ЦЕНТР КОРПОРАТИВНОГО ОБУЧЕНИЯ
ЭНЕРГИЯ ЗНАНИЙ

Частное образовательное учреждение дополнительного профессионального образования
«Центр корпоративного обучения»

ПРИКАЗ

03.09.2020 220

г. Добрянка

О введении в действие Политики ПТ-060-1 «Политика информационной безопасности» в ЧОУ ДПО «Центр корпоративного обеспечения»

В целях организации и стандартизации деятельности в области информационных технологий в Группе «Интер РАО», в связи с утверждением Советом директоров АО «Интер РАО – Электрогенерация» (протокол от 27.07.2020 № 341) Политики ПТ-060-1 «Политика информационной безопасности АО «Интер РАО – Электрогенерация» и Решением единственного участника ООО «Интер РАО – Управление Электрогенерацией» (от 27.07.2020 № 299) Политики ПТ-060-1 «Политика информационной безопасности» ООО «Интер РАО – Управление электрогенерацией», на основании приказа от 11.08.2020 № УЭГ/321/ЭГ/315 «О введении в действие Политики ПТ-060-1 «Политика информационной безопасности» в АО «Интер РАО – Электрогенерация» и ООО «Интер РАО – Управление Электрогенерацией»,

ПРИКАЗЫВАЮ:

1. Ввести в действие Политику ПТ-060-1 «Политика информационной безопасности в ЧОУ ДПО «ЦКО» в соответствии с приложением №1 к настоящему приказу.
2. Руководителям подразделений ознакомить сотрудников с настоящим приказом.
3. Контроль за исполнением настоящего приказа оставляю за собой.

Приложение: Политика ПТ-060-1 информационной безопасности в ЧОУ ДПО «ЦКО».

Директор И.А. Анисимов

Гагарин Олег Станиславович, 221

Рассылается: руководители структурных подразделений

Приложение 1 к приказу
№ 120
от «03» 09 2020г.

УТВЕРЖДЕНА
Директор ЧОУ ДПО «ЦКО»
_____И.А. Анисимов
«03» 09 2020г.

ПОЛИТИКА

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЧОУ ДПО «ЦЕНТР КОРПОРАТИВНОГО ОБУЧЕНИЯ»

ПТ-060-1

СОДЕРЖАНИЕ

1. ИНФОРМАЦИЯ О ДОКУМЕНТЕ

Краткое описание документа	Политика информационной безопасности определяет общие намерения, принципы и ответственность ЧОУ ДПО «Центр корпоративного обучения» в области информационной безопасности. Политика информационной безопасности выступает в качестве документа верхнего уровня для Регламентов процессов, Методик, Инструкций и Положений по направлению информационной безопасности
Корпоративный стандарт	Да
Ограничение доступа	Нет
Ответственный за применение ВНД	Отдел программного и технического обеспечения/начальник отдела
Владелец документа	ЧОУ ДПО «Центр корпоративного обучения»/Директор

2. ОТВЕТСТВЕННОСТЬ И ОБЛАСТЬ ПРИМЕНЕНИЯ

2.1. Настоящая Политика информационной безопасности (далее - Политика) разработана в соответствии с законодательством Российской Федерации, ЧОУ ДПО «Центр корпоративного обучения» (далее - Учреждение), рекомендациями международных стандартов управления информационной безопасностью[1], с учетом лучших российских и международных практик в части обеспечения информационной безопасности (далее - ИБ), требованиями нормативных актов Российской Федерации, федерального органа исполнительной власти, уполномоченного в области безопасности, федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации.

2.2. Политика является верхнеуровневым документом, определяющим общие цели и задачи ИБ в Учреждении, способы контроля реализации требований Политики. Набор внутренних нормативных документов по ИБ (методики, положения, регламенты, инструкции), который детализирует положения настоящей Политики (не включая вопросы, связанные с защитой государственной тайны), должен соответствовать настоящей Политике.

2.3. Политика является документом, доступным для работников Учреждения, и представляет собой официально принятую руководством Учреждения позицию по отношению к проблемам информационной безопасности Учреждения и принимаемым в рамках обеспечения информационной безопасности мерам.

2.4. Политика обязательна для исполнения всеми работниками и структурными подразделениями Учреждения, а также рекомендована к соблюдению Подконтрольными

[1] ISO/IEC 27001:2013 «Information technology – Security techniques – Information security management systems – Requirements»

юридическими лицами Учреждения, и должна учитываться в отношениях с внешними организациями (подрядчики, аудиторы и т.д.).

2.5. Любые решения Работников Учреждения и внутренние нормативные документы не должны противоречить настоящей Политике в части учета требований информационной безопасности.

2.6. Политика утверждается решением Директора. Изменения и дополнения в настоящую Политику вносятся решением Директора. Основанием для внесения изменений могут служить изменения регуляторных требований, изменения характера угроз, возникновение новых рисков информационной безопасности, изменение принципов построения ИТ-инфраструктуры, информационных и автоматизированных систем. Необходимость актуализации Политики рассматривается не реже 1 раза в 3 года.

2.7. Руководство Учреждения осознает значимость вопросов информационной безопасности, всецело поддерживает необходимость обеспечения информационной безопасности Учреждения и Подконтрольных лиц с целью обеспечения непрерывности, конкурентоспособности, рентабельности бизнеса, соответствия требованиям законодательства, выполнения контрактных и иных обязательств, формирования положительной репутации и имиджа Учреждения и Подконтрольных лиц.

2.8. Стратегическим решением обеспечения информационной безопасности Учреждения является создание, внедрение, поддержка и постоянное совершенствование систем информационной безопасности (СУИБ и СОИБ), основанных на приоритетах безопасности ИТ-инфраструктуры, информационных и автоматизированных систем на основе методологии управления рисками, учитывающих законодательные, контрактные и иные бизнес требования к информационной безопасности.

2.9. Направления ИБ автоматизированных систем управления технологическим процессом и ИБ критической информационной инфраструктуры Руководители Учреждения и Подконтрольных лиц считают одними из приоритетных направлений ИБ.

2.10. Каждый работник должен стремиться к повышению своей осведомленности в области ИБ, соблюдению требований данной Политики, законодательства РФ и внутренних нормативных документов в функциональном направлении информационной безопасности.

2.11. Если отдельные пункты настоящей Политики вступают в противоречие с законодательством Российской Федерации эти пункты утрачивают силу. Недействительность этих пунктов настоящей политики не влечет признание недействительности других пунктов Политики или Политики в целом.

Настоящий документ регламентирует деятельность следующих подразделений и должностных лиц, включая исполняющих роли:

Наименование подразделения/должности/роли
Все Работники Учреждения
Подконтрольные лица

3. ОПРЕДЕЛЕНИЯ РОЛЕЙ И ТЕРМИНОВ

Наименование роли	Определение роли
Директор	• Утверждение политики ИБ. • Обеспечение достаточного финансирования мероприятий в рамках реализации политики. • Инициирование внесения изменений в Политику. • Обеспечение выявления, оценки, осуществления мер воздействия на риски информационной безопасности и отчетности по рискам информационной безопасности; • Определение перечней значимой информации, обрабатываемой в рамках реализации процессов (бизнес-процессов) в зоне функциональной ответственности; • Учет мер и механизмов обеспечения информационной безопасности в бизнес-процессах и средствах автоматизации Учреждения; • Выполнение мероприятий программы развития информационной безопасности; • Поддержание уровня информационной безопасности, установленного внутренними нормативными документами, документацией на информационные системы или иными документами Учреждения в рамках должностных обязанностей; • Выполнение мероприятий по повышению уровня осведомленности работников Учреждения в области информационной безопасности; • Формирование и обеспечение деятельности подразделений информационной безопасности и подразделений информационной безопасности объектов критической информационной инфраструктуры; • Формирование и обеспечение непрерывного функционирования средств и систем информационной безопасности

Начальник отдела программного и технического обеспечения ЧОУ ДПО «ЦКО»	• Организация достижения целей и исполнения задач Политики информационной безопасности ЧОУ ДПО «ЦКО»; • Разработка программ развития информационной безопасности группы и контроль её выполнения, в том числе контроль включения мероприятий по ИБ в бизнес-планы Подконтрольных лиц; • Координация процессов управления рисками ИБ в компаниях Группы, в том числе координация деятельности и методологическая поддержка компаний Группы в области информационной безопасности; • Формирование предложений по мерам, механизмам и средствам автоматизации ЧОУ ДПО «ЦКО», организация исполнения согласованных предложений с включением затрат в бизнес-планы ЧОУ ДПО «ЦКО» и контроль их реализации; • Формирование предложений по мерам, механизмам и средствам обеспечения информационной безопасности в бизнес-процессах и средствах автоматизации Учреждения; • Обеспечение контроля формирования и исполнения мероприятий функционального направления «Информационная безопасность» в рамках бизнес-планов ЧОУ ДПО «ЦКО»; • Разработка внутренних нормативных документов по информационной безопасности; • Организация процессов обнаружения, локализации и реагирования на инциденты информационной безопасности; • Обеспечение выполнения требований нормативно-правовых актов органов власти по направлению информационной безопасности, Политики и внутренних нормативных документов, детализирующих положения Политики; • Планирование мероприятий по повышению уровня осведомленности работников ЧОУ ДПО «ЦКО» в области информационной безопасности
Руководители прямого подчинения ЧОУ ДПО «ЦКО»	• Содействие отделу программного и технического обеспечения в координации процессов управления рисками информационной безопасности в Учреждении; Определение перечней значимой информации, обрабатываемой в рамках реализации процессов (бизнес-процессов) в зоне функциональной ответственности;

	• Учет мер и механизмов обеспечения информационной безопасности в бизнес-процессах и средствах автоматизации ЧОУ ДПО «ЦКО» в зоне функциональной ответственности; • Поддержание уровня информационной безопасности, установленного внутренними нормативными документами, документацией на информационные системы или иными документами ЧОУ ДПО «ЦКО» в рамках должностных обязанностей; • Подготовка инициатив по внесению изменений в Политику информационной безопасности
Все работники Учреждения	• Соблюдение требований нормативно-правовых актов органов власти по направлению ИБ и внутренних нормативных документов по ИБ. • Поддержание установленного внутренними нормативными документами, документацией на информационные системы или оборудование, или иными документами Учреждения уровня информационной безопасности в рамках должностных обязанностей

Остальные определения терминов, сокращений приведены в «Глоссарии» Корпоративного портала.

Наименование термина	**Сокращение**	**Определение термина (расшифровка сокращения)**
Вводимые определения:		
ГосСОПКА	ГосСОПКА	Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации
Доступность		Свойство возможности доступа и использования по требованию санкционированной Сущности[2] (физическое лицо, организация, компьютерный процесс и т.д.)
Информационная безопасность	ИБ	Сохранение конфиденциальности, целостности и доступности информации[2] . В контексте данного документа рассматривается информация только в цифровом виде
Инцидент информационной безопасности	ИИБ, инцидент	Одиночное или серия событий информационной безопасности, которые имеют значительную вероятность нарушения бизнес-деятельности и угрожающие информационной безопасности[2]
Конфиденциальность		Свойство подтверждающее, что информация не была несанкционированно доступна или раскрыта физическим лицам, сущностям (в том числе организациям) или процессам[2]
Подразделение информационной безопасности	подразделение ИБ	Подразделение (или работник) Учреждения,уполномоченное установленным порядком и ответственное за обеспечение и управление ИБ Учреждения. Для ЧОУ ДПО «ЦКО» таким подразделением является Отдел программного и технического обеспечения. [3]

[2] Международный стандарт ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary.

[3] Отдел программного и технического обеспечения выполняет функции подразделения по информационной безопасности до создания выделенного подразделения по информационной безопасности (за исключением случаев создания выделенного подразделения ИБ ОКИИ).

Подразделение информационной безопасности объектов критической информационной инфраструктуры	подразделение ИБ ОКИИ	Подразделение (или работник) Учреждения, уполномоченное установленным порядком и ответственное за обеспечение и управление ИБ в части защиты объектов критической инфраструктуры (далее – ОКИИ). Для ЧОУ ДПО «ЦКО» ответственность за защиту ОКИИ возлагается на отдельного работника назначаемого директором Учреждения.
Риск ИБ		Нарушение в работе автоматизированных бизнес-процессов, ИТ-систем, вызванное инцидентами информационной безопасности. Несоблюдение требований регулятора в области информационной безопасности
Событие информационной безопасности	СИБ	Определенное состояние системы, сервиса или сети свидетельствующее о возможном нарушении информационной безопасности, политики или неэффективности мер защиты, или ранее не известная ситуация, которая имеет значение для информационной безопасности[2]
Система обеспечения информационной безопасности	СОИБ	Формализованная совокупность технических мер, реализованная структурированным набором средств информационной безопасности, включающих специализированные средства защиты и встроенные средства и механизмы защиты программно-аппаратных средств, составляющих информационные и/или автоматизированные системы и ИТ-инфраструктуру, а также организационных мер, связанных с

[3] Назначение ответственного лица определяется согласно приказу ФСТЭК РФ от 21 декабря 2017 года № 235

		обеспечением непрерывности функционирования таких средств информационной безопасности
Система управления информационной безопасностью	СУИБ	Формализованная совокупность взглядов и подходов в области управления организационными процессами, направленными на достижение установленного уровня защищенности, включая: мероприятия, направленные на организацию и контроль исполнения мер ИБ, разработанные и внедрённые внутренние нормативные документы, формализованные процессы ИБ, регламенты, инструкции и т.д.
Специализированная ИБ-организация		Организация из числа Подконтрольных лиц ЧОУ ДПО «ЦКО», выполняющая функции обеспечения и\или управления ИБ на основании соответствующего договора, удовлетворяющая требованиям законодательства в области регулирования соответствующих видов деятельности
Угроза		Потенциальная причина нежелательного события, которое может привести к ущербу для информационной (или автоматизированной) системы или для организации[4]
ФСБ России	ФСБ России	Федеральная служба безопасности Российской Федерации (ФСБ России) является федеральным органом исполнительной власти, в пределах своих полномочий осуществляющим государственное управление в области обеспечения безопасности Российской Федерации, борьбы с терроризмом, защиты и охраны государственной границы Российской Федерации (далее именуется - государственная граница), охраны внутренних морских вод, территориального моря, исключительной экономической зоны, континентального шельфа Российской Федерации и их природных ресурсов, обеспечивающим информационную

[4] Международный стандарт ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary.

		безопасность Российской Федерации и непосредственно реализующим основные направления деятельности органов федеральной службы безопасности, определенные законодательством Российской Федерации, а также координирующим контрразведывательную деятельность федеральных органов исполнительной власти, имеющих право на ее осуществление
ФСТЭК России	ФСТЭК России	Федеральная служба по техническому и экспортному контролю Российской Федерации (ФСТЭК России) является федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации, а также специально уполномоченным органом в области экспортного контроля
Целостность		Свойство точности, корректности и полноты информации[5]
Действующие определения:		
Группа «Интер РАО»	Группа	ПАО «Интер РАО» и его дочерние Учреждения
Департамент информационной безопасности	ДИБ	Департамент информационной безопасности ПАО «Интер РАО»
ИТ-инфраструктура		Совокупность средств вычислительной техники, коммуникационного оборудования и линий связи, автоматизированных систем управления, обеспечивающих функционирование производственных процессов, процедур и нормативных документов, являющихся основой для функционирования информационных сервисов и производства электроэнергии с целью обеспечения функционирования бизнес-процессов Учреждения.
Учреждение	Учреждение	ЧОУ ДПО «Центр корпоративного обучения»

[5] Международный стандарт ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary.

Учредитель	Учредитель	АО «Интер РАО – Электрогенерация»
Подконтрольное лицо (подконтрольная организация)	Подконтрольное лицо, Подконтрольное лицо Учреждения, ДО	Юридическое лицо, находящееся под прямым или косвенным контролем контролирующего лица. Подконтрольным лицом, имеющим существенное значение для деятельности Учреждения, является подконтрольное лицо, на долю которого приходится не менее 5 процентов консолидированной стоимости активов или не менее 5 процентов консолидированного дохода Учреждения
Работник		Физическое лицо, работающее по трудовому договору в должности согласно штатному расписанию и подчиняющееся внутреннему трудовому распорядку организации. В РФ общие права и обязанности работников установлены трудовым законодательством

4. ЦЕЛИ В ФУНКЦИОНАЛЬНОМ НАПРАВЛЕНИИ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ДЕЯТЕЛЬНОСТИ ЧОУ ДПО «ЦЕНТР КОРПОРАТИВНОГО ОБУЧЕНИЯ»

4.1. Выявление и минимизация Рисков информационной безопасности:

- Организация обеспечения соответствия системы информационной безопасности нормативным требованиям по ИБ, при достижении максимальной адекватности мер по защите от выявленных угроз информационной безопасности;
- Организация приоритетной реализации мер, направленных на предотвращение возникновения инцидентов ИБ;
- Организация соблюдения мер, направленных на обнаружение инцидентов ИБ и мер сокращающих время начала ликвидации последствий, вызванных инцидентами ИБ.

4.2. Поддержание оптимального уровня защищенности и устойчивости к компьютерным атакам информационных ресурсов и активов Группы:

- Организация мероприятий, направленных на обеспечение устойчивого бесперебойного функционирования информационных систем и информационной инфраструктуры Учреждения, бесперебойность и защищенность технологических процессов, нарушение которых может быть вызвано инцидентами ИБ;
- Организация мероприятий, направленных на обеспечение защиты информации, обрабатываемой с использованием средств автоматизации от нарушения установленных свойств конфиденциальности, целостности и доступности, вызванного инцидентом ИБ.

4.3. Вышеуказанные цели достигаются путем решения задач по организации:

- Выявления и регулярной актуализации угроз информационной безопасности и рисков

информационной безопасности Учреждения, оценка последствий от их реализации;

- Определения актуальных типов нарушителей, способных реализовывать угрозы информационной безопасности;
- Прогнозирования и описания потенциально опасных сценариев реализации угроз информационной безопасности;
- Регулярной проверки реализуемости выявленных сценариев;
- Регистрации и своевременного реагирования на компьютерные атаки и Инциденты
- Обеспечения защищенности ИТ-инфраструктуры Учреждения;
- Обеспечения соответствия системы защиты требованиям законодательства в области
- Разработки и внедрения необходимой нормативной документации.

5. ПРИНЦИПЫ В ФУНКЦИОНАЛЬНОМ НАПРАВЛЕНИИ ИБ: СУИБ И СОИБ

5.1. Общие принципы организации ИБ:

- Риск-ориентированный подход к ИБ.
- Обеспечение ИБ ИТ-инфраструктуры.
- Определение и закрепление ролей и ответственности.
- Интеграция ИБ в важнейшие бизнес-операции.
- Кадровое обеспечение деятельности ИБ.
- Финансирование процессов обеспечения ИБ.
- Соблюдение требований внутренних нормативных документов и законодательства в области ИБ.
- Адекватность, измеримость и контролируемость защитных мер.
- Непрерывность ИБ.

5.2. **Риск-ориентированный подход** при организации защиты информационных и автоматизированных систем. Риск-ориентированный подход должен опираться на Политику управления рисками и внутреннего контроля и документы уполномоченных федеральных органов исполнительной власти.

5.3. **Обеспечение ИБ ИТ-инфраструктуры** Учреждения и Подконтрольных лиц производится путем разработки и внедрения организационно-технических мероприятий и контрольных процедур, направленных на снижение вероятности или воздействия для всех актуальных угроз безопасности, выявленных по итогам моделирования угроз в соответствии с требованиями ФСТЭК России и ФСБ России. При этом уровень защищенности (категория значимости) ИТ-инфраструктуры должен быть не ниже самого высокого уровня защищенности (категории значимости) информационной системы, размещаемой в этой ИТ-инфраструктуре или использующей эту ИТ-инфраструктуру.

5.4. **Определение и закрепление ролей и ответственности** подразумевает, что ответственность уполномоченных лиц Учреждения на реализацию мероприятий ИБ (определение и актуализация Рисков ИБ, формирование, финансирование и обеспечение непрерывности мер ИБ, исполнение требований внутренних нормативных документов и Политики), должна быть формализована и закреплена за конкретными работниками.

5.5. **Интеграция ИБ в бизнес-процессы** – Мероприятия по обеспечению ИБ должны быть учтены при формировании новых процессов (бизнес-процессов), а также при формировании средств их автоматизации владельцами бизнес-процессов. Существующие

процессы (бизнес-процессы), а также структура и архитектура средств их автоматизации должны пересматриваться их владельцами с учетом мероприятий ИБ.

В целях минимизации возможных последствий от реализации Рисков ИБ владельцами процессов (бизнес-процессов) должны быть разработаны и формализованы планы на случай прекращения/нарушения функционирования средств автоматизации таких процессов (бизнес-процессов).

Работники подразделения ИБ и подразделения ИБ ОКИИ Учреждения должны оказывать методологическую поддержку владельцам процессов (бизнес-процессов), средств их автоматизации, а также владельцам Рисков ИБ при определении мер ИБ.

Информационная безопасность должна стать неотъемлемым компонентом на всех стадиях жизненного цикла средств автоматизации процессов (бизнес-процессов). Общепринятые (лучшие) практики в области ИБ (например, тщательное тестирование/аудит для выявления слабых мест безопасности, независимая экспертиза и возможность обрабатывать ошибки, исключения и чрезвычайные ситуации) должны играть ключевую роль на всех этапах процесса разработки, создания, эксплуатации и вывода из эксплуатации информационных систем.

ИБ следует сделать важным компонентом повседневной деятельности, повышая осведомленность работников и обеспечивая наличие навыков, необходимых для поддержки установленного уровня защищенности. Каждый работник должен быть осведомлен, какой риск связан с вверенной ему информацией, реализуемым им процессом (бизнес-процессом), и иметь возможность принимать необходимые меры по ее защите, своевременно информировать лиц, ответственных за ИБ, при выявлении подозрений на Инцидент ИБ.

5.6. **Кадровое обеспечение деятельности ИБ** реализуется в рамках законодательства РФ в области информационной безопасности, в том числе с учетом соответствующих приказов ФСТЭК России и ФСБ России.

Для реализации настоящей Политики в Учреждении и Подконтрольных лицах, может быть определено или создано подразделение или может быть определен или назначен штатный специалист, ответственные за обеспечение и управление ИБ.

Если для реализации настоящей Политики, для нужд обеспечения и управления ИБ в Обществе и его Подконтрольных лицах, не определено или не создано подразделение, не определен или не назначен специалист, то вся ответственность за организацию исполнения данной Политики возлагается на единоличный исполнительный орган Учреждения и его Подконтрольных лиц.

Работники подразделений ИБ и подразделения ИБ ОКИИ обязаны постоянно совершенствоваться - повышать собственную квалификацию, обновлять теоретические знания и практические навыки для решения стоящих перед ними профессиональных задач, а Руководители Подконтрольных лиц обязаны обеспечивать возможность, поощрять и стимулировать такое совершенствование.

5.7. **Финансирование процессов обеспечения ИБ** подразумевает выделение достаточных ресурсов для реализации мероприятий (реализацию мер и внедрение средств ИБ) во исполнение данной политики, а также для оплаты труда работников подразделения ИБ и подразделения ИБ ОКИИ.

Расходы на мероприятия по ИБ в т.ч. должны быть включены в расходы (бюджет) мероприятий по созданию, модернизации, техническому перевооружению или поддержке каждой создаваемой (модернизируемой, поддерживаемой) информационной и/или автоматизированной системы. В случае выявления актуальных угроз или Рисков ИБ в существующих информационных и/или автоматизированных системах, финансирование мероприятий по ИБ может производится в рамках отдельных ИБ-проектов или ИБ- мероприятий[6].

Финансирование мероприятий ИБ, направленных на повышение безопасности ИТ-инфраструктуры, должно осуществляться в зависимости от Рисков ИБ и угроз ИБ, актуальных для информационных и/или автоматизированных систем.

5.8. **Соблюдение требований внутренних нормативных документов и законодательства в области ИБ** подразумевает обязательность исполнения действующего законодательства и нормативных -правовых актов государственных органов Российской Федерации и стран присутствия Подконтрольных лиц, внутренних нормативных документов, а также нормативных правовых актов по безопасности информации, принятыми органами государственной власти и управления в пределах их компетенции. Должна обеспечивается неотвратимость наказания за их нарушение с учетом внутренних нормативных документов функционального направления управления персоналом. Стратегические решения в области ИБ могут приниматься с учетом консультаций и позиции федеральных органов исполнительной власти, уполномоченных в области ИБ. Деятельность в области ИБ осуществляется с учётом требований нормативных документов и указаний соответствующих органов власти уполномоченных в области информационной безопасности, а также в соответствии с Комплаенс Политикой. Безопасность информации, обрабатываемой без использования средств автоматизации, обеспечивается всеми работниками, осуществляющими обработку такой информации путем соблюдения требований законодательства и внутренних нормативных документов, определяющих порядок такой обработки (в том числе, но не ограничиваясь порядком допуска к обработке, допустимыми методами и процедурами обработки). Потребность в обеспечении информационной безопасности, а также внутренние нормативные документы о порядке обработки той или иной информации формируют подразделения Учреждения, являющиеся ответственными за определение порядка обработки той или иной информации и/или являющиеся владельцами той или иной информации.

5.9. **Адекватность, измеримость и контролируемость защитных мер.** На этапе проектирования мер ИБ должно проводиться их соотнесение с актуальными угрозами ИБ и Рисками ИБ, определяться количественные и качественные характеристики, соответствующие проектируемым мерам. Для обеспечения высокого уровня защищённости Учреждения и Подконтрольных лиц следует проводить регулярный контроль эффективности реализованных мер.

5.10. **Непрерывность** подразумевает непрерывность реализации функционирования мер и средств, обеспечивающих информационную безопасность Учреждения.

---

[6] Для автоматизированных систем управления технологическими процессами (включая системы релейной защиты и противоаварийной автоматики) электростанций и тепловых сетей расходы на мероприятия по ИБ должны включаться в бюджет проектов вновь создаваемых систем. В случае выявления актуальных угроз или Рисков ИБ в существующих автоматизированных системах управления технологическими процессами (включая системы релейной защиты и противоаварийной автоматики) электростанций и тепловых сетей, в том числе при их модернизации (реконструкции), техническом перевооружении финансирование мероприятий по ИБ должно производится в рамках отдельных ИБ-проектов или ИБ-мероприятий

6. ОПИСАНИЕ СИСТЕМ В ФУНКЦИОНАЛЬНОМ НАПРАВЛЕНИИ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

6.1. В целях достижения максимального эффекта от создаваемой системы ИБ необходимо разделить процессы между двумя взаимно дополняющими друг друга системами:

- Система управления информационной безопасностью (СУИБ);
- Система обеспечения информационной безопасности (СОИБ).

6.2. **Система управления информационной безопасностью**

6.2.1. Адаптация, контроль адаптации и реализация в Учреждении и Подконтрольных лицах корпоративных стандартов и организационных мер в области информационной безопасности;

6.2.2. Контроль за соблюдением требований законодательства в области информационной безопасности в Учреждении и Подконтрольных лицах;

6.2.3. Экспертиза принимаемых в Учреждении и Подконтрольных лицах корпоративных стандартов, ВНД и организационно-распорядительных документов на предмет их соответствия Политике информационной безопасности и разработанным на её основе ВНД и корпоративным стандартам;

6.2.4. Обеспечение исполнения и адаптации ВНД в области информационной безопасности в Учреждении и Подконтрольных лицах, в том числе обеспечение соответствия Политике информационной безопасности;

6.2.5. Обеспечение исполнения организационно-распорядительных документов и решений в Учреждении и Подконтрольных лицах по результатам аудитов, расследований и проверок в области информационной безопасности;

6.2.6. Обеспечение процессов управления информационной безопасностью, выполнения требований и принятия мер по обеспечению информационной безопасности в Учреждении и Подконтрольных лицах;

6.2.7. Контроль бизнес-процессов в Учреждении и Подконтрольных лицах с целью выявления реальных и потенциальных угроз информационной безопасности;

6.2.8. Организация и контроль обеспечения информационной безопасности объектов критической информационной инфраструктуры в Учреждении;

6.2.9. Контроль обеспечения информационной безопасности объектов критической информационной инфраструктуры в Подконтрольных лицах;

6.2.10. Организация мероприятий по минимизации последствий угроз информационной безопасности, в том числе, инициирование и участие в служебных расследованиях, аудитах информационной безопасности по фактам нарушений в области информационной безопасности в Учреждении и Подконтрольных лицах;

6.2.11. Мониторинг требований нормативных правовых актов в области информационной безопасности, организация взаимодействия с ФСТЭК России, ФСБ России, Министерством энергетики по вопросам информационной безопасности;

6.2.12. Планирование мероприятий по повышению уровня осведомленности работников Учреждения и Подконтрольных лицах в области информационной безопасности.

6.3 Система обеспечения информационной безопасности

6.3.1. Определение функциональных требований к системам информационной безопасности, применяемым в Учреждении и Подконтрольных лицах (за исключением систем автоматизации экономической и собственной безопасности Учреждения);

6.3.2. Определение требований к функциям и механизмам безопасности, реализуемым в информационных технологиях, информационных и телекоммуникационных системах, автоматизированных системах управления, разрабатываемым и применяемым в Учреждении и Подконтрольных лицах;

6.3.3. Использование типовых решений и следование единой технической политике в области информационной безопасности и контроль их применения в Учреждении и Подконтрольных лицах;

6.3.4. Контроль внедрения процедур безопасной разработки и приемки результатов разработки программного обеспечения, контроль за применением процедур в Учреждении и Подконтрольных лицах;

6.3.5. Мониторинг событий информационной безопасности и реагирования на инциденты информационной безопасности в Учреждении и Подконтрольных лицах;

6.3.6. Взаимодействие со ФСТЭК России и ФСБ России по вопросам технической защиты информации, применения средств криптографической защиты и взаимодействия с ГосСОПКА;

6.3.7. Организация и участие в реализации мероприятий по ликвидации последствий инцидентов информационной безопасности в Учреждении и Подконтрольных лицах;

6.3.8. Организация и участие в расследованиях инцидентов информационной безопасности в Учреждении и Подконтрольных лицах;

6.3.9. Анализ результатов расследования инцидентов информационной безопасности в Учреждении и Подконтрольных лицах;

6.3.10. Организация и участие в аудитах информационной безопасности в Учреждении и Подконтрольных лицах.

7. ОПИСАНИЕ ТИПОВ ОБЪЕКТОВ ЗАЩИТЫ В ОБЛАСТИ ДЕЙСТВИЯ ПОЛИТИКИ

Обеспечение информационной безопасности в Обществе должно осуществляться в отношении информации и/или процессов (бизнес-процессов) к которым предъявлены требования по ИБ. Владелец риска (владелец бизнес-процесса) утверждает верхнеуровневые требования к ИБ: необходимость реализации мер обеспечения ИБ в принципе, требуемый уровень защищенности (категория значимости) [7].

Для установления учетности и ответственности в отношении каждого ИТ-актива должен быть определен владелец. Владелец ИТ-актива может не обладать правами собственности на ИТ-актив, но он несет ответственность за его получение, разработку, поддержку, использование и безопасность[8].

---

[7] В том числе с учетом конфиденциальности информации, предполагаемой к обработке или уже обрабатываемой и требований действующего законодательства.

[8] Пункт 8.2.1.2 ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности

Обработка информации и исполнения требований по информационной безопасности осуществляется в следующих основных типах средств автоматизации:

- Информационные системы, предназначенные для автоматизации процессов в рамках деятельности Учреждения и Подконтрольных лиц: автоматизированная система коммерческого учета электроэнергии (АСКУЭ), автоматизированные системы расчётов (биллинг), личные кабинеты клиентов, информационные порталы и пр., в том числе в составе объектов критической информационной инфраструктуры;
- Автоматизированные системы управления технологического процесса (АСУ ТП), в том числе в составе объектов критической информационной инфраструктуры;
- Средства диспетчерского и технологического управления, информационные системы и системы связи входящие в состав системы обмена технологической информацией с автоматизированной системой системного оператора (СОТИАССО): системы телемеханики, системы сбора и передачи информации (ССПИ, предназначенные для сбора и передачи оперативной диспетчерско-технологической информации о режиме работы энергообъекта (станции) на верхний уровень), системы телефонной связи (предназначены для передачи диспетчерских команд и ведения технологического режима по управлению энергетическим режимом работы энергообъекта, в рамках работы объекта в энергосистеме), системы автоматического вторичного регулирования частоты и мощности (АВРЧМ), терминал участника балансирующего рынка (Modes Terminal), регистраторы аварийных событий и процессов (РАСП), системы мониторинга переходных режимов (СМПР) и т.д.;
- Информационные системы, автоматизирующие вспомогательные процессы Учреждения и Подконтрольных лиц (бухгалтерский учет, кадровый учет, управлением закупками и пр.);
- Информационные сервисы, направленные на автоматизацию процессов в ИТ-инфраструктуре (единый каталог пользователей, централизованные системы идентификации и аутентификации, файлообменные ресурсы, корпоративная электронная почта и пр.).
- ИТ-инфраструктура и компоненты автоматизации управления ИТ-инфраструктурой (оборудование корпоративной сети передачи данных и локальных вычислительных сетей, вычислительное оборудование Центра обработки данных оборудование систем и сетей хранения данных, инфраструктура рабочих мест пользователей и пр.).

8. НОРМАТИВНЫЕ ССЫЛКИ[9]

8.1. Внешние нормативные ссылки

№ п/п	Номер и Дата документа	Наименование документа
1	ISO/IEC 27000:2018	Международный стандарт Information technology — Security techniques — Information security management systems — Overview and vocabulary
2	ISO/IEC 27001:2013	Международный стандарт «Information technology – Security techniques – Information security
3	от 26.07.2017 № 187-ФЗ	Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной
4	от 27.07.2006 № 152-ФЗ	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»
5	ГОСТ Р ИСО/МЭК 27005-2010	Информационная технология (ИТ). Методы и средства обеспечения безопасности. Менеджмент

[9] Нормативные правовые акты и внутренние нормативные документы, включенные в настоящий раздел, в случае внесения в них изменений, дополнений после утверждения данной Политики, применяются в актуальной редакции

8.2. Внутренние нормативные ссылки

№ п/п	Номер ВНД или Номер ОРД, Дата ОРД	Наименование документа
1		
2		
3		
4		

9. КОНТРОЛЬ ВЕРСИЙ ДОКУМЕНТА

Номер версии	Дата создания версии	Должность ответственного за разработку ВНД	ФИО Ответственного за разработку ВНД
1	28.08.2020	Отдел программного и технического обеспечения/Начальник отдела	Гагарин Олег Станиславович