СОПОСТАВЛЕНИЕ ТРЕБОВАНИЙ ПРИКАЗА ФСТЭК ОТ 14 МАРТА 2014 Г. № 31 С ТРЕБОВАНИЯМИ МЕЖДУНАРОДНЫХ СТАНДАРТОВ

Специалисты Positive Technologies сопоставили меры защиты, установленные приказом ФСТЭК от 14 марта 2014 г. № 31, с требованиями следующих документов:

- семейство отраслевых стандартов NERC Critical Infrastructure Protection (NERC CIP);
- семейство стандартов ISA/IEC 62443 Industrial Automation and Control Systems Security;
- рекомендации NIST SP 800-82 «Guide to Industrial Control Systems (ICS) Security» и NIST SP 800-53 «Security and Privacy Controls for Federal Information Systems and Organizations».

В целом приказ предусматривает более широкий набор требований, чем указанные документы. По результатам сопоставления можно отметить ряд мер защиты, которыми можно было бы дополнить требования приказа:

1. Разделение на сетевом уровне корпоративной ЛВС и технологических сетей (ISA-62443-2-1, NIST – SP800-82). Требование о необходимости сегментирования ЛВС в приказе присутствует (ЗИС-17), однако в соответствующем методическом документе предлагаем явно отметить необходимость отделения технологических сетей от корпоративных.
2. Инвентаризация компонентов АСУ ТП. Подобное требование есть во всех рассмотренных документах, при этом инвентаризация предусматривает не только идентификацию компонентов, участвующих в технологических процессах, но и хранение дополнительной информации, позволяющей определить их назначение, степень критичности и т.п.
3. Проверка персонала перед предоставлением допуска к работе с АСУ ТП (NERC CIP, ISA/IEC 62443)
4. Мероприятия, связанные с увольнением персонала (блокирование учетных записей, смена паролей и т.п. – ISA-62443-2-1, NERC-CIP).

Кроме того, представляется полезным определить основные недостатки в обеспечении ИБ, которые встречаются в системах АСУ ТП, как это сделано в ISA-62443-2-1 и NIST SP 800-82.

ПУНКТ ИЗ ДОКУМЕНТА	NERC-CIP (REV5 - DRAFT) (NOVEMBER 7, 2011)	IEC-62443-2-1 (ISA99.02.01) (NOVEMBER 28, 2012)	NIST – SP800-82 (JUNE 2011)	NIST – SP800-53 (SUPPLEMENT SP800-82 STANDART*)
ИАФ.0 Разработка правил и процедур (политик) идентификации и аутентификации субъектов доступа и объектов доступа	CIP-003-5 R2 CIP-007-5 R5	11.7.7 Identification and Authentication Policy and Procedures	Supplement SP800-53 standart	IA-1
ИАФ.1 Идентификация и аутентификация пользователей, являющихся работниками оператора	CIP-007-5 5.1	11.5.2 User identification and authentication	6.3.1 Identification and Authentication	NONE
ИАФ.2 Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных	NONE	11.5.2 User identification and authentication	6.3.1 Identification and Authentication	NONE
ИАФ.3 Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	CIP-004-5 R.6	11.7.8 Identifier management	In accordance with SP800-53	IA-5
ИАФ.4 Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	NONE	11.7.9 Authenticator management	In accordance with SP800-53	IA-5
ИАФ.5 Исключение отображения для пользователя действительного значения аутентификационной информации и (или) количества вводимых символов (защита обратной связи при вводе аутентификационной информации)	NONE	NONE	Supplement SP800-53 standart	IA-6
ИАФ.6 Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	NONE	6.2 External parties	6.2.1 Personnel Security	NONE
ИАФ.7 Идентификация и аутентификация объектов файловой системы, запускаемых и исполняемых модулей, объектов систем управления базами данных, объектов, создаваемых прикладным и специальным программным обеспечением, иных объектов доступа	NONE	NONE	partially applicable 6.3.1 Identification and Authentication	NONE
УПД.0 Разработка правил и процедур (политик) управления доступом субъектов доступа к объектам доступа	CIP-003-5 R2 CIP-007-5 R5	11.1 Access control policy	Supplement SP800-53 standart	AC-1
УПД.1	NONE	11.2.5 Account Management	6.3.2 Access Control	AC

ПУНКТ ИЗ ДОКУМЕНТА	NERC-CIP (REV5 - DRAFT) (NOVEMBER 7, 2011)	IEC-62443-2-1 (ISA99.02.01) (NOVEMBER 28, 2012)	NIST – SP800-82 (JUNE 2011)	NIST – SP800-53 (SUPPLEMENT SP800-82 STANDART*)
Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей			In accordance with SP800-53	
УПД.2 Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	NONE	11.6 Application and information access control	6.3.2 Access Control In accordance with SP800-53	AC
УПД3 Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами автоматизированной системы управления, а также между автоматизированными системами управления	partially applicable CIP-005-5 R2 CIP-007-5 R1	11.4 Network access control	5 Network Architecture	NONE
УПД.4 Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование автоматизированной системы управления	CIP-004-5 R6 In accordance with CIP-007-5 R5	11.6 Application and information access control	6.3.2 Access Control In accordance with SP800-53	AC
УПД.5 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование автоматизированной системы управления	CIP-004-5 R6 In accordance with CIP-007-5 R5	11.2.2 Privilege management	6.3.2 Access Control In accordance with SP800-53	AC
УПД.6 Ограничение неуспешных попыток входа в автоматизированную систему управления (доступа к системе)	CIP-007-5 5.6	11.5.1 Secure log-on procedures	6.3.2 Access Control In accordance with SP800-53	AC
УПД.7 Предупреждение пользователя при его входе в автоматизированную систему управления о том, что в ней реализованы меры защиты информации, и о необходимости соблюдения им установленных владельцем правил обработки информации	NONE	NONE	6.3.2 Access Control In accordance with SP800-53	AC
УПД.8 Оповещение пользователя после успешного входа в автоматизированную систему управления о его предыдущем входе в автоматизированную систему управления	NONE	11.5.1 Secure log-on procedures	6.3.2 Access Control In accordance with SP800-53	AC
УПД.9 Ограничение числа параллельных сеансов доступа для	NONE	NONE	6.3.2 Access Control In accordance with SP800-	AC

ПУНКТ ИЗ ДОКУМЕНТА	NERC-CIP (REV5 - DRAFT) (NOVEMBER 7, 2011)	IEC-62443-2-1 (ISA99.02.01) (NOVEMBER 28, 2012)	NIST – SP800-82 (JUNE 2011)	NIST – SP800-53 (SUPPLEMENT SP800-82 STANDART*)
каждой учетной записи пользователя автоматизированной системы управления			53	
УПД.10 Блокирование сеанса доступа в автоматизированную систему управления после установленного времени бездействия (неактивности) пользователя или по его запросу	NONE	11.5.5 Session time-out	6.3.2 Access Control In accordance with SP800-53	AC
УПД.11 Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации	NONE	11.4.9 Permitted Actions Without Identification or Authentication	6.3.2 Access Control In accordance with SP800-53	AC
УПД.12 Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки	NONE	NONE	NONE	NONE
УПД.13 Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	CIP-005-5 R.1	11.4.6 Network connection control 11.4.10 Remote Access	5.8.2 Remote Support Access	NONE
УПД.14 Регламентация и контроль использования в автоматизированной системе управления технологий беспроводного доступа	CIP-003-5 2.2	11.7.3 Wireless Access Restrictions	6.3.2.5 Wireless	NONE
УПД.15 Регламентация и контроль использования в автоматизированной системе управления мобильных технических средств	NONE	11.7.1 Mobile computing and communications 11.7.4 Use Control for Portable and Mobile Devices	Supplement SP800-53 standart	AC-19
УПД.16 Управление взаимодействием с автоматизированными (информационными) системами сторонних организаций (внешние системы)	NONE	11.4.11 Use of External Information Systems 6.2 External parties	Supplement SP800-53 standart	SC
УПД.17 Обеспечение доверенной загрузки средств вычислительной техники	NONE	NONE	NONE	NONE
ОПС.0 Разработка правил и процедур (политик) ограничения программной среды	CIP-003-5 R2 CIP-010-1 1.1	12.6.2 Configuration Management Policy and Procedures	6.2.4 Configuration Management In accordance with SP800-53	CM
ОПС.1 Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров	NONE	12.2 Correct processing in applications 12.4 Security of system files	6.2.4 Configuration Management In accordance with SP800-	CM

ПУНКТ ИЗ ДОКУМЕНТА	NERC-CIP (REV5 - DRAFT) (NOVEMBER 7, 2011)	IEC-62443-2-1 (ISA99.02.01) (NOVEMBER 28, 2012)	NIST – SP800-82 (JUNE 2011)	NIST – SP800-53 (SUPPLEMENT SP800-82 STANDART*)
запуска компонентов, контроль за запуском компонентов программного обеспечения			53	
ОПС.2 Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения	CIP-010-1 1.1	12.4.1 Control of operational software	6.2.4 Configuration Management In accordance with SP800-53	CM
ОПС.3 Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов	CIP-010-1 1.1	12.4.1 Control of operational software	6.2.4 Configuration Management ☐ In accordance with SP800-53	CM
ОПС.4 Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов	NONE	NONE	NONE	NONE
ЗНИ.0 Разработка правил и процедур (политик) защиты машинных носителей	CIP-003-5 R2 CIP-007-5 1.2	10.7.1 Management of removable media	Supplement SP800-53 standart	MP
ЗНИ.1 Учет машинных носителей информации	NONE	10.7.5 Media labeling	6.2.7 Media Protection In accordance with SP800-53	MP
ЗНИ.2 Управление доступом к машинным носителям информации	NONE	10.7.3 Information handling procedures	6.2.7 Media Protection	MP
ЗНИ.3 Контроль перемещения машинных носителей информации за пределы контролируемой зоны	NONE	10.7.7 Media transport 10.8.3 Physical media in transit	6.2.7 Media Protection In accordance with SP800-53	MP
ЗНИ.4 Исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях, и (или) использования носителей информации в иных автоматизированных системах управления	NONE	10.7.3 Information handling procedures	6.2.7 Media Protection In accordance with SP800-53	MP
ЗНИ.5 Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации	CIP-007-5 1.2	NONE	6.2.7 Media Protection In accordance with SP800-53	MP

ПУНКТ ИЗ ДОКУМЕНТА	NERC-CIP (REV5 - DRAFT) (NOVEMBER 7, 2011)	IEC-62443-2-1 (ISA99.02.01) (NOVEMBER 28, 2012)	NIST – SP800-82 (JUNE 2011)	NIST – SP800-53 (SUPPLEMENT SP800-82 STANDART*)
ЗНИ.6 Контроль ввода (вывода) информации на машинные носители информации	NONE	10.7.3 Information handling procedures	6.2.7 Media Protection In accordance with SP800-53	MP
ЗНИ.7 Контроль подключения машинных носителей информации	NONE	10.7 Media handling	6.2.7 Media Protection In accordance with SP800-53	MP
ЗНИ.8 Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания)	NONE	10.7.2 Disposal of media	6.2.7 Media Protection In accordance with SP800-53	MP
РСБ.0 Разработка правил и процедур (политик) регистрации событий безопасности	CIP-003-5 R2 CIP-007-5 R4	10.10 Monitoring 10.10.7 Audit and Accountability Policy and Procedures	6.3.3 Audit and Accountability In accordance with SP800-53	AU
РСБ.1 Определение событий безопасности, подлежащих регистрации, и сроков их хранения	CIP-007-5 4.1	10.10.1 Audit logging 10.10.2 Monitoring system use 10.10.4 Administrator and operator logs	6.3.3 Audit and Accountability In accordance with SP800-53	AU
РСБ.2 Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	CIP-007-5 4.1	10.10.1 Audit logging 10.10.2 Monitoring system use	6.3.3 Audit and Accountability In accordance with SP800-53	AU
РСБ.3 Сбор, запись и хранение информации о событиях безопасности в течении установленного времени хранения	CIP-007-5 4.4	10.10.10 Audit Record Retention	6.3.3 Audit and Accountability In accordance with SP800-53	AU
РСБ.4 Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти	CIP-007-5 4.3	10.10.5 Fault logging	6.3.3 Audit and Accountability In accordance with SP800-53	AU
РСБ.5 Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них	CIP-007-5 4.5	10.10.9 Audit Monitoring, Analysis and Reporting	6.3.3 Audit and Accountability In accordance with SP800-53	AU
РСБ.6	NONE	10.10.6 Clock synchronization	6.3.3 Audit and	AU

ПУНКТ ИЗ ДОКУМЕНТА	NERC-CIP (REV5 - DRAFT) (NOVEMBER 7, 2011)	IEC-62443-2-1 (ISA99.02.01) (NOVEMBER 28, 2012)	NIST – SP800-82 (JUNE 2011)	NIST – SP800-53 (SUPPLEMENT SP800-82 STANDART*)
Генерирование временных меток и (или) синхронизация системного времени в автоматизированной системе управления			Accountability In accordance with SP800-53	
РСБ.7 Защита информации о событиях безопасности	NONE	10.10.3 Protection of log information	6.3.3 Audit and Accountability In accordance with SP800-53	AU
РСБ.8 Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей	NONE	10.10.4 Administrator and operator logs	6.3.3 Audit and Accountability In accordance with SP800-53	AU
АВЗ.0 Разработка правил и процедур (политик) антивирусной защиты	CIP-003-5 R2 CIP-007-5 R3	10.4 Protection against malicious and mobile code	6.2.6 System and Information Integrity In accordance with SP800-53	SI-3
АВЗ.1 Реализация антивирусной защиты	CIP-007-5 3.1 CIP-007-5 3.2	10.4.1 Controls against malicious code 10.4.2 Controls against mobile code 10.4.3 Malicious Code Protection	6.2.6.1 Malicious Code Detection	NONE
АВЗ.2 Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	CIP-007-5 3.3	10.4.1 Controls against malicious code	6.2.6 System and Information Integrity In accordance with SP800-53	SI-3
СОВ.0 Разработка правил и процедур (политик) обнаружения вторжений	CIP-003-5 R2 CIP-005-5 1.5	NONE	6.2 Operational Controls 6.2.6 System and Information Integrity In accordance with SP800-53	SI
СОВ.1 Обнаружение вторжений	CIP-005-5 1.5	10.6.2 Security of network services	5.4 Recommended Defense-in-Depth Architecture 6.2.6 System and Information Integrity In accordance with SP800-53	SI
СОВ.2 Обновление базы решающих правил	NONE	NONE	NONE	NONE
АНЗ.0	CIP-003-5 R2	5.1.1 Cyber security policy document	6.1.1 Security Assessment	CA

ПУНКТ ИЗ ДОКУМЕНТА	NERC-CIP (REV5 - DRAFT) (NOVEMBER 7, 2011)	IEC-62443-2-1 (ISA99.02.01) (NOVEMBER 28, 2012)	NIST – SP800-82 (JUNE 2011)	NIST – SP800-53 (SUPPLEMENT SP800-82 STANDART*)
Разработка правил и процедур (политик) контроля (анализа) защищенности	CIP-010-1 R.3	12.6 Technical Vulnerability Management	and Authorization In accordance with SP800-53	
АН3.1 Выявление, анализ уязвимостей и оперативное устранение вновь выявленных уязвимостей	CIP-007-5 2.2	12.6 Technical Vulnerability Management 12.6.1 Control of technical vulnerabilities	6.1.1 Security Assessment and Authorization In accordance with SP800-53	CA
АН3.2 Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	CIP-007-5 2.3	12.6.1 Control of technical vulnerabilities	6.2.6.3 Patch Management	NONE
АН3.3 Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации	CIP-010-1 1.4 CIP-010-1 1.5	12.6.4 Configuration Change Control 12.6.5 Monitoring Configuration Changers	6.2.4 Configuration Management ☐ In accordance with SP800-53	CM
АН3.4 Контроль состава технических средств, программного обеспечения и средств защиты информации	CIP-010-1 R.1	12.6.4 Configuration Change Control 12.6.5 Monitoring Configuration Changers	6.2.4 Configuration Management ☐ In accordance with SP800-53	CM
АН3.5 Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе	CIP-007-5 5.4	11.2.3 User password management 10.10.4 Administrator and operator logs	6.3.3 Audit and Accountability In accordance with SP800-53	AU
ОЦЛ.0 Разработка правил и процедур (политик) обеспечения целостности	CIP-003-5 R2	11.1.3 System and Information Integrity Policy and Procedures	6.2.6 System and Information Integrity In accordance with SP800-53	SI
ОЦЛ.1 Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации	NONE	11.1.3 System and Information Integrity Policy and Procedures	6.2.6 System and Information Integrity In accordance with SP800-53	SI
ОЦЛ.2 Контроль целостности информации, содержащейся в базах данных	NONE	11.7.10 Software and Information Integrity	6.2.6 System and Information Integrity In accordance with SP800-53	SI

ПУНКТ ИЗ ДОКУМЕНТА	NERC-CIP (REV5 - DRAFT) (NOVEMBER 7, 2011)	IEC-62443-2-1 (ISA99.02.01) (NOVEMBER 28, 2012)	NIST – SP800-82 (JUNE 2011)	NIST – SP800-53 (SUPPLEMENT SP800-82 STANDART*)
ОЦЛ.3 Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций	CIP-009-5 R1	10.5 Back-up	6.2.3 Contingency Planning In accordance with SP800-53	CP
ОЦЛ.4 Обнаружение и реагирование на поступление в автоматизированную систему управления незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к ее функционированию (защита от спама)	NONE	NONE	6.2.6 System and Information Integrity In accordance with SP800-53	SI
ОЦЛ.5 Контроль содержания информации, передаваемой из автоматизированной системы управления (контейнерный, основанный на свойствах объекта доступа, и контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи информации	NONE	11.7.13 Information Output Handling and Retention	6.2.6 System and Information Integrity In accordance with SP800-53	SI
ОЦЛ.6 Ограничение прав пользователей по вводу информации в автоматизированную систему управления	NONE	11.7.11 Information Input Restrictions	6.2.6 System and Information Integrity In accordance with SP800-53	SI
ОЦЛ.7 Контроль точности, полноты и правильности данных, вводимых в автоматизированную систему управления	NONE	NONE	6.2.6 System and Information Integrity In accordance with SP800-53	SI
ОЦЛ.8 Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях	NONE	NONE	6.2.6 System and Information Integrity In accordance with SP800-53	SI
ОДТ.0 Разработка правил и процедур (политик) обеспечения доступности	CIP-003-5 R2 Partially applicableCIP-009-5 R1	5.1.1 Cyber security policy document 14 Business Continuity Management	6.2.3 Contingency Planning In accordance with SP800-53	CP
ОДТ.1 Использование отказоустойчивых технических средств	CIP-003-5 R2	14.1.12 Alternate Control Site 14.2 Telecommunications Service	5.10 Redundancy and Fault Tolerance	
ОДТ.2 Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной	Partially applicable CIP-009-5 R1	14.1.12 Alternate Control Site 14.2 Telecommunications Service	5.10 Redundancy and Fault Tolerance	NONE

ПУНКТ ИЗ ДОКУМЕНТА	NERC-CIP (REV5 - DRAFT) (NOVEMBER 7, 2011)	IEC-62443-2-1 (ISA99.02.01) (NOVEMBER 28, 2012)	NIST – SP800-82 (JUNE 2011)	NIST – SP800-53 (SUPPLEMENT SP800-82 STANDART*)
системы				
ОДТ.3 Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование	Partially applicable CIP-009-5 R1	14.1.5 Testing, maintaining and re-assessing business continuity plans	5.9 Single Points of Failure 5.10 Redundancy and Fault Tolerance	NONE
ОДТ.4 Периодическое резервное копирование информации на резервные машинные носители информации	CIP-009-5 R1	14.1.13 IACS Backup	6.2.3 Contingency Planning In accordance with SP800-53	CP
ОДТ.5 Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течении установленного временного интервала	CIP-009-5 R1	14.1.11 Alternate Storage Site 14.1.14 IACS Recovery and Reconstruction	6.2.3 Contingency Planning In accordance with SP800-53	CP
ОДТ.6 Кластеризация автоматизированной системы управления и (или) ее сегментов	NONE	14.1.12 Alternate Control Site	5.10 Redundancy and Fault Tolerance	
ОДТ.7 Контроль состояния и качества предоставления поставщиком телекоммуникационных услуг вычислительных ресурсов (мощностей), в том числе по передаче информации	NONE	14.2 Telecommunication Services	NONE	NONE
ЗСВ.0 Разработка правил и процедур (политик) защиты среды виртуализации	NONE	NONE	NONE	NONE
ЗСВ.1 Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации	NONE	NONE	NONE	NONE
ЗСВ.2 Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин	NONE	NONE	NONE	NONE
ЗСВ.3 Регистрация событий безопасности в виртуальной инфраструктуре	NONE	NONE	NONE	NONE
ЗСВ.4 Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками	NONE	NONE	NONE	NONE

ПУНКТ ИЗ ДОКУМЕНТА	NERC-CIP (REV5 - DRAFT) (NOVEMBER 7, 2011)	IEC-62443-2-1 (ISA99.02.01) (NOVEMBER 28, 2012)	NIST – SP800-82 (JUNE 2011)	NIST – SP800-53 (SUPPLEMENT SP800-82 STANDART*)
информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры				
ЗСВ.5 Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией	NONE	NONE	NONE	NONE
ЗСВ.6 Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных	NONE	NONE	NONE	NONE
ЗСВ.7 Контроль целостности виртуальной инфраструктуры и ее конфигураций	NONE	NONE	NONE	NONE
ЗСВ.8 Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры	NONE	NONE	NONE	NONE
ЗСВ.9 Реализация и управление антивирусной защитой в виртуальной инфраструктуре	NONE	NONE	NONE	NONE
ЗСВ.10 Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей	NONE	NONE	NONE	NONE
ЗТС.0 Разработка правил и процедур (политик) защиты технических средств	CIP-003-5 R2 CIP-006-5 R1	9.1 Secure areas 9.2 Equipment security	6.2.2 Physical and Environmental Protection In accordance with SP800-53	PE
ЗТС.1 Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам	NONE	9.2.3 Cabling security	6.2.2 Physical and Environmental Protection In accordance with SP800-53	PE
ЗТС.2 Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования	CIP-006-5 R1	9.1 Secure areas	6.2.2 Physical and Environmental Protection In accordance with SP800-53	PE
ЗТС.3	CIP-006-5 R1	9.1 Secure areas	6.2.2 Physical and	PE

ПУНКТ ИЗ ДОКУМЕНТА	NERC-CIP (REV5 - DRAFT) (NOVEMBER 7, 2011)	IEC-62443-2-1 (ISA99.02.01) (NOVEMBER 28, 2012)	NIST – SP800-82 (JUNE 2011)	NIST – SP800-53 (SUPPLEMENT SP800-82 STANDART*)
Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования автоматизированной системы управления и помещения и сооружения, в которых они установлены		9.2 Equipment security	Environmental Protection In accordance with SP800-53	
ЗТС.4 Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	NONE	9.2.11 Access Control for Display Medium	6.2.2 Physical and Environmental Protection In accordance with SP800-53	PE
ЗТС.5 Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов)	NONE	9.2 Equipment security	6.2.2 Physical and Environmental Protection In accordance with SP800-53	PE
ЗИС.0 Разработка правил и процедур (политик) защиты автоматизированной системы и ее компонентов	CIP-003-5 R2	5. Security policy 10. Communications operating procedures	6.2.2 Physical and Environmental Protection 6.3.2 Access Control 6.3.4 System and Communications Protection 6.2.6 System and Information Integrity	PE AC SC SI
ЗИС.1 Разделение функций по управлению (администрированию) автоматизированной системы управления, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций автоматизированной системы управления	NONE	11.2.6 Separation of Duties	6.3.2 Access Control In accordance with SP800-53	AC
ЗИС.2 Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом	NONE	NONE	NONE	NONE
ЗИС.3 Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче)	NONE	10.8 Exchange of information	6.3.4 System and Communications Protection In accordance with SP800-	SC

ПУНКТ ИЗ ДОКУМЕНТА	NERC-CIP (REV5 - DRAFT) (NOVEMBER 7, 2011)	IEC-62443-2-1 (ISA99.02.01) (NOVEMBER 28, 2012)	NIST – SP800-82 (JUNE 2011)	NIST – SP800-53 (SUPPLEMENT SP800-82 STANDART*)
по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи			53	
ЗИС.4 Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации)	NONE	10.6 Network security management	6.3.4 System and Communications Protection In accordance with SP800-53	SC
ЗИС.5 Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств	NONE	NONE	NONE	NONE
ЗИС.6 Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с информацией, при обмене информацией с иными автоматизированными (информационными) системами	NONE	partially applicable 12.2.3 Message integrity	6.2.6 System and Information Integrity In accordance with SP800-53	SI
ЗИС.7 Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода	NONE	10.4.2 Controls against mobile code	6.3.4 System and Communications Protection In accordance with SP800-53	SC
ЗИС.8 Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи	NONE	NONE	NONE	NONE
ЗИС.9 Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации	NONE	NONE	NONE	NONE
ЗИС.10 Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по	NONE	NONE	6.3.4 System and Communications Protection	SC

ПУНКТ ИЗ ДОКУМЕНТА	NERC-CIP (REV5 - DRAFT) (NOVEMBER 7, 2011)	IEC-62443-2-1 (ISA99.02.01) (NOVEMBER 28, 2012)	NIST – SP800-82 (JUNE 2011)	NIST – SP800-53 (SUPPLEMENT SP800-82 STANDART*)
сетевым именам или определения сетевых имен по сетевым адресам			In accordance with SP800-53	
ЗИС.11 Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов	NONE	10.6 Network security management	6.3.4 System and Communications Protection In accordance with SP800-53	SC
ЗИС.12 Исключение возможности отрицания пользователем факта отправки информации другому пользователю	NONE	partially applicable 12.2.3 Message integrity	partially applicable 6.3.4 System and Communications Protection In accordance with SP800-53	SC
ЗИС.13 Исключение возможности отрицания пользователем факта получения информации от другого пользователя	NONE	NONE	partially applicable 6.3.4 System and Communications Protection In accordance with SP800-53	SC
ЗИС.14 Использование устройств терминального доступа для обработки информации	NONE	NONE	NONE	NONE
ЗИС.15 Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации	NONE	11.7.10 Software and Information Integrity	6.2.6 System and Information Integrity In accordance with SP800-53	SI
ЗИС.16 Выявление, анализ и блокирование скрытых каналов передачи информации в обход реализованных мер защиты информации или внутри разрешенных сетевых протоколов	NONE	12.5.4 Information leakage	6.2.6 System and Information Integrity In accordance with SP800-53	SI
ЗИС.17 Разбиение автоматизированной системы управления на сегменты (сегментирование) и обеспечение защиты периметров сегментов	partially applicable CIP-005-5 R1 Security Perimeter	11.4.5 Segregation in networks	5.2 Logically Separated Control Network 5.3 Network Segregation	NONE
ЗИС.18 Обеспечение загрузки и исполнения программного обеспечения с машинных носителей информации, доступных только для чтения, и контроль целостности данного программного обеспечения	NONE	Partially applicable 11.7.10 Software and Information Integrity	6.2.6 System and Information Integrity In accordance with SP800-53	SI

ПУНКТ ИЗ ДОКУМЕНТА	NERC-CIP (REV5 - DRAFT) (NOVEMBER 7, 2011)	IEC-62443-2-1 (ISA99.02.01) (NOVEMBER 28, 2012)	NIST – SP800-82 (JUNE 2011)	NIST – SP800-53 (SUPPLEMENT SP800-82 STANDART*)
ЗИС.19 Изоляция процессов (выполнение программ) в выделенной области памяти	NONE	12.2.2 Control of internal processing	6.2.6 System and Information Integrity In accordance with SP800-53	SI
ЗИС.20 Защита беспроводных соединений, применяемых в автоматизированной системы управления	Policies CIP-003-5 2.2 Partially applicable CIP-005-5 Security Perimeter	10.6 Network security management Partially applicable 11.7 Mobile computing and teleworking	6.3.2.5 Wireless NIST SP 800-48 provides guidance on wireless network security with particular emphasis on the IEEE 802.11b and Bluetooth standards NIST SP 800-97 provides guidance on IEEE 802.11i wireless network security	NONE
ЗИС.21 Исключение доступа пользователя к информации, возникшей в результате действий предыдущего пользователя через реестры, оперативную память, внешние запоминающие устройства и иные общие для пользователей ресурсы	NONE	NONE	NONE	NONE
ЗИС.22 Защита автоматизированной системы управления от угроз безопасности информации, направленных на отказ в обслуживании	NONE	NONE	6.3.4 System and Communications Protection In accordance with SP800-53	SC
ЗИС.23 Защита периметра (физических и (или) логических границ) автоматизированной системы управления при ее взаимодействии с иными автоматизированными (информационными) системами и информационно-телекоммуникационными сетями	CIP-005-5 R1 – Electronic Security Perimeter	9.1 Secure areas 10.8 Exchange of information 11.4.6 Network connection control	5.4 Recommended Defense-in-Depth Architecture 6.2.2 Physical and Environmental Protection In accordance with SP800-53 6.3.4 System and Communications Protection In accordance with SP800-53	PE SC
ЗИС.24 Прекращение сетевых соединений по их завершении или по истечении заданного владельцем временного интервала неактивности сетевого соединения	NONE	11.5.5 Session time-out	6.3.2 Access Control In accordance with SP800-53	AC

ПУНКТ ИЗ ДОКУМЕНТА	NERC-CIP (REV5 - DRAFT) (NOVEMBER 7, 2011)	IEC-62443-2-1 (ISA99.02.01) (NOVEMBER 28, 2012)	NIST – SP800-82 (JUNE 2011)	NIST – SP800-53 (SUPPLEMENT SP800-82 STANDART*)
ЗИС.25 Использование в автоматизированной системе управления различных типов общесистемного, прикладного и специального программного обеспечения (создание гетерогенной среды)	NONE	NONE	NONE	NONE
ЗИС.26 Использование прикладного и специального программного обеспечения, имеющих возможность функционирования в средах различных операционных систем	NONE	NONE	NONE	NONE
ЗИС.27 Создание (эмуляция) ложных компонентов автоматизированной системы управления, предназначенных для обнаружения, регистрации и анализа действий нарушителей в процессе реализации угроз безопасности информации	NONE	NONE	6.3.4 System and Communications Protection In accordance with SP800-53	SC
ЗИС.28 Воспроизведение ложных и (или) скрытие истинных отдельных информационных технологий и (или) структурно-функциональных характеристик автоматизированной системы управления или ее сегментов, обеспечивающее навязывание нарушителю ложного представления об истинных информационных технологиях и (или) структурно-функциональных характеристиках	NONE	NONE	6.3.4 System and Communications Protection In accordance with SP800-53	SC
ЗИС.29 Перевод автоматизированной системы или ее устройств (компонентов) в заранее определенную конфигурацию, обеспечивающую защиту информации, в случае возникновении отказов (сбоев)	CIP-009-5 R1 Recovery Plan Specifications	14.1.14 IACS Recovery and Reconstruction	6.2.3 Contingency Planning In accordance with SP800-53	CP
ЗИС.30 Защита мобильных технических средств, применяемых в автоматизированной системе управления	NONE	11.7.1 Mobile computing and communications	NONE	NONE
ОБР.0 Разработка правил и процедур (политик) обеспечения безопасной разработки программного обеспечения	NONE	Partially applicable 12.5 Security in development and support process	NONE	NONE
ОБР.1 Анализ уязвимостей и угроз безопасности информации в ходе разработки программного обеспечения	NONE	Partially applicable 12.5.1 Change control 12.2.1 Input data validation 12.2.2 Control of internal process	NONE	NONE

ПУНКТ ИЗ ДОКУМЕНТА	NERC-CIP (REV5 - DRAFT) (NOVEMBER 7, 2011)	IEC-62443-2-1 (ISA99.02.01) (NOVEMBER 28, 2012)	NIST – SP800-82 (JUNE 2011)	NIST – SP800-53 (SUPPLEMENT SP800-82 STANDART*)
		12.2.3 Output data validation		
ОБР.2 Статистический анализ кода программного обеспечения в ходе разработки программного обеспечения	NONE	NONE	NONE	NONE
ОБР.3 Ручной анализ кода программного обеспечения в ходе разработки программного обеспечения	NONE	NONE	NONE	NONE
ОБР.4 Тестирование на проникновение в ходе разработки программного обеспечения	NONE	NONE	NONE	NONE
ОБР.5 Динамический анализ кода программного обеспечения в ходе разработки программного обеспечения	NONE	NONE	NONE	NONE
ОБР.6 Документирование процедур обеспечение безопасной разработки программного обеспечения разработчиком и представление их заказчику (оператору)	NONE	NONE	NONE	NONE
ОПО.0 Разработка правил и процедур (политик) управления обновлениями программного обеспечения (включая получения, проверку и установку обновлений)	CIP-007-5 R2 Security Patch Management	12.6 Technical Vulnerability Management	6.2.6.3 Patch Management NIST SP 800-40 Version 2	NONE
ОПО.1 Получение обновлений программного обеспечения от разработчика или уполномоченного им лица	CIP-007-5 R2 Security Patch Management	12.6.2 Control of Technical Vulnerabilities	6.2.6.3 Patch Management NIST SP 800-40 Version 2	NONE
ОПО.2 Тестирование обновлений программного обеспечения до его установки на макете или в тестовой зоне	NONE	12.6.4 Configuration Change Control	6.2.6.3 Patch Management NIST SP 800-40 Version 2	NONE
ОПО.3 Централизованная установка обновлений программного обеспечения	NONE	NONE	6.2.6.3 Patch Management NIST SP 800-40 Version 2	NONE
ПЛН.0 Разработка правил и процедур (политик) планирования мероприятий по обеспечению защиты информации	NONE	4.4 IACS security management system (IACS-SMS)	6.1.2 Planning In accordance with SP800-53	PL
ПЛН.1 Определение лиц, ответственных за планирование и контроль мероприятий по обеспечению защиты информации в автоматизированной системе управления	NONE	4.5 Management responsibility	6.1.2 Planning In accordance with SP800-53	PL
ПЛН.2	NONE	4.4.2 Establishing and managing the	6.1.2 Planning	PL

ПУНКТ ИЗ ДОКУМЕНТА	NERC-CIP (REV5 - DRAFT) (NOVEMBER 7, 2011)	IEC-62443-2-1 (ISA99.02.01) (NOVEMBER 28, 2012)	NIST – SP800-82 (JUNE 2011)	NIST – SP800-53 (SUPPLEMENT SP800-82 STANDART*)
Разработка, утверждение и актуализация (обновление) плана мероприятий по обеспечению защиты информации в автоматизированных системах управления		IACS-SMS	In accordance with SP800-53	
ПЛН.3 Контроль выполнения мероприятий по обеспечению защиты информации в автоматизированных системах управления, предусмотренных утвержденным планом	NONE	4.4.2.3 Monitor and review IACS-SMS	6.1.2 Planning In accordance with SP800-53	PL
ДНС.0 Разработка правил и процедур (политик) обеспечения действий в нештатных (непредвиденных) ситуациях	CIP-009-5 R1	14 Business continuity management	6.2.3 Contingency Planning In accordance with SP800-53	CP
ДНС.1 Разработка плана действий в случае возникновения нештатных (непредвиденных) ситуаций	CIP-009-5 R1	14.1.3 Developing and implementing continuity plans including information security 14.1.7 Contingency Plan	6.2.3 Contingency Planning In accordance with SP800-53	CP
ДНС.2 Обучение и отработка действий пользователей в случае возникновения нештатных (непредвиденных) ситуаций	CIP-004-5 2.8	8.2.2 Security awareness, education, and training 14.1.9 Contingency Training	6.2.3 Contingency Planning In accordance with SP800-53	CP
ДНС.3 Создание альтернативных мест хранения и обработки информации в случае возникновения нештатных (непредвиденных) ситуаций	Partially applicable CIP-009-5 R1, R2	14.1.12 Alternate Control Site 14.2 Telecommunications Service	5.10 Redundancy and Fault Tolerance	NONE
ДНС.4 Резервирование программного обеспечения, технических средств, каналов передачи данных автоматизированных систем управления в случае возникновения нештатных (непредвиденных) ситуаций	Partially applicable CIP-009-5 R1	14.1.12 Alternate Control Site 14.2 Telecommunications Service 14.1.13 IACS Backup	5.10 Redundancy and Fault Tolerance 6.2.3 Contingency Planning In accordance with SP800-53	CP
ДНС.5 Обеспечение возможности восстановления автоматизированных систем управления и (или) ее компонент в случае возникновения нештатных (непредвиденных) ситуаций	CIP-009-5 R2	14.1.13 IACS Backup 14.1.14 IACS recovery and Reconstruction	6.2.3 Contingency Planning In accordance with SP800-53	CP
ИПО.0 Разработка правил и процедур (политик) информирования и обучения пользователей	CIP-004-5 R1 – Security Awareness Program CIP-004-5 R3–Cyber	5.1.1 Cyber security policy document 4.5.2.2 Training, awareness and competence	6.2.9 Awareness and Training In accordance with SP800-	AT

ПУНКТ ИЗ ДОКУМЕНТА	NERC-CIP (REV5 - DRAFT) (NOVEMBER 7, 2011)	IEC-62443-2-1 (ISA99.02.01) (NOVEMBER 28, 2012)	NIST – SP800-82 (JUNE 2011)	NIST – SP800-53 (SUPPLEMENT SP800-82 STANDART*)
	Security Training	8.2.2 Security awareness, education, and training	53 4.2.8 Provide Training and Raise Security Awareness	
ИПО.1 Информирование пользователей об угрозах безопасности информации, о правилах эксплуатации системы защиты автоматизированной системы управления и отдельных средств защиты информации	CIP-004-5 R1 – Security Awareness Program	4.5.2.2 Training, awareness and competence 8.2.2 Security awareness, education, and training	6.2.9 Awareness and Training In accordance with SP800-53 4.2.8 Provide Training and Raise Security Awareness	AT
ИПО.2 Обучение пользователей правилам эксплуатации системы защиты автоматизированной системы управления и отдельных средств защиты информации	CIP-004-5 R2 – Cyber Security Training Program	4.5.2.2 Training, awareness and competence 8.2.2 Security awareness, education, and training	6.2.9 Awareness and Training In accordance with SP800-53 4.2.8 Provide Training and Raise Security Awareness	AT
ИПО.3 Проведение практических занятий с пользователями по эксплуатации системы защиты автоматизированной системы управления и отдельных средств защиты информации	CIP-004-5 Table R2 – Cyber Security Training Program	8.2.2 Security awareness, education, and training	6.2.9 Awareness and Training In accordance with SP800-53 4.2.8 Provide Training and Raise Security Awareness	AT
УБИ.0 Разработка правил и процедур (политик) анализа угроз безопасности информации и рисков от их реализации	NONE	5.1.1 Cyber security policy document 4.4 IACS security management system (IACS-SMS)	6.1.3 Risk Assessment In accordance with SP800-53	RA
УБИ.1 Периодический анализ изменения угроз безопасности информации, возникающих в ходе ее эксплуатации автоматизированной системы управления	NONE	4.4.2.3 Monitor and review IACS-SMS 4.7 Management review of the IACS-SMS	6.1.3 Risk Assessment In accordance with SP800-53	RA
УБИ.2 Периодическая переоценка последствий от реализации угроз безопасности информации (оценка риска)	NONE	4.4.2.3 Monitor and review IACS-SMS 4.7 Management review of the IACS-SMS	6.1.3 Risk Assessment In accordance with SP800-53	RA
ИНЦ.0 Разработка правил и процедур (политик) выявления инцидентов и реагирования на них	CIP-003-5 R2 1.6 CIP-008-5 R1	5.1.1 Cyber security policy document 13 Cyber security incident management	4.2.4 Define ICS Specific Security Policies and Procedures	NONE
ИНЦ.1	CIP-008-5 1.3	13.2.4 Incident Response Policy and	6.2.8 Incident Response	IR

ПУНКТ ИЗ ДОКУМЕНТА	NERC-CIP (REV5 - DRAFT) (NOVEMBER 7, 2011)	IEC-62443-2-1 (ISA99.02.01) (NOVEMBER 28, 2012)	NIST – SP800-82 (JUNE 2011)	NIST – SP800-53 (SUPPLEMENT SP800-82 STANDART*)
Определение лиц, ответственных за выявление инцидентов и реагирование на них		Procedures	In accordance with SP800-53	
ИНЦ.2 Обнаружение, идентификация и регистрация инцидентов	CIP-007-5 4.1 CIP-008-5 R2	13.2 Management of cyber security incidents and improvements	6.2.8 Incident Response In accordance with SP800-53 NIST SP 800-61 provides guidance on incident handling and reporting	IR
ИНЦ.3 Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов	NONE	13.1.1 Reporting cyber security events 13.2.9 Incident Reporting	6.2.8 Incident Response In accordance with SP800-53 NIST SP 800-61 provides guidance on incident handling and reporting	IR
ИНЦ.4 Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий	CIP-008-5 R3	13.2.1 Responsibilities and procedures 13.2.7 Incident Handling	6.2.8 Incident Response In accordance with SP800-53 NIST SP 800-61 provides guidance on incident handling and reporting	IR
ИНЦ.5 Принятие мер по устранению последствий инцидентов	CIP-008-5 R2	13.2.7 Incident Handling	6.2.8 Incident Response In accordance with SP800-53 NIST SP 800-61 provides guidance on incident handling and reporting	IR
ИНЦ.6 Планирование и принятие мер по предотвращению повторного возникновения инцидентов	CIP-008-5 R3	13.2.4 Incident Response Policy and Procedures	6.2.8 Incident Response In accordance with SP800-53 NIST SP 800-61 provides guidance on incident handling and reporting	IR
УКФ.0 Разработка правил и процедур (политик) управления конфигурацией автоматизированной системой управления и ее системы защиты	CIP-010-1 R1	12.6.2 Configuration Management Policy and Procedures		NONE
УКФ.1 Определение лиц, которым разрешены действия по внесению изменений в конфигурацию автоматизированной системы управления и ее системы	CIP-010-1 R1 1.2	12.6.6 Access Restriction for Change	6.2.4 Configuration Management In accordance with SP800-53	CM

ПУНКТ ИЗ ДОКУМЕНТА	NERC-CIP (REV5 - DRAFT) (NOVEMBER 7, 2011)	IEC-62443-2-1 (ISA99.02.01) (NOVEMBER 28, 2012)	NIST – SP800-82 (JUNE 2011)	NIST – SP800-53 (SUPPLEMENT SP800-82 STANDART*)
защиты				
УКФ.2 Управление изменениями конфигурации автоматизированной системы управления и ее системы защиты	CIP-010-1 1.4	12.6.4 Configuration Change Control	6.2.4 Configuration Management In accordance with SP800-53	CM
УКФ.3 Анализ потенциального воздействия планируемых изменений в конфигурации автоматизированной системы управления и системы защиты на обеспечение защиты персональных данных и согласование изменений в конфигурации автоматизированной системы управления с должностным лицом (работником), ответственным за обеспечение безопасности автоматизированной системы управления	CIP-010-1 1.5	12.6.5 Monitoring Configuration Changes	6.2.4 Configuration Management In accordance with SP800-53	CM
УКФ.4 Документирование информации (данных) об изменениях в конфигурации автоматизированной системы управления и ее системы защиты	CIP-010-1 1.4	12.6.3 Baseline Configuration 12.6.4 Configuration Change Control	6.2.4 Configuration Management In accordance with SP800-53	CM
УКФ.5 Регламентация и контроль технического обслуживания, в том числе дистанционного (удаленного), технических средств и программного обеспечения автоматизированной системы управления	NONE	9.2.4 Equipment maintenance 12.6.9 System Maintenance Policy and Procedures 12.6.10 Controlled Maintenance 12.6.12 Remote Maintenance 12.6.13 Maintenance Personnel	6.2.4 Configuration Management 6.2.5 Maintenance In accordance with SP800-53	CM MA