



УТВЕРЖДАЮ

Заместитель генерального
директора по производству

АО «ГК «Титан»

А.Г. Данилов

«21 » октября 2024г.

ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ
ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

TTN-IN-TT-04

Содержание

1	Область применения	3
2	Нормативные ссылки	3
3	Определения, обозначения и сокращения.....	4
4	Общие положения	4
5	Объекты защиты	5
6	Требования по информационной безопасности для стадии ПИР.....	5
7	Требования к применяемым программным и программно-аппаратным средствам, в том числе к средствам защиты информации	9
8	Состав документации по результату ПИР	10
9	Требования по информационной безопасности для стадии СМР/ПНР	12
	Приложение А (обязательное) Базовые требования к построению схем сетевой инфраструктуры.....	13

1 Область применения

1.1 Настоящий документ устанавливает общие требования к разработке разделов: информационная безопасность для автоматизированной системы управления производственными и технологическими процессами; информационная безопасность для информационно-управляющих систем производственно-хозяйственной деятельности.

1.2 Положения настоящего документа распространяются на объекты критической информационной инфраструктуры, автоматизированные системы управления технологическими и производственными процессами, системы производственно-хозяйственной деятельности.

1.3 Положения настоящего документа вступают в силу с момента его утверждения и действуют до момента утверждения актуализированной версии, либо отмены настоящего документа.

2 Нормативные ссылки

2.1 Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

2.2 Приказ ФСТЭК от 14 марта 2014 г. N 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».

2.3 Постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».

2.4 Приказ ФСТЭК России от 21 декабря 2017 г. № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования».

2.5 Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

2.6 Методика оценки угроз безопасности информации, утвержденной ФСТЭК России от 5 февраля 2021 года.

2.7 Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".

2.8 Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных».

2.9 Положение о Федеральной службе по техническому и экспортному контролю, утвержденное Указом Президента Российской Федерации от 16 августа 2004 г. № 1085.

2.10 ГОСТ 34.201-2020 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем».

2.11 ГОСТ Р 51583 «Порядок создания автоматизированных систем в защищенном исполнении».

2.12 ГОСТ Р 51624 «Автоматизированные информационные системы в защищенном исполнении».

2.13 ГОСТ 34.602-2020 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы».

2.14 Постановление Правительства РФ от 14.11.2023 №1912 «О порядке перехода субъектов критической информационной инфраструктуры Российской Федерации на

преимущественное применение доверенных программно-аппаратных комплексов на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации».

3 Определения, обозначения и сокращения

АРМ: автоматизированное рабочее место.

АСУТП: автоматизированная система управления технологическим процессом.

АСУПП: автоматизированная система управления производственным процессом.

ИС: информационная система.

ИСПД: информационная система персональных данных.

Исполнитель: организация выполняющая работы по созданию СОИБ.

ИУС ПХД: информационно-управляющие системы производственно-хозяйственной деятельности. Под ИУС ПХД в настоящем документе понимается совокупность информации, процедур, персонала, аппаратного и программного обеспечения, объединенных регулируемыми взаимоотношениями для осуществления целенаправленной деятельности по управлению производственно-хозяйственной деятельностью Компании.

Компания: АО «ГК «Титан»».

МТО: материально-техническое обеспечение.

ОКИИ: объект критической информационной инфраструктуры. Под термином ОКИИ в настоящем документе понимаются системы АСУТП и АСУПП, реализующие функции контроля за технологическим и (или) производственным оборудованием и производимыми ими процессами, а также управления таким оборудованием для обеспечения реализации основных видов деятельности Компании.

ПДн: персональные данные.

СМР: строительно-монтажные работы.

СОИБ: система обеспечения информационной безопасности.

ПИР: Проектно-изыскательские работы.

ПНР: пуско-наладочные работы.

ПО: программное обеспечение.

разработка: процесс перевода результатов проектирования в аппаратные и/или программные компоненты, в результате которого аппаратное и/или программное обеспечение системы становится работоспособным.

техническое задание (ТЗ): исходный технический документ для проведения работы, устанавливающий требования к системе или к какой-либо деятельности, документации, разрабатываемой на систему или при выполнении какой-либо деятельности, а также требования к объему, срокам проведения работ и форме представления результатов.

4 Общие положения

4.1 При проектировании систем обеспечения информационной безопасности (СОИБ) информационно-управляющих систем производственно-хозяйственной деятельности (ИУС ПХД) следует учитывать ограничительные условия санкционной политики.

4.2 Построение системы обеспечения информационной безопасности для подсистем АСУ ТП и ИУС ПХД осуществляется в соответствии с требованиями законодательства Российской Федерации, нормативных документов федеральных органов исполнительной власти, уполномоченных в области обеспечения безопасности и технической защиты информации, локальных нормативных актов Компании.

4.3 При проектировании систем обеспечения информационной безопасности автоматизированных систем управления технологическими и производственными процессами (АСУТП (ПП)), объектов критической информационной инфраструктуры (ОКИИ) с определенной Заказчиком категорией значимости руководствоваться требованиями приказов ФСТЭК России и ФСБ России, принятых во исполнение Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской

Федерации» с учетом ограничительных условий санкционной политики.

5 Объекты защиты

5.1 Объектами защиты ОКИИ являются:

- программно-аппаратные средства (включая автоматизированные рабочие места, серверы, телекоммуникационное оборудование, линии связи, программируемые логические контроллеры, производственное, технологическое оборудование (исполнительные устройства);
- программные средства (включая микропрограммное, общесистемное, прикладное);
- хранимая и обрабатываемая в указанных системах информация (данные) о параметрах (состоянии) управляемого (контролируемого) объекта или процесса (входная (выходная) информация, управляющая (командная) информация, контрольно-измерительная информация, иная критически важная (технологическая) информация), в том числе конфигурационная информация;
- средства защиты информации.

5.2 Объектами защиты в ИУС ПХД являются:

- хранимая и обрабатываемая информация, подлежащие защите в соответствии с действующим законодательством, а также информация, модификация или утрата которой может привести к нарушению хода реализации бизнес-процессов Компании;
- программно-технический комплекс, включающий серверное оборудование (серверы прикладных систем, СУБД, файл-серверы, серверы с использованием средств терминального доступа и средств виртуализации, коммуникационные и другие серверы), телекоммуникационное оборудование (коммутаторы, маршрутизаторы и т.д.), средства межсетевого экранирования, оборудование систем телефонной связи и т.п.;
- АРМ пользователей;
- производственное, технологическое оборудование (контроллерное оборудование, оборудование систем измерения, исполнительные устройства, и т.п.);
- программные средства (микропрограммное, общесистемное, прикладное);
- средства защиты информации.

5.3 Требования по информационной безопасности формируются с учетом уровня значимости объекта защиты, модели угроз и нарушителя, режима работы ОКИИ, экономической целесообразности, уровней критичности объектов защиты, типов пользователей и их прав доступа, режима работы ИУС ПХД, и не должны быть ниже требований, установленных текущим законодательством РФ, локальными нормативными документами Компании в области информационной безопасности ОКИИ.

5.4 Для каждого ОКИИ разрабатывается отдельный комплект документации на СОИБ.

6 Требования по информационной безопасности для стадии ПИР

6.1 Формирование задач по созданию СОИБ должно начинаться одновременно с формированием замысла создания ОКИИ, ИУС ПХД (далее по тексту ИС).

6.2 Требования по безопасности информации для ИС должны формулироваться на основе анализа назначения ИС, защищаемых элементов ИС и среды применения ИС.

6.3 Необходимые данные для формирования требований получают в процессе проведения обследования ИС.

6.4 При обследовании проводятся анализ и идентификация процессов, связанных с обработкой защищаемой информации. Анализируются документы, используемые при организации и проведении работ по созданию СОИБ. В результате обследования определяются узловые элементы процессов обработки, передачи и хранения защищаемой информации, для каждого из которых должны быть установлены:

- объекты и процессы, связанные с защищаемой информацией;
- субъекты, участвующие в обработке, передаче и хранении информации
- их роли (полномочия и ответственность) в отношении к обрабатываемой

информации;

- правила, которыми они должны руководствоваться при обработке информации;
- угрозы, способные негативно повлиять на информацию, и процессы ее обработки и передачи.

6.5 Исполнителем должно быть проведено обследование объекта, в результате которого необходимо представить отчет об обследовании объекта защиты и имеющейся системы защиты, который содержит:

- назначение объекта защиты;
- основные цели и задачи, выполняемые объектом защиты;
- компоненты объекта защиты (в соответствии с п. 4.1 и 4.2 настоящих Требований);
- организационную структуру объекта защиты (категории, роли, функции, полномочия и количество персонала);
- технические характеристики объекта защиты (перечень технических средств,
- их аппаратная платформа, используемое на них системное ПО, прикладное ПО, перечень и состояние служб АРМ, сведения о наличии сертификатов соответствия ФСТЭК, ФСБ, нахождения продукта в жизненном цикле поддержки производителем);
- схему сетевой инфраструктуры комплекса технических средств на уровнях L1/L2/L3 в соответствии с уровнями модели OSI (схема должна соответствовать требованиям, приведенным в Приложении А);
- перечни субъектов доступа и объектов доступа, сведения о политиках управления доступом;
- выявленные типы субъектов доступа (пользователи, процессы (локальные службы, обращения смежных систем)) и объектов доступа, являющихся объектами защиты (автоматизированные рабочие места, информационные активы, программное обеспечение, промышленные серверы, телекоммуникационное оборудование, программируемые логические контроллеры, исполнительные устройства, иные объекты доступа);
- выявленные методы управления доступом (дискреционный, мандатный, ролевой или иные методы), типы доступа (чтение, запись, выполнение или иные типы доступа) и правила разграничения доступа субъектов доступа к объектам доступа (на основе списков, меток безопасности, ролей и иных правил), подлежащие реализации в автоматизированной системе объекта защиты;
- схему функциональной структуры (включая субъект-объектную связь) (в соответствии с требованиями, приведенными в Приложении А);
- сведения об имеющихся/используемых средствах защиты информации;
- описание имеющейся архитектуры подсистемы безопасности, включая состав, места установки с указанием на схеме сетевой инфраструктуры, взаимосвязи средств защиты информации.

6.6 Категорирование (уточнение категории) ОКИИ:

- Исполнителем должно быть проведено категорирование (уточнение категории) ОКИИ.
- Определение категории значимости объектов критической информационной инфраструктуры проводится в соответствии с Постановлением Правительства Российской Федерации от 8 февраля 2018 года №127 «Об утверждении правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».

6.7 Результаты категорирования ОКИИ оформляются проектом акта категорирования с приложением исходных данных (сведения об используемых программных и программно-аппаратных средствах, структурная схема, перечень возможных инцидентов, последствия нарушения функций автоматизации), а также используемых материалы при расчете ущерба, и согласовываются с Заказчиком.

6.8 Формирование модели угроз безопасности информации

6.8.1 По результатам проведения предпроектного обследования и категорирования

ОКИИ, классификации ИУС ПХД Исполнителем формируется Модель угроз, согласно требованиям Методики оценки угроз безопасности информации, утвержденной ФСТЭК России от 5 февраля 2021 года (далее - Методика).

6.8.2 Модель угроз безопасности информации ИС должна содержать в соответствии с Методикой следующие разделы с соблюдением форм представления, прилагаемых к Методике:

- Описание ИС, как объекта защиты;
- Возможные негативные последствия от реализации (возникновения) угроз безопасности информации;
- Возможные объекты воздействия угроз безопасности информации ИС;
- Источники угроз безопасности информации;
- Способы реализации (возникновения) угроз безопасности информации;
- Актуальные угрозы безопасности информации ИС;
- Меры по информационной безопасности, направленные на нейтрализацию актуальных угроз безопасности информации ИС.

6.8.3 С учетом актуальных угроз информационной безопасности, определенными в Модели угроз, формируется перечень мер по обеспечению информационной безопасности.

6.8.4 В качестве исходных данных для анализа угроз безопасности информации должен использоваться банк данных угроз безопасности информации, ведение которого осуществляется ФСТЭК России в соответствии с подпунктом 21 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденному Указом Президента Российской Федерации от 16 августа 2004 г. № 1085.

6.8.5 Перечнем мер по обеспечению информационной безопасности должны обеспечиваться:

- идентификация и аутентификация субъектов и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации;
- аудит безопасности;
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности информации;
- целостность автоматизированной системы управления и информации;
- доступность технических средств и информации;
- защита среды виртуализации;
- защита технических средств и оборудования;
- защита автоматизированной системы и ее компонентов;
- безопасная разработка прикладного и специального программного обеспечения;
- управление обновлениями программного обеспечения;
- планирование мероприятий по обеспечению защиты информации;
- обеспечение действий в нештатных (непредвиденных) ситуациях;
- информирование и обучение персонала;
- анализ угроз безопасности информации и рисков от их реализации;
- выявление инцидентов и реагирование на них (управление инцидентами);
- управление конфигурацией автоматизированной системы управления и ее системы защиты.

6.8.6 Выбор мер защиты информации для их реализации в ИС в рамках ее системы защиты должен включать:

- определение базового набора мер защиты по обеспечению безопасности значимого объекта критической информационной инфраструктуры;
- адаптацию базового набора мер по обеспечению безопасности значимого объекта критической информационной инфраструктуры;

- дополнение адаптированного набора мер по обеспечению безопасности значимого объекта критической информационной инфраструктуры мерами, установленными иными нормативными правовыми актами в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации и защиты информации.

6.8.7 Базовый набор мер по обеспечению безопасности значимого объекта критической информационной инфраструктуры определяется на основе категории значимости объекта критической информационной инфраструктуры в соответствии с приложением к приказу ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

6.8.8 Базовый набор мер по обеспечению безопасности значимого объекта критической информационной инфраструктуры подлежит адаптации в соответствии с угрозами безопасности информации, применяемыми информационными технологиями и особенностями функционирования объекта. При этом из базового набора могут быть исключены меры, непосредственно связанные с информационными технологиями, не используемыми в значимом объекте критической информационной инфраструктуры, или характеристиками, не свойственными объекту. В случае если базовый набор мер, не позволяет обеспечить блокирование (нейтрализацию) всех угроз безопасности информации, в него дополнительно включаются меры, приведенные в приложении к приказу ФСТЭК России от 25 декабря 2017 г. № 239.

6.8.9 Технические меры по обеспечению безопасности ИС реализуются посредством использования программных и программно-аппаратных средств, применяемых для обеспечения безопасности - средств защиты информации (в том числе встроенных в общесистемное, прикладное программное обеспечение).

6.8.10 При этом в приоритетном порядке подлежат применению средства защиты информации, встроенные в программное обеспечение и (или) программно-аппаратные средства значимых объектов (при их наличии).

6.8.11 При этом в ходе разработки системы защиты ИС должно быть проведено обоснование достаточности применения мер по обеспечению промышленной безопасности или физической безопасности для блокирования (нейтрализации) соответствующих угроз безопасности информации.

6.8.12 При отсутствии возможности реализации отдельных мер защиты информации на каком-либо из уровней ИС и (или) невозможности их применения к отдельным объектам и субъектам доступа, в том числе вследствие их негативного влияния на штатный режим функционирования ИС, на этапах адаптации базового набора мер защиты информации или уточнения адаптированного базового набора мер защиты информации разрабатываются иные (компенсирующие) меры, обеспечивающие адекватное блокирование (нейтрализацию) угроз безопасности информации и необходимый уровень защищенности ИС.

6.8.13 В качестве компенсирующих мер, в первую очередь, рассматриваются меры по обеспечению промышленной и (или) физической безопасности ИС.

6.8.14 При этом в ходе разработки организационных и технических мер должно быть обосновано применение компенсирующих мер, а при приемочных испытаниях (аттестации) оценена достаточность и адекватность данных компенсирующих мер для блокирования (нейтрализации) угроз безопасности информации.

6.8.15 Полученный перечень мер по обеспечению информационной безопасности должен быть оформлен по средствам формирования Частного технического задания с указанием актуальной угрозы и меры противодействия ей, а также указанием конкретной реализации меры (наименование орг. меры, наименование ПО, наименование ТС) сформированных в соответствии с положениями приказа ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» с учетом категории значимости объекта критической информационной инфраструктуры и модели угроз.

6.8.16 При разработке технического задания (частного технического задания) на

создание подсистемы безопасности значимого объекта критической информационной инфраструктуры должны быть учтены положения ГОСТ 34.602-2020.

6.9 Требования к ИУС ПХД.

6.9.1 Требования настоящего раздела применяются в случае отсутствия обработки ПДн в ИУС ПХД, в ином случае применяются требования раздела 6.11 настоящего документа.

6.9.2 Исполнителем должна быть проведена классификация ИУС ПХД.

6.9.3 Классификация объектов защиты проводится Исполнителем проекта в рамках создания/модификации подсистемы безопасности в соответствии с уровнем критичности объекта защиты.

6.9.4 «Классификация объектов защиты».

6.9.5 В качестве исходных данных для определения степени тяжести возможных последствий рассматриваются:

- стоимость ПО, технические средства обработки, хранения и передачи информации;
- величины возможных штрафных санкций, предусмотренных государственными нормативно-правовыми актами, договорами за нарушение информационной безопасности объекта защиты;
- возможный ущерб от нарушения функционирования ПО, технических средств обработки, хранения и передачи информации;
- затраты на восстановление функционирования и устранение последствий нарушения безопасности объекта защиты.

6.10 Результаты классификации ИУС ПХД оформляются актом классификации объектов защиты с приложением исходных данных, используемых для расчетов критичности ИУС ПХД, и согласовываются с Заказчиком.

6.11 Требования к ИСПД применяются только в случае обработки ПДн в ИУС ПХД.

6.12 Исполнителем должна быть проведена классификация ИСПД.

6.13 Классификация ИСПД проводится Исполнителем проекта в рамках создания/модификации подсистемы безопасности в соответствии с уровнем защищенности ПДн, согласно требованиям постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

6.14 Результаты классификации ИСПД оформляются Актом определения уровня защищенности ПДн при их обработке в ИСПД, который согласовывается с Заказчиком.

6.15 По результатам проведения предпроектного обследования и классификации

6.16 ИСПД Исполнителем должна быть сформирована модель угроз, согласно требованиям Методики оценки угроз безопасности информации, утвержденной ФСТЭК России от 5 февраля 2021 года (далее - Методика).

7 Требования к применяемым программным и программно-аппаратным средствам, в том числе к средствам защиты информации

7.1 Для обеспечения безопасности ОКИИ должны применяться сертифицированные на соответствие требованиям по безопасности средства защиты информации удовлетворяющие требованиям Постановления Правительства РФ от 14.11.2023 №1912 [2.14].

7.2 Иные средства защиты информации (прошедшие процедуру оценки соответствия в форме испытаний или приемки, которые проводятся с привлечением организаций, имеющих в соответствии с законодательством Российской Федерации лицензии на деятельность в области защиты информации) могут применяться только по согласованию с Заказчиком.

7.3 Для обеспечения безопасности в случаях не указанных в п. 7.1 и 7.2 настоящего документа, должны применяться средства защиты информации, прошедшие процедуру оценки соответствия в форме испытаний или приемки, которые проводятся с привлечением организаций, имеющих в соответствии с законодательством Российской Федерации лицензии на деятельность в области защиты информации, согласованные с Заказчиком.

7.4 В решениях по обеспечению безопасности ИС обеспечить приоритет:

- программному обеспечению, включенному в Единый реестр российских программ

для электронных вычислительных машин и баз данных, за исключением случаев, когда в нем отсутствует программное обеспечение с необходимыми функциональными, техническими и эксплуатационными характеристиками;

- средствам вычислительной техники, телекоммуникационному оборудованию и средствам защиты информации, которым присвоен статус отечественного происхождения и программное обеспечение которых прошло контроль отсутствия не декларированных возможностей.

7.5 Применяемые средства защиты информации должны быть согласованы с Заказчиком.

7.6 Параметры и характеристики применяемых средств защиты информации должны обеспечивать реализацию технических мер по обеспечению безопасности ИС.

7.7 Применяемые в ИС программные и программно-аппаратные средства, в том числе средства защиты информации, должны эксплуатироваться в соответствии с инструкциями (правилами) по эксплуатации, разработанными разработчиками (производителями) этих средств, и иной эксплуатационной документацией. Применяемые средства защиты информации должны быть обеспечены гарантийной, технической поддержкой со стороны разработчиков (производителей).

7.8 Прикладное программное обеспечение, планируемое к внедрению в рамках создания (модернизации или реконструкции, ремонта) ИС и обеспечивающее выполнение его функций по назначению, должно соответствовать следующим требованиям по безопасности, установленным п. 29.3.1-29.3.3 п. 29.3 приказа ФСТЭК России от 25 декабря 2017 г. № 239:

7.8.1 Требования по безопасной разработке программного обеспечения:

- наличие руководства по безопасной разработке программного обеспечения;
- проведение анализа угроз безопасности информации программного обеспечения.

7.8.2 Требования к испытаниям по выявлению уязвимостей в программном обеспечении:

- проведение статического анализа исходного кода программы;
- проведение фаззинг-тестирования программы, направленного на выявление в ней уязвимостей.

7.8.3 Требования к поддержке безопасности программного обеспечения:

- наличие процедур отслеживания и исправления обнаруженных ошибок и уязвимостей программного обеспечения;
- определение способов и сроков доведения разработчиком (производителем) программного обеспечения до его пользователей информации об уязвимостях программного обеспечения, о компенсирующих мерах по защите информации или ограничениях по применению программного обеспечения, способов получения пользователями программного обеспечения его обновлений, проверки их целостности и подлинности.

7.9 В соответствии с п. 29.4 приказа ФСТЭК России от 25 декабря 2017 г. № 239 проектировщик СОИБ обязан включить в документацию сведения о соответствии прикладного программного обеспечения, планируемого к внедрению в рамках создания (модернизации или реконструкции, ремонта) ИС и обеспечивающее выполнение его функций по назначению, требованиям п. 7.8 настоящего документа.

7.10 В случае непредоставления проектировщиком ИС сведений о соответствии прикладного программного обеспечения ИС, обеспечивающего выполнение его функций по назначению требованиям п. 7.8 настоящего документа, проектировщику СОИБ необходимо предусмотреть дополнительные мероприятия по проведению оценки соответствия в форме обязательной сертификации.

8 Состав документации по результату ПИР

8.1 Результатом работ по проектированию СОИБ является разработанная проектная документация: на этапе формирования требований, рабочая, эксплуатационная документация и документация на испытания.

8.2 Проектная документация на этапе формирования требований к СОИБ ИС, должна содержать:

- отчет о предпроектном обследовании ИС;
- акт категорирования (уточнения категории) объекта КИИ;
- перечень угроз безопасности информации и уязвимостей для каждого объекта КИИ;
- частная модель угроз безопасности информации значимого объекта КИИ;
- модель нарушителя безопасности информации;
- частное техническое задание на создание системы безопасности значимых объектов КИИ;

КИИ;

8.3 Рабочая документация на создание/модификацию СОИБ ИС должна содержать:

- пояснительную записку;
- схему сетевой инфраструктуры комплекса технических средств на уровнях L1/L2/L3 в соответствии с уровнями модели OSI (схема должна соответствовать требованиям, приведенным в Приложении А), наложенную на соответствующую схему защиты ИС;
- схему функциональной структуры СОИБ (схема должна соответствовать требованиям, приведенным в Приложении А);
- чертеж установки технических средств (размещение оборудования);
- схему соединений и внешних проводок;
- план расположения оборудования и проводок;
- таблицу соединений и подключений;
- спецификацию СОИБ;
- описание настроек (порядок и перечень параметров настроек средств защиты информации, как встроенных, так и накладных);
- программа и методика опытной эксплуатации системы безопасности;
- журнал опытной эксплуатации системы безопасности;
- рабочая (эксплуатационная) документация на систему безопасности;
- протокол проведения анализа уязвимостей значимого объекта КИИ;
- программа и методика приемочных испытаний значимого объекта КИИ и его системы безопасности;
- протокол проведения приемочных испытаний значимого объекта КИИ и его системы безопасности.

8.4 В пояснительной записке должны быть приведены:

- краткая характеристика объектов защиты с указанием информации об установленном на них ПО (версия и релиз ОС, прикладного специализированного ПО);
- перечни субъектов доступа и объектов доступа, сведения о правах и политиках управления доступом;
- перечень подлежащих реализации организационных и технических мер применительно ко всем объектам и субъектам доступа на аппаратном, системном, прикладном и сетевом уровнях, в том числе в среде виртуализации, с обоснованием выбора мер;
- подробные сведения о видах и типах средств защиты информации, обеспечивающих реализацию технических мер по обеспечению безопасности объекта защиты, их версия, информация о выполняемых ими функциях безопасности, об ограничениях на применение, о совместимости с программными и программно-аппаратными средствами объекта защиты;
- подробное описание архитектуры подсистемы безопасности, включая состав, места установки, взаимосвязи средств защиты информации;
- подробное описание перечня мер по обеспечению безопасности при взаимодействии объекта защиты с иными системами и описание решений по их реализации;
- предложения по внесению изменений в существующие документы и/или проекты методических и организационно-распорядительных документов;
- подробное описание организационных мер защиты, применяемым к объектам защиты, с указанием пунктов методических и организационно-распорядительных документов, описывающих их применение;

- взаимосвязь между мерами защиты, объектами защиты и средствами защиты информации.

8.5 Раскрытие мероприятий по подготовке вводу в действие СОИБ ИС в соответствии со следующей структурой:

- комплектация системы;
- пусконаладочные работы;
- проведение предварительных испытаний системы;
- проведение опытной эксплуатации системы;
- проведение приемочных испытаний системы;
- постоянная эксплуатация системы;
- сопровождение системы;
- мероприятия по обучению и проверке квалификации персонала;
- мероприятия по изменению ИС;
- сметные расчеты, содержащие в том числе перечень и стоимость проведения строительно-монтажных и пусконаладочных работ проекта СОИБ ИС, перечень и стоимость основных средств защиты информации (программных, программно-аппаратных, аппаратных) проекта ИС;

- проект организации строительства, содержащий в том числе график реализации проекта СОИБ ИС (поставка МТО, СМР/ПНР, проведение испытаний).

8.6 При разработке раздела проектной документации с решениями по созданию подсистемы безопасности ИС должны быть учтены требования ГОСТ 34.201-2020.

8.7 Эксплуатационная документация на создание/модификацию подсистемы безопасности ИС должна содержать:

- руководство администратора информационной безопасности;
- инструкцию по эксплуатации комплекса технических средств;
- руководство пользователя;
- формуляр;
- паспорт.

8.8 Руководство администратора информационной безопасности, инструкция по эксплуатации комплекса технических средств, руководство пользователя должны разрабатываться с учетом предложений по внесению изменений в существующие документы и/или проектов методических и организационно-распорядительных документов на СОИБ.

9 Требования по информационной безопасности для стадии СМР/ПНР

9.1 До проведения СМР/ПНР Исполнитель готовит техническое решение на изменение инфраструктуры и согласует его с Заказчиком.

9.2 В случае выполнения работ «под ключ» Исполнитель выполняет СМР/ПНР по системам обеспечения информационной безопасности в соответствии с нормативными документами РФ и согласовывает с Заказчиком.

Приложение А (обязательное)

Базовые требования к построению схем сетевой инфраструктуры

1 Требования к Схеме сетевой инфраструктуры комплекса технических средств на уровнях L1/L2/L3 в соответствии с уровнями модели OSI.

1.1 Схема сетевой инфраструктуры комплекса технических средств должна отображать комбинированное представление физического, канального и сетевого уровней (L1/L2/L3) модели взаимодействия открытых систем.

1.2 Схема сетевой инфраструктуры комплекса технических средств на уровне L1/L2/L3 должна содержать:

1.2.1 Технические средства, входящие в состав ИС. (автоматизированные рабочие места, промышленные серверы, телекоммуникационное оборудование, каналы связи, программируемые логические контроллеры, исполнительные устройства).

1.2.2 Пограничное телекоммуникационное оборудование смежных систем, с которыми осуществляет межсетевое взаимодействие ИС.

1.2.3 IP-адреса, DNS-имена, номера и типы портов технических средств.

1.2.4 Номера VLAN, создаваемых на телекоммуникационном оборудовании.

1.2.5 Границы проектирования, контролируемой зоны, здания, помещений.

1.3 Линии подключения должны быть представлены на схеме для каждого порта в отдельности.

2 Требования к Схеме функциональной структуры (субъектно-объектная связь).

2.1 Схема функциональной структуры должна содержать:

2.1.1 Субъекты доступа (пользователи, процессы (локальные службы, обращения смежных систем), входящие в состав ИС.

2.1.2 Объекты доступа (автоматизированные рабочие места, информационные активы, программное обеспечение, промышленные серверы, телекоммуникационное оборудование, программируемые логические контроллеры, исполнительные устройства, иные объекты доступа), входящие в состав ИС, а также смежных систем, с которыми осуществляется взаимодействие ИС.

2.1.3 Порт (сокеты), протокол прикладного уровня, по которому осуществляется взаимодействие между субъектом и объектом доступа.

2.1.4 Направление передачи данных между субъектом и объектом доступа.

3 Требования к Схеме функциональной структуры СОИБ.

3.1 Схема функциональной структуры СОИБ должна содержать:

3.1.1 Уровни архитектуры СОИБ (уровень мониторинга и администрирования, уровень общекорпоративных средств защиты информации, уровень средств защиты информации конечного узла).

3.1.2 Отображение применяемых на каждом из уровней архитектуры СОИБ средств защиты информации с указанием внутриуровневого и межуровневого взаимодействия.

Лист согласования

РАЗРАБОТАНО

Ведущий инженер по КИПиА



К.А. Исаков

04 10 2024г.

Главный специалист по КИПиА



Р.О. Сидоров

04 10 2024г.

СОГЛАСОВАНО

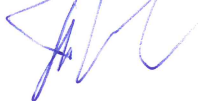
Главный инженер проекта



П.В. Болдырев

___ 2024г.

Руководитель ПО



В.С. Трифонов

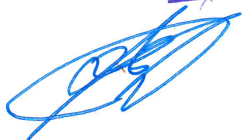
___ 2024г.

Заместитель генерального
директора по информационным
технологиям

А.А. Ключенко

___ 2024г.

Директор ДЭБиЗИ



Н.А. Желнов

___ 2024г.

Лист регистрации изменений

Номер измен ения	Номера листов (страниц)			Идентификационн ое обозначение извещения об изменении	ФИО работника, внесшего изменение	Дата
	замененных	новых	удаленных			