логов (например, при переполнении памяти или отказе хранилища).

Примечание: так же должны быть реализованы формы с перечнем контролируемых событий безопасности, инструкции по анализу журналов и регламент проведения инвентаризации активов.

АНТИВИРУСНАЯ ЗАЩИТА

(АВЗ.0, АВЗ.1, АВЗ.2, АВЗ.4)

В проекте должны быть предусмотрены эшелонированная система антивирусной защиты, обеспечивающая обнаружение и блокирование вредоносного программного кода в контуре АСУ ТП без нарушения работоспособности технологических процессов.

Указанные меры реализуются путем применения:

1. Разработка политики антивирусной защиты (АВЗ.0): создание регламента, определяющего порядок развертывания средств антивирусной защиты, перечень защищаемых объектов, настройки сканирования, а также действия персонала при обнаружении вредоносного ПО.
2. Реализация антивирусной защиты (АВЗ.1): внедрение и настройка отечественного сертифицированного ПО (антивирусных средств), совместимого с используемым в АСУ ТП системным и прикладным программным обеспечением.
3. Антивирусная защита электронной почты и иных сервисов (АВЗ.2): обеспечение фильтрации входящих потоков данных на уровне межсетевых экранов или специализированных шлюзов безопасности с использованием отечественного сертифицированного ПО.
4. Обновление базы данных признаков вредоносных компьютерных программ (АВЗ.4): проектирование и настройка инфраструктуры для безопасного обновления антивирусных баз внутри изолированного сегмента АСУ ТП, а также разработка инструкции по их регулярной актуализации без прямого доступа в сеть «Интернет».

Примечание: в состав эксплуатационной документации должны входить инструкции по администрированию средств антивирусной защиты, регламент обновления сигнатурных баз в изолированном контуре и протоколы тестирования совместимости антивирусного ПО со специфическим ПО АСУ ТП.

ОБЕСПЕЧЕНИЕ ЦЕЛОСТНОСТИ

(ОЦЛ.0, ОЦЛ.1)

В проекте должны быть предусмотрены механизмы контроля неизменности программной среды и

данных, а также защиты системы от несанкционированных исправлений или повреждений кода. Указанные меры реализуются путем применения:

1. Разработка политики обеспечения целостности (ОЦЛ.0): создание регламента, определяющего объекты контроля целостности (файлы ОС, прикладное ПО АСУ ТП, конфигурации оборудования), правила проведения проверок и порядок действий персонала при обнаружении нарушений целостности.
2. Контроль целостности программного обеспечения (ОЦЛ.1): внедрение и настройка отечественного сертифицированного ПО, обеспечивающего автоматический контроль целостности исполняемых модулей, системных библиотек и конфигурационных файлов. Механизмы защиты должны обеспечивать блокировку запуска или уведомление администратора при выявлении несанкционированных изменений.

Примечание: в состав эксплуатационной документации должны входить инструкции по настройке средств контроля целостности, перечень контролируемых объектов с указанием их эталонных контрольных сумм, а также регламент периодической проверки целостности ПО АСУ ТП.

ОБЕСПЕЧЕНИЕ ДОСТУПНОСТИ

(ОДТ.0, ОДТ.4, ОДТ.5, ОДТ.6, ОДТ.8)

В проекте должны быть предусмотрены комплекс мер по обеспечению устойчивого функционирования АСУ ТП и возможности оперативного восстановления работоспособности системы после сбоев или инцидентов.

Указанные меры реализуются путем применения:

1. Разработка политики обеспечения доступности (ОДТ.0): создание регламента, определяющего критичные компоненты системы, допустимое время восстановления, а также порядок действий персонала при возникновении нештатных ситуаций и отказов оборудования.
2. Резервное копирование информации, обеспечение возможности восстановления информации и программного обеспечения (ОДТ.4, ОДТ.5, ОДТ.6): внедрение и настройка отечественного сертифицированного ПО для автоматизированного резервного копирования данных и образов операционных систем. Подрядчик обязан спроектировать защищенное хранилище резервных копий и провести тестирование процедур восстановления для подтверждения их работоспособности.
3. Контроль предоставляемых вычислительных ресурсов и каналов связи (ОДТ.8): использование встроенных механизмов мониторинга ОС и активного сетевого оборудования, а также отечественного сертифицированного ПО для контроля загрузки процессоров, оперативной памяти, дискового пространства и пропускной способности каналов связи с целью предупреждения отказов системы из-за нехватки ресурсов.

Примечание: в состав эксплуатационной документации должны входить регламент резервного копирования, инструкции по пошаговому восстановлению программного обеспечения и данных из резервных копий, а также протоколы успешно проведенного тестового восстановления системы

ЗАЩИТА ТЕХНИЧЕСКИХ СРЕДСТВ И СИСТЕМ

(ЗТС.0, ЗТС.2, ЗТС.3, ЗТС.4, ЗТС.5)

В проекте должны быть предусмотрены комплекс мер по физической защите оборудования АСУ ТП, исключающий несанкционированный доступ к аппаратным средствам и защищающий их от внешних деструктивных воздействий.

Указанные меры реализуются путем применения:

1. Разработка политики защиты технических средств и систем (ЗТС.0): создание регламента, определяющего требования к размещению оборудования, правила доступа в помещения с техническими средствами АСУ ТП и порядок контроля целостности корпусов и шкафов управления.
2. Организация контролируемой зоны и управление физическим доступом (ЗТС.2, ЗТС.3): проектирование границ контролируемой зоны и внедрение технических средств (электронных замков, считывателей, датчиков вскрытия), интегрированных с отечественным сертифицированным ПО систем контроля и управления доступом (СКУД) для регистрации и ограничения входа в пультовые, серверные и к шкафам ПЛК.
3. Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр (ЗТС.4): проектирование расположения мониторов АРМ операторов и крупнопанельных дисплеев таким образом, чтобы исключить возможность

- визуального съема информации посторонними лицами через окна или дверные проемы.
4. Защита от внешних воздействий (ЗТС.5): использование специализированных защищенных шкафов (класса IP), систем бесперебойного питания, заземления и климат-контроля для защиты технических средств от пыли, влаги, перепадов температуры и электромагнитных помех в соответствии с условиями эксплуатации на объекте.

Примечание: в состав эксплуатационной документации должны входить схемы размещения оборудования с указанием границ контролируемой зоны, инструкции по управлению физическим доступом и регламент проверки целостности печатей (пломб) на аппаратных средствах

ЗАЩИТА АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ И ЕЕ КОМПОНЕНТОВ

(ЗИС.1, ЗИС.2, ЗИС.3, ЗИС.5, ЗИС.8, ЗИС.19, ЗИС.20, ЗИС.21, ЗИС.32, ЗИС.34, ЗИС.38, ЗИС.39,)

В проекте должна быть реализована сетевая архитектура, обеспечивающая безопасное взаимодействие компонентов АСУ ТП и защита от внешних сетевых атак.

Указанные меры реализуются за счёт:

1. Разработка политики защиты информационной (автоматизированной) системы и ее компонентов (ЗИС.0): создание регламента, определяющего правила сетевого обмена, топологию сети и порядок внесения изменений в сетевую конфигурацию.
2. Защита периметра, эшелонированная защита и организация демилитаризованной зоны (ЗИС.2, ЗИС.3, ЗИС.5, ЗИС.34): внедрение и настройка отечественного сертифицированного ПО и аппаратных средств (межсетевых экранов уровня UTM) для сегментации сети, фильтрации трафика и защиты от атак типа «DoS/DDoS». Для обмена данными с внешними сетями должна быть спроектирована демилитаризованная зона (DMZ).
3. Разделение функций по управлению с иными функциями (ЗИС.1): выделение трафика администрирования в отдельный защищенный сегмент (VLAN) с запретом доступа к нему из технологической сети.
4. Соккрытие архитектуры, конфигурации и обеспечение доверенных каналов (ЗИС.8, ЗИС.19, ЗИС.20): использование механизмов маскировки внутренней структуры сети и применение отечественного сертифицированного ПО (VPN-шлюзов) для шифрования данных при их передаче по открытым каналам связи, обеспечивая создание доверенных маршрутов обмена информацией.
5. Запрет несанкционированной удаленной активации устройств и защита беспроводных соединений (ЗИС.21, ЗИС.32): программное и аппаратное отключение функций удаленного включения периферийных устройств (камер, микрофонов), а также обязательное использование механизмов авторизации и шифрования для разрешенных беспроводных сегментов.
6. Защита информации при использовании мобильных устройств и управление перемещением виртуальных машин (ЗИС.38, ЗИС.39): применение отечественного сертифицированного ПО для контроля мобильных средств доступа (если предусмотрено проектом) и обеспечения безопасности миграции виртуальных ресурсов внутри серверного кластера.

Примечание: в состав эксплуатационной документации должны входить детальная схема сетевой архитектуры, таблицы маршрутизации, перечень разрешенных сетевых протоколов и портов (матрица сетевых доступов), а также инструкции по настройке межсетевых экранов и VPN-шлюзов

(ИНЦ.0, ИНЦ.1, ИНЦ.2, ИНЦ.3, ИНЦ.4, ИНЦ.5):

В проекте должны быть реализованы организационные процедуры и технические инструменты, обеспечивающие своевременное обнаружение, локализацию и ликвидацию последствий компьютерных атак и сбоев в АСУ ТП.

Указанные меры реализуются за счёт:

1. Разработка политики реагирования на компьютерные инциденты (ИНЦ.0): создание регламента, определяющего критерии отнесения событий к инцидентам, состав аварийной команды (группы реагирования), порядок связи и распределение ответственности.
2. Устранение последствий компьютерных инцидентов и принятие мер по предотвращению их повторного возникновения (ИНЦ.4, ИНЦ.5): разработка планов действий по восстановлению работоспособности системы (планов аварийного восстановления) и процедур «разбора полетов» для корректировки настроек средств защиты после инцидента.

Примечание: в состав эксплуатационной документации должны входить регламент реагирования на компьютерные инциденты, пошаговые инструкции для персонала при обнаружении типовых атак и формы отчетов (актов) о результатах расследования инцидентов.

УПРАВЛЕНИЕ КОНФИГУРАЦИЕЙ

(УКФ.0, УКФ.2, УКФ.3):

В проекте должны быть реализованы механизмы строгого контроля состава и настроек аппаратных и программных средств АСУ ТП, исключающие стихийное изменение параметров системы.

Выполнение данных требований обеспечивается за счет:

1. Разработка политики управления конфигурацией информационной (автоматизированной) системы (УКФ.0): создания регламента, определяющего эталонное состояние системы, порядок документирования настроек и периодичность проверки соответствия текущей конфигурации проектным данным.
2. Управление изменениями (УКФ.2): внедрения процедур санкционирования, тестирования и фиксации любых изменений в ПО или аппаратной части АСУ ТП, включая ведение журналов версий и учет выполненных доработок.
3. Установка (инсталляция) только разрешенного к использованию программного обеспечения (УКФ.3): применения отечественного сертифицированного ПО, обеспечивающего контроль состава установленного софта и блокировку попыток инсталляции программ, не входящих в утвержденный «белый список» (перечень разрешенного ПО).

Примечание: В состав эксплуатационной документации должны входить регламент управления конфигурацией, перечень (эталон) разрешенного программного обеспечения и актуальные формуляры на компоненты АСУ ТП с фиксацией их версий и контрольных сумм

УПРАВЛЕНИЕ ОБНОВЛЕНИЯМИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

(ОПО.0, ОПО.1, ОПО.2, ОПО.3, ОПО.4):

В проекте должны быть реализованы процедуры и технические решения по безопасному обновлению ПО, исключающие внесение уязвимостей и нарушение стабильности технологического процесса.

Выполнение данных требований обеспечивается за счет:

1. Разработка политики управления обновлениями программного обеспечения (ОПО.0): создания регламента, определяющего периодичность поиска обновлений, ответственных лиц, а также критичность обновлений для различных компонентов АСУ ТП.
2. Поиск, получение обновлений программного обеспечения от доверенного источника (ОПО.1): определения перечня официальных ресурсов разработчиков и проектирования защищенных каналов (или процедур офлайн-переноса) для получения дистрибутивов без прямого подключения компонентов АСУ ТП к сети «Интернет».
3. Контроль целостности обновлений программного обеспечения (ОПО.2): обязательной проверки подлинности и неизменности полученных файлов путем сверки их контрольных сумм с эталонными значениями, предоставленными разработчиком ПО.
4. Тестирование обновлений программного обеспечения (ОПО.3): проведения предварительной проверки обновлений на выделенном стенде (или тестовом сегменте), имитирующем работу реальной АСУ ТП, для подтверждения отсутствия конфликтов с технологическим ПО.
5. Установка обновлений программного обеспечения (ОПО.4): применения отечественного сертифицированного ПО для централизованного или локального развертывания проверенных обновлений в периоды планового обслуживания системы.

Примечание: в состав эксплуатационной документации должны входить регламент управления обновлениями, инструкции по проверке контрольных сумм дистрибутивов и протоколы успешного тестирования обновлений на совместимость с прикладным ПО АСУ ТП

ПЛАНИРОВАНИЕ МЕРОПРИЯТИЙ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ

(ПЛН.0, ПЛН.1, ПЛН.2):

В проекте должна быть реализована система планирования и контроля деятельности по защите информации, обеспечивающую системный подход к безопасности АСУ ТП на всех этапах её жизненного цикла.

1. Выполнение данных требований обеспечивается за счет:
2. Разработка политики планирования мероприятий по обеспечению защиты информации (ПЛН.0): создания регламента, определяющего порядок долгосрочного и краткосрочного планирования работ по ИБ, назначение ответственных подразделений и установление целей обеспечения безопасности.
3. Разработка, утверждение и актуализация плана мероприятий по обеспечению защиты информации (ПЛН.1): формирования детального графика работ (плана-графика), включающего проведение технических проверок, инструктажей персонала, процедур продления лицензий и сертификатов на используемые средства защиты.
4. Контроль выполнения мероприятий по обеспечению защиты информации (ПЛН.2): внедрения процедур регулярной отчетности, и использования отечественного сертифицированного ПО (систем мониторинга или управления задачами) для фиксации фактов выполнения плановых работ и выявления отклонений от утвержденного графика.

Примечание: в состав эксплуатационной документации должны входить регламент планирования, типовой годовой план мероприятий по обеспечению защиты информации и формы отчетности о выполнении плановых показателей.

ОБЕСПЕЧЕНИЕ ДЕЙСТВИЙ В НЕШТАТНЫХ СИТУАЦИЯХ

(ДНС.0, DNS.1, DNS.2, DNS.5, DNS.6):

В проекте должен быть реализован комплекс организационных и технических мер, обеспечивающих готовность персонала и системы к функционированию в условиях аварийных ситуаций, сбоев или инцидентов ИБ.

Выполнение данных требований обеспечивается за счет:

1. Разработка политики обеспечения действий в нештатных ситуациях (ДНС.0): создания регламента, определяющего классификацию нештатных ситуаций, цели и задачи по обеспечению непрерывности технологического процесса и распределение полномочий сотрудников.
2. Разработка плана действий в нештатных ситуациях (ДНС.1): формирования детальных планов аварийного восстановления, содержащих алгоритмы действий по локализации угроз и переводу системы в безопасный режим функционирования.
3. Обеспечение возможности восстановления информационной (автоматизированной) системы в случае возникновения нештатных ситуаций (ДНС.5): внедрения и настройки отечественного сертифицированного ПО для создания резервных копий конфигураций, проектов SCADA и образов, а также проектирования схем горячего или холодного резервирования аппаратных средств.
4. Анализ возникших нештатных ситуаций и принятие мер по недопущению их повторного возникновения (ДНС.6): установления процедуры обязательного технического расследования каждого случая нештатной работы системы с целью корректировки настроек средств защиты и актуализации проектных решений.

Примечание: в состав эксплуатационной документации должны входить регламент обеспечения действий в нештатных ситуациях, план аварийного восстановления (DRP), программы и методики проведения тренировок персонала, а также типовые формы актов анализа причин возникновения нештатных ситуаций

5. ТРЕБОВАНИЯ К ТЕХНИЧЕСКОМУ ОБЕСПЕЧЕНИЮ АСУ ТП И СРЕДСТВАМ ЗАЩИТЫ

ИНФОРМАЦИИ (РЕКОМЕНДУЕМЫЕ)

МАШИННЫЕ НОСИТЕЛИ ИНФОРМАЦИИ

Машинные носители информации (внешние накопители), используемые для хранения резервных копий, должны поставляться в количестве не менее 2-х единиц на каждый тип бэкапа и удовлетворять следующим характеристикам:

- иметь ёмкость не менее 1000 ГБ (1 ТБ) для хранения полных образов системных дисков серверов, АРМ и баз данных АСУ ТП;
- иметь ёмкость не менее 100 ГБ для резервных копий конфигураций СПО, ПЛК, сетевого оборудования и средств защиты (МЭ, АВЗ);
- иметь интерфейс подключения не ниже USB 3.0 (или аналогичный по скорости передачи данных).

При выборе средств МЭ, АСО и АВЗ следует учитывать рекомендации разработчиков АСУ ТП (обязательное требование) и средства защиты, применяемые в Обществе (рекомендательное требование), при условии их соответствия требованиям по импортозамещению и наличия действующих сертификатов ФСБ и ФСТЭК России. В части обеспечения сетевой безопасности проектируемые решения должны быть технологически совместимы с существующей инфраструктурой защищенной сети ViPNet Общества (сеть №12295). Проектируемые средства защиты информации должны обеспечивать функционирование в едином ключевом пространстве и под управлением имеющихся у Общества средств централизованного управления сетью ViPNet, иметь действующие сертификаты ФСБ России по классу КС2, действующие сертификаты ФСТЭК России по 4 классу защиты.

Применение иных решений допускается при условии обеспечения полной интеграции в действующую защищенную сеть без создания параллельных систем управления и без снижения установленного уровня защищенности

Программно-технические средства защиты информации в АСУ ТП должны обеспечивать:

- Отключение всех служб и сервисов на АРМ и серверах, не используемых в процессе эксплуатации. Включение необходимых для обслуживания сервисов должно производиться временно в соответствии с регламентом управления конфигурацией;
- Программную или физическую блокировку всех неиспользуемых коммуникационных портов (USB, COM, PS/2 и др.) и интерфейсов на АРМ, серверах и сетевом оборудовании;
- Запрет загрузки ОС с внешних носителей в BIOS/UEFI всех компьютеров и серверов, а также обязательную установку пароля на изменение настроек BIOS/UEFI;
- Обязательное документирование всех параметров конфигурации АСУ ТП.

В состав эксплуатационной документации на АСУ ТП и средства защиты должны входить перечни и эталонные значения конфигурационных параметров (в том числе контрольные суммы ПО), инструкции по восстановлению защитных мер и актуальная матрица сетевых доступов.