Приложение № 10
к решению Совета директоров ПАО «Россети Центр»
Протокол от 16.06.2022 № 34/22

Утверждено решением Совета директоров ПАО
«Россети» от 29.04.2022
(Протокол от 04.05.2022 № 492)

Изменения
в Положение ПАО «Россети» «О единой технической политике в электросетевом комплексе (далее – Положение)

1. Внести следующие изменения в раздел 1.1. «Цели и основные задачи единой технической политики в электросетевом комплексе»:

1.1. Первый буллит абзаца «Цели» изложить в следующей редакции:

«• определение основных технических направлений и унификация технических и технологических решений, обеспечивающих повышение надежности, эффективности и снижении ресурсоемкости функционирования электросетевого комплекса в краткосрочной и среднесрочной перспективе при обеспечении надлежащей безопасности и надежности энергоснабжения потребителей»;

1.2. Добавить буллиты в абзац «Цели»:

• обеспечение единства подходов при новом строительстве, эксплуатации и выводе из эксплуатации электросетевых объектов;

• обеспечение синхронизации внедрения отраслевых технологий и оборудования и ИТ – технологий, устройств и программного обеспечения;

1.3. Добавить буллит в абзац «Задачи»:

• импортозамещение.

2. Изложить пункт «3.5.3. Принципы управления производственными активами» в следующей редакции:

«Основными принципами управления производственными активами Общества являются:

- ориентация на достижение стратегических целей Государства, Общества и ДЗО;

- системность принятия решений, применение единых критериев, принципов, правил, методик для процессов планирования, осуществления, контроля и оценки эффективности выполнения работ по операционной и инвестиционной деятельности;

- ориентация на получение положительных эффектов в краткосрочной, среднесрочной и долгосрочной перспективах за счет повышения эффективности управления производственными активами на протяжении всего жизненного цикла активов;

- обеспечение функционирования системы управления производственными активами во всех ДЗО Общества, являющихся составной и неотъемлемой частью общей системы управления активами Общества;

- снижение доли оборудования, ЛЭП и сооружений, имеющих высокие и средние уровни риска, сопряженного с их эксплуатацией, с учетом последствий их отказа.».

3. Внести следующие изменения в раздел 3.5.4. «Задачи развития системы управления производственными активами»:

3.1. Изложить первый абзац в следующей редакции:

« - переход от системы управления производственными активами по планово-предупредительному виду организации ремонта к организации ремонта по фактическому техническому состоянию с учетом вероятности и тяжести последствий отказа основного технологического оборудования (рисков);».

3.2. Изложить восьмой абзац в следующей редакции:

« - обеспечение расчетов и мониторинга индексов технического состояния оборудования ПС, ЛЭП и сооружений с оценкой вероятности отказа, тяжести последствий, оценкой риска из-за отказа и оценкой стоимости владения для планирования вида и объема технического воздействия в соответствии с требованиями действующих НПА;».

3.3. Изложить девятый абзац в следующей редакции:

« - оптимизация затрат на ремонтную деятельность, модернизацию, техническое перевооружение оборудования, технологических и инженерных систем, зданий и сооружений с обеспечением необходимого уровня безопасности, эксплуатационной надежности и обеспечения требуемого уровня качества электроснабжения потребителей, а также с учетом перспективного развития электросетевого комплекса;».

4. Изложить пункт 2.1.4.6 раздела 2.1.4 «Коммутационные аппараты» Положения в следующей редакции:

«2.1.4.6. В распределительных сетях напряжением 6-20 кВ дополнительно рекомендуется применять предохранители - разъединители и разъединители, отвечающие современным требованиям эксплуатации, при необходимости с возможностью дистанционного управления, а также разъединители с раздельным отключением фаз, при помощи оперативных изолирующих штанг.».

5. Дополнить раздел 2.1.7 «Трансформаторные и распределительные подстанции 6-35 кВ» Положения пунктом 2.1.7.13:

«2.1.7.13. В распределительных устройствах 0,4-20 кВ ПС, ТП, РП рекомендуется применять термоиндикаторы для периодического контроля температурного режима электротехнического оборудования.».

6. Изложить пункт 2.5.2.6 раздела 2.5.2. «Технические решения при проектировании, новом строительстве и реконструкции ВЛ» в следующей редакции:

«2.5.2.6 При проектировании ВЛ 35 кВ и выше необходимо предусматривать технические решения, обеспечивающие безопасность их эксплуатации, в том числе безопасные подъем/спуск, перемещение и производство работ на высоте. Тип и место установки систем индивидуальной защиты от падения должны быть определены при проектировании ВЛ в зависимости от применяемых конструкций опор (металлическая, решетчатая, многогранная или железобетонная) и условий прохождения трассы ВЛ по согласованию с Заказчиком.».

7. Изложить пункты 2.5.4.1 – 2.5.4.8 раздела 2.5.4 «Провода и грозозащитные тросы» Положения в следующей редакции:

«2.5.4.1. На ВЛ классом напряжения 35 кВ и выше следует применять провод:

- провод со стальным сердечником с профилированными жилами верхних повивов;

- провод с композитными сердечниками из углеродного волокна;

- провод с повышенной коррозионной стойкостью стальных сердечников;

- провод из алюминиевого сплава;

- сталеалюминиевый провод;

Выбор варианта применяемых проводов должен быть обоснован технико-экономическими расчетами при проектировании ВЛ.

2.5.4.2. На ВЛ классом напряжения 35 кВ и выше в качестве грозозащитных тросов могут применяться стальные тросы, сталеалюминевые провода, стальные тросы с повышенной коррозионной стойкостью (оцинкованные, для особо жестких условий работы), сталеалюминевые тросы, грозозащитные тросы со встроенным оптическим кабелем.

Выбор варианта применяемых грозозащитных тросов должен быть обоснован технико-экономическими расчетами при проектировании ВЛ.

2.5.4.3. Применение на отдельных участках ВЛ (большие переходы через водные объекты, горы, поймы, болота, сложные климатические условия) марок и сечений проводов, грозозащитных тросов, а также конструкции фазы, отличных от примененных на остальных участках ВЛ, должно быть подтверждено расчетами конструктивных элементов ВЛ и технико-экономическим обоснованием.

2.5.4.4. При новом строительстве и реконструкции ВЛ классом напряжения 110 кВ и выше, в местах пересечения ВЛ с автомобильными дорогами, инженерными сооружениями и коммуникациями, при проектировании необходимо обеспечить условие дальнейшей безопасной эксплуатации ВЛ с учетом исключения воздействия влияющих факторов,

таких как: перекрытие гирлянд изоляторов от воздействия химических реагентов при антигололедной обработке автодорог, повреждение проводов ВЛ при проезде негабаритной техники, повреждение проводов ВЛ от взрыва газо и нефте-проводов и др. В целях исключения указанных факторов, необходимо рассматривать применения повышенных опор обеспечивающих увеличенные габаритные расстояния от проводов ВЛ до пересекаемых объектов.

2.5.4.5. При наличии ТЭО на больших переходах через водные и другие естественные преграды в качестве проводов допускается применять стальные канаты из оцинкованных проволок и стальные канаты из плакированных алюминием проволок а также провод с витым композитным сердечником из углеродного волокна.

2.5.4.6. Срок службы проводов и грозозащитных тросов на ВЛ напряжением 35 кВ и выше должен быть не менее 50 лет.

2.5.4.7. На магистралях ВЛ 6-20 кВ следует применять сталеалюминиевый неизолированный провод или защищенный провод сечением не менее 70 мм2. На линейных ответвлениях (отпайках) от магистралей рекомендуется применение сталеалюминиевых проводов или защищенных проводов сечением не менее 35 мм2.

2.5.4.8. Защищенные провода рекомендуется применять на ВЛ 6-110 кВ в первую очередь:

- при прохождении трассы ВЛ по населенной местности;
- при прохождении ВЛ по лесным массивам;
- при пересечении ВЛ водных преград;
- при отсутствии возможности соблюдения габаритных расстояний при прохождении ВЛ в стеснённых условиях;
- при совместной подвеске с ВЛИ 0,4 кВ.

При соответствующем ТЭО допускается на ВЛ 6-35 кВ применение самонесущего кабеля.».

8. Пункты 2.5.4.10 - 2.5.4.14 8 раздела «Провода и грозозащитные тросы» Положения считать соответственно пп. 2.5.4.9 – 2.5.4.13.

9. Изложить пункт 2.10.10 раздела 2.10 «Система учета электрической энергии» Положения в следующей редакции:

«2.10.10. Для защиты приборов учета и (или) измерительного комплекса коммерческого и технического учета электрической энергии от несанкционированного доступа должно применяться пломбирование клеммных крышек приборов учета и испытательных коробок, а также испытательных и промежуточных клеммников цепей тока и напряжения, идентификация и аутентификация субъектов и объектов доступа. При подключении приборов учета и (или) измерительных комплексов коммерческого и технического учета электрической энергии к беспроводным сетям связи операторов сотовой связи защита информации от

несанкционированного доступа должна обеспечиваться путем применения выделенного APN (VPN) оператора сети передачи данных и топологии сети «Звезда» (Hub and Spoke).».

10. Изложить главу 3.6 «Информационная безопасность» Положения в следующие редакции:

«3.6. Информационная безопасность.

3.6.1. Цели и задачи информационной безопасности.

Цели: Обеспечение устойчивого функционирования критической информационной инфраструктуры субъектов электросетевого комплекса группы компаний «Россети» (далее – Субъекты) при проведении в отношении нее компьютерных атак, предотвращение неправомерного доступа к обрабатываемой информации, уничтожение такой информации, ее модифицирование, блокирование и распространения, а также иных неправомерных действий в отношении такой информации.

Задачи: Создание системы безопасности объектов критической информационной инфраструктуры (далее – ОКИИ) и обеспечение ее функционирования, в частности:

- повышение надежности и безопасности ОКИИ электросетевого комплекса группы компаний «Россети» за счет поставки цифрового оборудования, систем и технических средств защиты информации, обладающих минимальным набором встроенных функций безопасности и соответствующих по своим функциональным характеристикам требованиям нормативно-технической документации в области безопасности информации и условиям применения;
- в рамках создания, модернизации, эксплуатации ОКИ проведение регулярной оценки масштаба возможных последствий для Общества, социальных, политических, экономических, экологических последствий, а также последствий для обеспечения обороны страны, безопасности государства и правопорядка в случае возникновения компьютерных инцидентов на ОКИИ группы компаний «Россети», присвоение объектам информационной инфраструктуры одной из категорий значимости;
- обеспечение технологической безопасности и независимости от импортного оборудования, технических устройств, комплектующих, услуг (работ) иностранных компаний и использования иностранного программного обеспечения на объектах электросетевого комплекса за счет замещения программного обеспечения, микроконтроллеров и интегральных схем, а также применения в приоритетном порядке только такого программного обеспечения, сведения о котором включены в единый реестр российских программ для электронных вычислительных машин и баз данных;
- разработка корпоративных стандартов в области информационной безопасности;
- обеспечение безопасности ОКИИ в процессе эксплуатации:

- предотвращение неправомерного доступа к информации, обрабатываемой объектами информационной инфраструктуры, уничтожения такой информации, ее модифицирования, блокирования, копирования, предоставления и распространения, а также иных неправомерных действий в отношении такой информации;
- недопущение воздействия на технические средства обработки информации, в результате которого может быть нарушено и (или) прекращено функционирование ОКИИ и обеспечивающих (управляемых, контролируемых) им процессов;
- автоматизация процессов обнаружения и предупреждения компьютерных атак на ОКИИ энергетического комплекса группы компаний Россети с помощью алгоритмов машинного обучения и эвристического анализа;
- обеспечение непрерывного функционирования технических средств защиты информации;
- проведение регулярной инструментальной оценки эффективности подсистемы безопасности ОКИИ энергетического комплекса группы компаний Россети;
- обеспечение максимально быстрого восстановления (самовосстановления) ОКИИ;
- взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;
- применение риск-ориентированного управления активами информационной инфраструктуры, организации в рамках процесса эксплуатации проверки и установки критических обновлений программного обеспечения для элементов сети;
- обеспечение безопасности ОКИИ в процессе вывода из эксплуатации;
- проведение внутреннего контроля в области обеспечения безопасности ОКИИ путем осуществления плановых или внеплановых проверок;
- повышение уровня знаний работников по вопросам информационной безопасности, организация (пере)подготовки инженеров, техников, администраторов и операторов по вопросам информационной безопасности.

3.6.2. Основные принципы развития

Система безопасности объектов информационной инфраструктуры должна создаваться в соответствии с требованиями и положениям Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и Федерального

закона от 27.07.2006 № 152-ФЗ «О персональных данных», а также соответствующими подзаконными нормативно-правовыми актами.

Система безопасности объектов информационной инфраструктуры территориально-распределительных комплексов должна создаваться как типовая система безопасности, включающая силы и средства, предназначенные для обнаружения, предупреждения компьютерных атак и ликвидации последствий компьютерных инцидентов.

Принимаемые меры по обеспечению безопасности ОКИИ не должны оказывать отрицательного влияния на функционирование АСТУ, обмен технологической информацией, функций дистанционного управления электросетевым оборудованием и интеллектуальными устройствами из удаленных центров управления группы компаний «Россети» (ЦУС) и из диспетчерских центров АО «СО ЕЭС».

Результатом обеспечения безопасности информационной инфраструктуры должно стать сохранение достигнутых эффектов в части обеспечения надежности, технологической и экономической эффективности электроснабжения и других стратегических целей цифровой трансформации электроэнергетики России.

3.6.3. Основные требования

3.6.3.1. Объектами защиты в контексте обеспечения безопасности информационной инфраструктуры и обрабатываемой информации являются:

- корпоративные информационные системы (в том числе машинные носители информации, автоматизированные рабочие места, серверы, средства обработки буквенно-цифровой, графической, видео- и речевой информации, микропрограммное, общесистемное, прикладное программное обеспечение), обеспечивающие устойчивость финансово-хозяйственной деятельности;
- автоматизированные системы управления (в том числе автоматизированные рабочие места, промышленные серверы, программируемые логические контроллеры, производственное, технологическое оборудование (исполнительные устройства) имеющее функции как локального, так и дистанционного управления, либо имеющее функционирующие интерфейсы сетевого взаимодействия, микропрограммное, общесистемное, прикладное программное обеспечение), обеспечивающие надежное снабжение потребителей электроэнергией;
- корпоративные и технологические информационно-телекоммуникационные сети (в том числе телекоммуникационное оборудование, программное обеспечение, система управления, линии связи), формирующие единое информационное пространство и цифровую среду взаимодействия;
- сети электросвязи, используемые для организации взаимодействия объектов;

• архитектура и конфигурация информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, информация (данные) о параметрах (состоянии) управляемого (контролируемого) объекта или процесса (в том числе входная (выходная) информация, управляющая (командная) информация, контрольно-измерительная информация, персональные данные, иная критически важная (технологическая) информация, в том числе представляющая коммерческую ценность в силу неизвестности третьим лицам.

3.6.3.2. Обеспечение безопасности значимых ОКИИ осуществляется в зависимости от установленной категории значимости объектов в соответствии с требованиями, установленными федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации.

3.6.3.3. Обеспечение безопасности ОКИИ без установленной категории значимости осуществляется в соответствии с организационно-распорядительными документами группы компаний «Россети» требованиями настоящей Технической политики.

3.6.3.4. Для обеспечения безопасности ОКИИ, являющихся информационными системами персональных данных, настоящие Требования применяются с учетом Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 01.11.2012 № 1119.

3.6.3.5. В случае если объектом защиты является информация при осуществлении переводов денежных средств, то в соответствии с положением Банка России от 04.06.2020 № 719-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств» необходимо руководствоваться требованиями к обеспечению защиты информации при осуществлении переводов денежных средств, определяемыми во внутренних документах оператора по переводу денежных средств, банковского платежного агента (субагента), оператора платежных систем, оператора услуг платежной инфраструктуры.

3.6.3.6. В зависимости от категории значимости, требуемого уровня защищенности и актуальных угроз безопасности информации в системе безопасности ОКИИ должны быть реализованы следующие организационные и технические меры:

- идентификация и аутентификация (ИАФ);
- управление доступом (УПД);
- ограничение программной среды (ОПС);
- защита машинных носителей информации (ЗНИ);

- аудит безопасности (АУД);
- антивирусная защита (АВЗ);
- предотвращение вторжений (компьютерных атак) (СОВ);
- обеспечение целостности (ОЦЛ);
- обеспечение доступности (ОДТ);
- защита технических средств и систем (ЗТС);
- защита информационной (автоматизированной) системы и ее компонентов (ЗИС);
- планирование мероприятий по обеспечению безопасности (ПЛН);
- управление конфигурацией (УКФ);
- управление обновлениями программного обеспечения (ОПО);
- реагирование на инциденты информационной безопасности (ИНЦ);
- обеспечение действий в нештатных ситуациях (ДНС);
- информирование и обучение персонала (ИПО).

3.6.3.7. В качестве организационных мер по обеспечению безопасности ОКИИ применяется:

- организация контроля физического доступа к программно-аппаратным средствам компонент ОКИИ и его линиям связи;
- реализация правил разграничения доступа, регламентирующих права доступа субъектов доступа к объектам доступа, и введение ограничений на действия пользователей, а также на изменение условий эксплуатации, состава и конфигурации программных и программно-аппаратных средств;
- описание в организационно-распорядительных документах действий пользователей и администраторов компонент ОКИИ по реализации организационных мер;
- определение администратора безопасности ОКИИ;
- отработка действий пользователей и администраторов ОКИИ по реализации мер по обеспечению безопасности ОКИИ и восстановлению информационной инфраструктуры и обрабатываемой информации;
- повышение квалификации специалистов по ИБ, повышение осведомленности пользователей.

3.6.3.7.1. Технические меры по обеспечению информационной безопасности реализуются посредством преимущественного использования операционных систем из реестра Российского программного обеспечения, и следующих классов программных и программно-аппаратных средств – средств защиты информации (в том числе встроенных в общесистемное, прикладное программное обеспечение):

- средства защиты информации от несанкционированного доступа, в том числе средства идентификации и аутентификации, управления доступом, ограничения программной среды, защиты машинных носителей и информации, контроля целостности;

- межсетевые экраны уровня сети, уровня логических границ сети;
- межсетевые экраны уровня промышленной сети;
- средства обнаружения (предотвращения) вторжений (компьютерных атак) уровня сети, контроля и анализа сетевого трафика;
- средства регистрации и управления событиями безопасности;
- средства предупреждения компьютерных атак;
- средства защиты информации и данных при их передаче по каналам связи;
- средства защищенного удаленного доступа в ЛВС, в том числе средства терминального доступа;
- средства резервного копирования, в том числе средства создания и хранения резервных копий;
- средства управления ключевой информацией;
- средства (системы) контроля (анализа) защищенности, аудита безопасности;
- средства антивирусной защиты АРМ административно-управленческого персонала;
- средства антивирусной защиты АРМ производственного персонала, промышленных серверов;
- средства антивирусной защиты уровня сети, потовых и веб-серверов, файловых хранилищ, средства защиты от спама;
- средства защиты информации при использовании мобильных устройств;
- средства контроля действий по внесению изменений;
- средства от угроз отказа в обслуживании (DOS, DDOS-атак);
- средства управления перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных.

Средства защиты информации от несанкционированного доступа включают следующие механизмы защиты (в том числе встроенные в общесистемное, прикладное программное обеспечение и (или) программно-аппаратные средства):

- средства доверенной загрузки;
- идентификация и аутентификация пользователей;
- дискреционный контроль доступа пользователей; мандатный контроль доступа пользователей и процессов;
- маркировка документов и контроль их вывода на печать;
- защита ввода и вывода информации на отчуждаемый физический носитель;
- регистрация событий безопасности в журнале событий;
- контроль целостности критичных файлов и данных;
- контроль доступа к периферийным устройствам и портам ввода-вывода;

• гарантированное удаление данных на дисках и выборочное затирание файлов и др.

3.6.3.8. Базовый набор технических мер включает:

• средства защиты информации от несанкционированного доступа (включая встроенные функции безопасности в общесистемное, прикладное программное обеспечение и (или) программно-аппаратные средства);

• межсетевые экраны уровня сети;

• средства обнаружения (предотвращения) вторжений (компьютерных атак) уровня сети, уровня сервера, автоматизированного рабочего места;

• средства антивирусной защиты почтовых и веб-серверов, файловых хранилищ и автоматизированных рабочих мест;

• средства защиты информации и данных при их передаче по каналам связи;

• средства защищенного удаленного доступа в ЛВС, в том числе средства терминального доступа, двухфакторной аутентификации;

• средства резервного копирования, в том числе средства создания и хранения резервных копий.

Базовый набор мер по обеспечению безопасности подлежит адаптации в соответствии с актуальными угрозами безопасности информации, применяемыми информационными технологиями и особенностями функционирования ОКИИ. При этом из базового набора могут быть исключены меры, непосредственно связанные с информационными технологиями, не используемыми в составе ОКИИ, или не свойственными характеристиками.

3.6.3.9. В качестве средств защиты информации в приоритетном порядке подлежат применению средства защиты информации, встроенные в программное обеспечение и (или) программно-аппаратные средства (при их наличии).

3.6.3.10. В случае невозможности реализации заявленных целей встроенными средствами защиты информации соответствующий функционал должен обеспечиваться наложенными средствами защиты информации.

3.6.3.11. Для обеспечения безопасности информационно-телекоммуникационных сетей настоящие Требования применяются наряду с нормативными правовыми актами федерального органа исполнительной власти, осуществляющего функции по выработке и реализации государственной политики и нормативно-правовому регулированию в области связи, а также ГОСТ Р 62443 «Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы», ГОСТ Р 56498-2015 МЭК 62443-3:2008 Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 3. Защищенность (кибербезопасность) промышленного процесса измерения и управления.

3.6.3.12. В качестве цифрового оборудования, выполняющего функции граничного маршрутизатора, имеющего доступ к информационно-телекоммуникационной сети "Интернет", применяется цифровое оборудование с программным обеспечением, прошедшим оценку соответствия требованиям руководящих документов ФСТЭК России по безопасности информации в форме сертификации.

3.6.3.13. Технические средства защиты информации должны эксплуатироваться в соответствии с инструкциями (правилами) по эксплуатации, разработанными разработчиками (производителями) этих средств, и иной эксплуатационной документацией на технические средства защиты информации.

При установке и настройке технических средств защиты информации должно обеспечиваться выполнение ограничений на эксплуатацию этих средств, в случае их наличия в эксплуатационной документации.

3.6.3.14. Применяемые технические средства защиты информации должны быть обеспечены гарантийной и технической поддержкой.

3.6.3.15. Порядок создания информационных систем, автоматизированных систем управления, систем управления информационно-телекоммуникационными сетями, этапность 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», положениям Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и подзаконным нормативно-правовым актам, а также организационно-распорядительным документам Субъекта.

На стадиях (этапах) жизненного цикла в ходе создания (модернизации) объектов информационной инфраструктуры проводиться:

- анализ угроз безопасности информации и разработка модели угроз безопасности информации или ее уточнение (при ее наличии), определение категории значимости, требуемого уровня защищенности ОКИИ;
- проектирование организационных и технических мер по обеспечению информационной безопасности ОКИИ, разработка рабочей (эксплуатационной) документации на ОКИИ (в части обеспечения его безопасности);
- внедрение организационных и технических мер по обеспечению информационной безопасности ОКИИ, предварительные испытания, анализ уязвимостей, опытная эксплуатация, приемочные испытания и ввод в эксплуатацию ОКИИ и его подсистемы безопасности;
- регламентация процессов обеспечения информационной безопасности ОКИИ в ходе эксплуатации.

Проектные решения по обеспечению информационной безопасности объектов нового строительства, расширения, реконструкции, технического перевооружения или модернизации объектов электросетевого комплекса должны выполняться в соответствии с типовыми техническими решениями, утвержденных организационно-распорядительными документами Общества.

3.6.3.16. Результаты проектирования системы безопасности объектов информационной инфраструктуры отражаются в проектной документации (эскизном (техническом) проекте и (или) в рабочей документации), разрабатываемой с учетом ГОСТ 34.201-2020 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем» (далее – ГОСТ 34.201-2020) и стандартов организации, в соответствии с установленной категории значимости.

3.6.3.17. Защита информации при использовании технологий виртуализации осуществляется в соответствии с ГОСТ Р 56938-2016 «Защита информации при использовании технологии виртуализации. Общие положения».

3.6.3.18. Требования в отношении функциональной безопасности автоматизированных систем управления предприятием, оперативно-технологического управления, технологического управления должны соответствовать ГОСТ Р МЭК 61508-1-2012, 61508-2-2012, 61508-3-2018.

3.6.4. Оценка соответствия по требованиям безопасности информации

3.6.4.1. Ввод в эксплуатацию ОКИИ допускается при наличии протокола (акта) приемочных испытаний с положительным заключением о соответствии и эффективности принятых организационно-технических мер защиты установленным требованиям по обеспечению безопасности.

3.6.4.2. Для обеспечения безопасности ОКИИ должны применятся технические средства защиты информации, прошедшие оценку на соответствие требованиям по безопасности информации в формах обязательной сертификации, испытаний или приемки.

Подтверждение соответствия технических средств защиты информации требованиям по безопасности информации, в том числе требованиям по совместимости с автоматизированными системами управления технологическими процессами выполняется в рамках проверки качества (аттестации), изложенной в разделе 3.6.6 настоящего Положения.

3.6.4.3. Оценка соответствия и эффективности принятых организационно-технических мер защиты ОКИИ установленным требованиям по обеспечению безопасности проводятся Субъектами самостоятельно или с привлечением организаций, имеющих в соответствии с законодательством Российской Федерации лицензии на соответствующую деятельность в области защиты информации.

Повторная оценка соответствия принятых организационно-технических мер защиты установленным требованиям по обеспечению безопасности проводится через три года.

3.6.4.4. Оценка соответствия и эффективности принятых организационно-технических мер защиты ОКИИ, обрабатывающих ПДн, проводиться по решению Субъекта с привлечением организации, имеющей в соответствии с законодательством Российской Федерации лицензии на соответствующую деятельность в области защиты информации.

3.6.4.5. Оценка соответствия и эффективности принятых организационно-технических мер защиты ОКИИ взаимодействующих с государственными информационными системами проводиться в обязательном порядке с привлечением организаций, имеющих в соответствии с законодательством Российской Федерации, лицензии на соответствующую деятельность в области защиты информации.

3.6.5. Ограничения по применению технологий/оборудования

3.6.5.1. При выборе средств защиты информации, в том числе сопутствующего встроенного программного обеспечения, должно учитываться возможное наличие ограничений со стороны разработчиков (производителей) или иных лиц на применение этих средств на всей территории Российской Федерации.

3.6.5.2. При реализации технических мер по защите информации не допускается применение алгоритма криптографического хеширования SHA-1, протоколов SNMP v1, v2.

3.6.5.3. В ОКИИ не допускается:

- наличие удаленного доступа непосредственно (напрямую) к программным и программно-аппаратным средствам, в том числе средствам защиты информации, для обновления или управления со стороны лиц, не являющихся работниками ПАО «Россети», а также работниками его дочерних и зависимых обществ;
- наличие локального доступа к программным и программно-аппаратным средствам, в том числе средствам защиты информации, для обновления или управления со стороны лиц, не являющихся работниками ПАО «Россети», а также работниками его дочерних и зависимых обществ без контроля со стороны Субъекта;
- передача информации, в том числе технологической информации, разработчику (производителю) программных и программно-аппаратных средств, в том числе средств защиты информации, или иным лицам без контроля со стороны Субъекта.

В случае технической необходимости, организация удаленного доступа к программным и программно-аппаратным средствам, в том числе средствам защиты информации, в объекте принимаются организационные и технические меры по обеспечению безопасности такого доступа, предусматривающие:

• определение лиц и устройств, которым разрешен удаленный доступ к программным и программно-аппаратным средствам объекта, предоставление им минимальных полномочий при доступе к этим средствам;

• контроль доступа к программным и программно-аппаратным средствам объекта;

• защиту информации и данных при их передаче по каналам связи при удаленном доступе к программным и программно-аппаратным средствам объекта;

• мониторинг и регистрацию действий лиц, которым разрешен удаленный доступ к программным и программно-аппаратным средствам объекта, а также инициируемых ими процессов, анализ этих действий в целях выявления фактов неправомерных действий;

• обеспечение невозможности отказа лиц от выполненных действий при осуществлении удаленного доступа к программным и программно-аппаратным средствам объекта;

• обеспечение двухфакторной аутентификации при удаленном доступе.

3.6.5.4. Входящие в состав ОКИИ программные и программно-аппаратные средства, осуществляющие хранение и обработку информации, должны размещаться на территории Российской Федерации (за исключением случаев, когда размещение указанных средств осуществляется в зарубежных обособленных подразделениях Субъекта (филиалах, представительствах), а также случаев, установленных законодательством Российской Федерации и (или) международными договорами Российской Федерации).

3.6.5.5. Эксплуатационно-техническое обслуживание, техническая поддержка программных и программно-аппаратных средств, в том числе СУБД должна оказываться Правообладателем (разработчиком) или представителем Правообладателя, зарегистрированным на территории Российской Федерации.

3.6.6. Проверка качества (аттестация) цифрового оборудования, систем и технических средств защиты информации

3.6.6.1. Проверке качества (аттестации) подлежит цифровое оборудование и системы, обеспечивающие поиск, сбор, хранение, обработку, представление, распространение цифровой информации на объектах электросетевого комплекса группы компаний «Россети», в том числе технические средства защиты информации.

3.6.2. Проверка качества (аттестация) цифрового оборудования, систем и технических средств защиты информации является внутренней системой проверки Общества и направлена на подтверждение:

• отсутствия уязвимостей и недостатков в составе программного обеспечения, способных привести к нарушениям проектных значений параметров выполнения целевых функций и (или) привести к технологическим нарушениям;

• выполнение встроенными средствами защиты информации минимального набора функций безопасности, соответствующих по своим функциональным характеристикам требованиям нормативно-технической документации в области безопасности информации и условиям применения на объектах электросетевого комплекса Общества и ДЗО;

• наличие в эксплуатационной документации описания условий безопасной эксплуатации;

• совместимость технических средств защиты информации с автоматизированными системами управления технологическими процессами;

• реализации производителем-изготовителем, разработчиком мер по разработке безопасного программного обеспечения на всех этапах жизненного цикла в соответствии с ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования»;

• реализации производителем-изготовителем, разработчиком процедур устранения недостатков, уязвимостей и обновления программного обеспечения;

• отсутствия нарушений авторских прав на передачу и использование программного обеспечения на объектах электросетевого комплекса Общества и ДЗО.

3.6.6.2. Проверка качества (аттестация) осуществляется на соответствие требованиям по безопасности информации, установленным нормативно-правовыми актами Российской Федерации и организационно-распорядительными документами Общества и ДЗО, а также на соответствие техническим условиям, согласованными производителем-изготовителем, разработчиком с Обществом.

3.6.6.3. Проверку качества (аттестацию) на соответствие требованиям по безопасности информации организует Общество в соответствии с решением, принятым Правлением Общества, в порядке, регламентированным приказом 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».

3.6.6.4. Результаты проверки качества (аттестации) оформляются заключением аттестационной комиссии и утверждается Обществом с учетом выводов о возможности применения цифрового оборудования, систем и технических средств защиты информации на объектах электросетевого комплекса группы компаний «Россети».

11. Изложить пункты 4.6.3 и 4.6.6 раздела 4.6 «Импортозамещение в электросетевом комплексе» Положения в следующей редакции:

«4.6.3. В рамках реализации импортозамещения постановлением Правительства Российской Федерации от 17.07.2015 № 719 «О подтверждении производства промышленной продукции на территории Российской

Федерации» определены требования к промышленной продукции, предъявляемые в целях ее отнесения к продукции, произведенной в Российской Федерации, постановлением Правительства Российской Федерации от 16.09.2016 № 925 «О приоритете товаров российского происхождения, работ, услуг, выполняемых, оказываемых российскими лицами, по отношению к товарам, происходящим из иностранного государства, работам, услугам, выполняемым, оказываемым иностранными лицами» установлен приоритет товаров российского происхождения по отношению к товарам, произведенным на территории иностранного государства.

Постановлением Правительства РФ от 03.122020 № 2013 «О минимальной доле закупок товаров российского происхождения» установлена минимальная доля закупок товаров российского происхождения. В рамках указанного Постановления товаром российского происхождения признается товар, включенный:

- в реестр промышленной продукции, произведенной на территории Российской Федерации, или в реестр промышленной продукции, произведенной на территории государства - члена Евразийского экономического союза, за исключением Российской Федерации, предусмотренные постановлением Правительства Российской Федерации от 30.042020 № 616 «Об установлении запрета на допуск промышленных товаров, происходящих из иностранных государств, для целей осуществления закупок для государственных и муниципальных нужд, а также промышленных товаров, происходящих из иностранных государств, работ (услуг), выполняемых (оказываемых) иностранными лицами, для целей осуществления закупок для нужд обороны страны и безопасности государства»;

- в единый реестр российской радиоэлектронной продукции, предусмотренный постановлением Правительства Российской Федерации от 10.07.2019 № 878 «О мерах стимулирования производства радиоэлектронной продукции на территории Российской Федерации при осуществлении закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд, о внесении изменений в постановление Правительства Российской Федерации от 16.09.2016 № 925 и признании утратившими силу некоторых актов Правительства Российской Федерации".

4.6.6. Приоритетными направлениями технической политики в области импортозамещения являются:

- минимизация использования импортного оборудования и материалов при формировании проектных решений и технических заданий, а именно первоочередное использование в технических заданиях на проектирование и проектных решениях оборудования и комплектующих отечественного производства (включенных в Реестр промышленной

продукции, произведенной на территории Российской Федерации, Реестр промышленной продукции, произведенной на территории государства - члена Евразийского экономического союза, за исключением Российской Федерации, или Единый реестр российской радиоэлектронной продукции), оборудования и комплектующих, локализация которых осуществляется полностью или частично за счет субсидий, представляемых из федерального бюджета в соответствии с соглашениями, заключаемыми производителями с Минпромторг России, а также оборудования и комплектующих, которые считаются произведенными на территории Российской Федерации в соответствии с требованиями постановления Правительства Российской Федерации от 17.07.2015 № 719 «О подтверждении производства промышленной продукции на территории Российской Федерации».

Оборудование и комплектующие импортного производства допускается применять по согласованию профильных структурных подразделений ПАО «Россети», курирующих вопросы технической политики и международного сотрудничества, при наличии соответствующего обоснования (в случае отсутствия аналогов, произведенных на территории Российской Федерации, отвечающих всем техническим требованиям, предъявляемым к ним заказчиком).

- типизация применяемого в электросетевом комплексе оборудования за счет разработки и внедрения стандартов организации на электротехническую продукцию, с целью учета производственных возможностей отечественных производителей и исключения избыточных требований к оборудованию, приводящих к необходимости закупки импортного оборудования;
- развитие локализации производства высокотехнологичного оборудования и компонентов на территории Российской Федерации.».