

Дополнительные требования по информационной безопасности.

Состав представляемых на рассмотрение материалов проектирования:

- анализ угроз безопасности информации и разработку модели угроз безопасности информации или ее уточнение (при ее наличии);
- категории значимости объекта информационной инфраструктуры;
- решения по организационным и техническим мерам обеспечения информационной безопасности объектов информационной инфраструктуры;
- требования к применяемым программным и программно-аппаратным средствам, в том числе средствам защиты информации;
- требования к защите средств и систем, обеспечивающих функционирование объекта информационной инфраструктуры (обеспечивающей инфраструктуре);
- требования к информационному взаимодействию значимого объекта с иными объектами критической информационной инфраструктуры, а также иными информационными системами, автоматизированными системами управления или информационно-телекоммуникационными сетями.

— Требования к предоставляемым материалам в части подсистемы Информационной безопасности:

- Руководящие указания по установке и настройке средств защиты информации, настройке программных и программно-аппаратных средств безопасности объектов информационной инфраструктуры;
- Руководящие указания по риск-ориентированному управлению объектами информационной инфраструктуры (ИТТ активами), организации в рамках процесса эксплуатации установки критических обновлений программного обеспечения для объектов;
- Руководящие указания по конфигурации параметров программных и программно-аппаратных средств информационно-телекоммуникационной сети для обеспечения безопасности объектов информационной инфраструктуры, в том числе по обеспечению безопасного удаленного мониторинга объектов информационной инфраструктуры Цифровой сети, организации удаленного доступа в информационно-телекоммуникационную сеть субъекта электроэнергетики;
- Разработать и согласовать программу информирования и обучение персонала объекта информационной инфраструктуры;
- Представить расчет нормативной численности персонала, ответственного за планирование и контроль мероприятий по обеспечению безопасности объекта информационной инфраструктуры, управление (администрирование) подсистемой информационной безопасности, управление средствами защиты информации, управление обновлениями программных и программно-аппаратных средств, в том числе средств защиты информации, с учетом особенностей функционирования значимого объекта, мониторинг и анализ зарегистрированных событий в значимом объекте, связанных с обеспечением безопасности (далее - события безопасности), сопровождение функционирования подсистемы безопасности значимого объекта в ходе ее эксплуатации, включая ведение эксплуатационной документации и организационно-распорядительных

документах по безопасности значимого объекта;

- Представить решения по централизованному управлению подсистемой безопасности объектов информационной инфраструктуры (при необходимости);

- Разработать и согласовать план мероприятий по обеспечению безопасности объектов информационной инфраструктуры на случай возникновения нештатных (непредвиденных) ситуаций;

- Разработать и согласовать проект Акта категорирования объекта критической информационной инфраструктуры.

Материалы проектной и рабочей документации в части информационной безопасности согласовать с подразделением информационной безопасности Предприятия электрических сетей, Департаментом комплексной безопасности персонала, объектов и информационной безопасности ПАО «МОЭСК», а также иными заинтересованными лицами.

3. Требования по обеспечению информационной безопасности.

Требования по обеспечению информационной безопасности

Порядок создания подсистемы информационной безопасности, построение этапов работ, а также разработка технической и рабочей документации должны соответствовать ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения».

Обеспечить создание подсистемы информационной безопасности, а также обеспечить выполнение:

- требований 187-ФЗ от 26.07.2017г. «О безопасности критической информационной инфраструктуры Российской Федерации» и подзаконных актов;

- требований Приказа ФСТЭК от 14 марта 2014 г. № 31 - не ниже 3 класса защищенности автоматизированной системы управления;

- требований РД «Автоматизированные системы. Защита от несанкционированного доступа. Классификация автоматизированных систем и требования по защите информации» не ниже уровня 1 Г;

- требований Распоряжения ПАО «Россети» «О единой технической политике в электросетевом комплексе»;

- средства защиты информации должны соответствовать требованиям не ниже 6-го или более высокого уровня доверия («Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий», утвержденные приказом ФСТЭК России от 02.06.2020 N 76);

Применяемое оборудование должно быть включено в Реестр промышленной продукции, произведенной на территории Российской Федерации.

Применяемое программное обеспечение должно быть включено в Единый реестр российских программ для электронно-вычислительных машин и баз данных.

Применяемое оборудование и программное обеспечение средств информационной безопасности, сети передачи данных, АСУТП, ТМ должно быть сертифицированным ФСТЭК России и/или допущенным к применению на объектах ПАО "Россети", в соответствии с требованиями Приказа ПАО «Россети» от 26.07.2023 № 305 «Об утверждении документов в области проверки качества (аттестации) оборудования, материалов и систем» и прошедшим проверку в соответствии с требованиями приказа ПАО «Россети» от 28.08.2020 № 391 «Об утверждении Методики проведения проверки цифрового оборудования и систем на соответствие требованиям безопасности информации, в том числе проведения проверки качества технических средств защиты информации в электросетевом комплексе».

В случае модернизации, реконструкции или создания автоматизированной системы мониторинга и диагностики энергетического оборудования, обеспечить выполнение требований Приказа Министерства энергетики РФ от 06.11.2018 №1015 «Об утверждении требований в отношении базовых (обязательных) функций и информационной безопасности объектов электроэнергетики при создании и последующей эксплуатации на территории Российской Федерации систем удаленного мониторинга и диагностики энергетического оборудования».

В случае организации дистанционного управления оборудованием, обеспечить выполнение требований Приказа Минэнерго России от 26.12.2023 № 1215 "Об утверждении дополнительных требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры, функционирующих в сфере электроэнергетики, при организации и осуществлении дистанционного управления технологическими режимами работы и эксплуатационным состоянием объектов электроэнергетики из диспетчерских центров субъекта оперативно-диспетчерского управления в электроэнергетике".

При проектировании и выполнении работ, учесть мероприятия, выполняемые в рамках смежных проектов.

Тома проектной и рабочей документации в части информационной безопасности и тома в части защищаемых объектов информационной инфраструктуры (системы АСУ ТП, ТМ, СДТУ, АСМД, дистанционного управления КА и/или оборудования РЗА) согласовать со структурным подразделением информационной безопасности филиала, Департаментом информационной безопасности ИА Общества и филиалом АО «СО ЕЭС» - «Московское РДУ». (в случае организации обмена информацией с филиалом АО «СО ЕЭС» - «Московское РДУ»).

Обеспечить комплексную защиту информации, определяющей режим функционирования и/или раскрывающей систему защиты конкретного объекта, в случае ее передачи за пределы контролируемой территории.

1) Оборудование структурных компонентов (функциональных систем и подсистем) систем обеспечения безопасности объекта, а также помещений, в которых размещаются центральный и локальные пульты управления с устанавливаемым в них оборудованием, должно проводиться с учетом реализации технических мероприятий по защите информации.

2) На структурные компоненты (функциональные системы и подсистемы) систем обеспечения безопасности объекта, разработать модели угроз для каждого типа энергообъекта.

3) Обеспечить целостность информации при передаче по внешним каналам связи по протоколу МЭК 670-5-101/104 с использованием шифрования или технологии инспекции промышленных протоколов.

4) Обеспечить целостность информации при передаче по внешним каналам связи по протоколу МЭК 670-5-101/104 с использованием шифрования.

5) Требования информационной безопасности, применяемые на всех объектах защиты:

- в случае наличия парольной защиты доступа, все пароли по умолчанию должны быть изменены;

- парольная политика к объектам защиты должна соответствовать установленным требованиям: по сложности пароля (не менее 15 символов, наличие символов в разном регистре, наличие специальных символов), сроку действия паролей и истории паролей;

- доступ персонала вне зависимости от объекта защиты должен быть персонализирован, необходимо исключить (при наличии технической возможности) возможность доступа к объектам защиты под одной учетной записью (одним паролем) для различных работников;

- встроенные учетные записи на всех компонентах объектов защиты должны быть отключены;

- высший приоритет применения на объектах защиты должны иметь механизмы доступа с применением многофакторной аутентификации;

- незадействованный функционал и компоненты объектов защиты должны быть отключены;

- на всех объектах защиты и их компонентах, должны быть включены и настроены функции регистрации событий безопасности с передачей на специально выделенный сервер сбора информации подсистемы мониторинга информационной безопасности;

- по всем компонентам объектов защиты должны быть установлены процедуры обновлений безопасности, время применения обновления безопасности на компонентах объектов защиты не должно превышать 24 часов.

6) Требования информационной безопасности, применяемые к информационно-телекоммуникационной сети (далее - ИТС):

- должен быть организован периметр технологического сегмента ИТС Объекта. Организация сетевого периметра ИТС Объекта должна быть обеспечена посредством межсетевых экранов;

- физическое соединение технологического сегмента ИТС Объекта с остальной ИТС Объекта при ее наличии, должно обеспечиваться только через устройство, реализующее функции межсетевого экранирования;

- физическое соединение технологического сегмента ИТС Объекта с остальной ИТС Объекта при ее наличии, должно обеспечиваться только через устройство, реализующее функции межсетевого экранирования;

– выделение сегментов должно обеспечиваться посредством, одновременного применения следующих технологий и методов в порядке эффективности защиты (при наличии такой возможности):

– физическое выделение, посредством организации сегментов за счет выделенных коммутирующих устройств, подключаемых только к межсетевым экранам (наиболее защищенный вариант);

– с применением средств криптографической защиты доступа к сети и защиты трафика (VPN) при условии, что указанные средства в сегменте образуются посредством установки специализированного ПО на каждом из конечных узлов (серверов, АРМ);

– VLAN;

– VRF.

На каждом из Объектов в ИТС должны быть выделены сегменты управления:

– сегмент управления ИТС (имеет доступ персонал, осуществляющий функции управления ИТС);

– сегмент управления АСТУ (имеет доступ персонал, осуществляющий функции управления АСТУ);

– сегмент управления подсистемами ИБ;

– сегмент оперативного управления Объектом (имеет доступ персонал, осуществляющий оперативное управление оборудованием Объекта).

– доступ к технологическому сегменту ИТС и другим входящим в него сегментам АС должен осуществляться только из сегмента оперативного управления.

– взаимодействие сегментов должно ограничиваться следующими правилами:

– доступ к сегментам управления из других сегментов запрещен;

– взаимодействие между сегментами должно происходить исключительно через средства межсетевого экранирования;

– взаимодействие между сегментами автоматизированных систем должно обеспечиваться в случае необходимости только посредством выделения специализированных выделенных «буферных» сегментов;

– правила на межсетевых экранах должны быть максимально точными включая указание адресов назначения и источника, портов назначения и источника.

– для взаимодействия с внешними сетями и АС должны создаваться «демилитаризованные» зоны – сегменты сети, в которые могут обращаться внешние «потребители» и из которых исключена возможность инициации соединений во внутренние сегменты сети Объекта;

– служебные протоколы оборудования образующего ИТС, должны быть доступны только из сегмента управления ИТС;

– должны быть отключены неиспользуемые и небезопасные (передающие информацию по сети в открытом, незашифрованном виде) протоколы и сервисы на сетевом оборудовании;

– неиспользуемые порты на коммутационном оборудовании должны быть отключены логически и физически;

– доступ на уровне ИТС должен осуществляться в случае необходимости дополнительных мер с применением протоколов 802.1x и фильтрации MAC адресов;

– устройства беспроводной связи должны находиться физически и логически за организованным периметром ИТС Объекта;

– технологические протоколы необходимо строго изолировать от внешнего проникновения;

– на сетевом оборудовании должны быть включены функции от подмены сетевых адресов и меры защиты от внедрения ложной маршрутной информации в протоколы маршрутизации;

– должен быть включен сбор событий на уровне трафика в сети и передаваться на сервер подсистемы мониторинга информационной безопасности для контроля легитимности сетевых соединений.

7) Требования информационной безопасности, применяемые к автоматизированным системам (далее АС):

– каждая АС должна быть изолирована, от других АС, при необходимости взаимодействия с другими АС, взаимодействие должно быть обеспечено методами исключающими возможность его использование в деструктивных целях для обеих АС;

– при необходимости сбора необходимой информации с АС, указанные АС должны позволять передавать информацию посредством отправки технологической и другой информации иницируя соединения самостоятельно (по примеру протокола Syslog). Методы в виде опроса сервисов, баз данных и т.д. систем должны быть исключены;

– должно обеспечиваться резервирование конфигураций и баз данных АС;

– все применяемые АС должны иметь актуальную и доступную проектную и эксплуатационную документацию;

– в целевом исполнении АС должны иметь механизмы электронной подписи и криптографической защиты информации, а также должны обладать процедурами двойного контроля или паритета ответственности, когда выполнение критических действий невозможно выполнить одновременно одним лицом;

– прямой доступ к базам данных АС должен быть исключен;

– территориально распределенные АС, с выведенным функционалом по управлению на централизованное удаленное управление в частности АСТУ, должны позволять осуществлять перевод управления на нижний (местный, Объектовый уровень). Функция отключения указанного внешнего управления должна гарантировать исключение возможности включения удаленного управления из вне;

– при выполнении контроля за АС необходимо обеспечить контроль за всеми ее компонентами на каждом конкретном Объекте (уровень системного программного обеспечения, уровень прикладного программного обеспечения (далее - ПО), уровень баз данных).

8) Требования информационной безопасности, применяемые к автоматизированным рабочим местам (далее АРМ) и серверам:

– На серверах АС и АРМ в обязательном порядке должны быть установлены средства антивирусной защиты с актуальными обновлениями;

– Должна быть исключена возможность использования внешних устройств беспроводной связи на серверах и АРМ (блокировка необходимых портов как физически так и логически);

– Подключение внешних устройств хранения данных по умолчанию должно быть запрещено, подключение должно быть вызвано потребностью технологического бизнес-процесса и только на ограниченное время с контролем со стороны работника службы безопасности;

– Должны быть включены пароли на доступ к встроенному ПО (BIOS, UEFI, сервисы управления) серверов и АРМ;

– Должен применяться только необходимый и согласованный состав ПО на АРМ и серверах. При наличии возможности со стороны средств безопасности установленных на АРМ и серверах должна быть реализована политика белых списков в отношении, используемого ПО;

– В целом исполнении доступ к АРМ и серверам должен обеспечиваться посредством средств многофакторной аутентификации;

– Подключение к сети Интернет АРМ, с которых осуществляется выполнение критических операций должно быть запрещено;

– Должен производиться контроль за хранением на серверах и АРМ парольной информации. В случае выявления должны быть инициированы проверки целостности скомпрометированных узлов и незамедлительная замена парольной информации для всех учетных записей, а также ревизия учетных записей;

– На всех АРМ и серверах должны быть включены персональные межсетевые экраны с правилами минимально необходимыми для функционирования объектов защиты. Весь остальной сетевой доступ должен быть заблокирован.

9) Требования к оборудованию:

– На всем технологическом оборудовании Объекта и оборудовании безопасности имеющим функции управления, должны быть максимально использованы функции безопасности при их наличии;

– Оборудование должно подключаться только к своим сегментам ИТС;

– Неиспользуемый функционал и интерфейсы связи должны быть отключены.

10) Требования к подсистемам информационной безопасности:

Минимальный состав подсистем ИБ должен состоять из:

– подсистемы антивирусной защиты;

– подсистемы межсетевого экранирования ИТС и конечных узлов;

– подсистемы анализа сетевого трафика и обнаружения компьютерных атак;

– подсистемы мониторинга информационной безопасности (централизация сбора и анализа событий безопасности регистрируемых на конечных узлах Объекта с целью контроля и выявления нарушений).

Предусмотреть сбор событий информационной безопасности для передачи в САЦ сетевой компании.

Необходимость разработки мероприятий защиты информации для каждого конкретного объекта определяется по результатам предпроектного обследования.

Использовать отдельные туннелированные каналы связи (стандарт VPN) для телеизмерений, учёта и качества электроэнергии, средств физической безопасности).

Создаваемые в рамках проводимых работ центральные и удаленные пулты управления безопасностью должны быть аттестованы на предмет соответствия

требованиям РД «Автоматизированные системы. Защита от несанкционированного доступа. Классификация автоматизированных систем и требования по защите информации» не ниже уровня 1Г.

___ . Требования к участникам:

Участник торгово-закупочных процедур или член коллективного участника, чьими силами планируется выполнение работ в части обеспечения информационной безопасности, на момент подачи заявки и выполнения работ должен отвечать следующим требованиям по наличию:

– Лицензии ФСТЭК на деятельность по технической защите конфиденциальной информации согласно п. д) ст.4 Положения введенного Постановлением Правительства РФ 2012 года № 79;

– Лицензии ФСБ на осуществлении работ по пунктам 2 и 3 «Перечня выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств».

___ . Нормативно-технические документы (НТД), определяющие требования к оформлению и содержанию проектной документации (ПД):

- Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

- Политика ПАО «Россети» в области информационных технологий, автоматизации и телекоммуникаций (Политика ИТТ, утверждена Советом директоров ПАО «Россети» (Протокол от 11.09.2017 №276).

- ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения».

Директор департамента
информационной безопасности

В.А. Краснокутский