АО «Хабаровская ремонтно-монтажная компания»

ПРИКАЗ
Хабаровск

25.12.2023 № 839/1

«О присоединении АО «Хабаровская ремонтно-монтажная компания» к Положению об охране конфиденциальности информации, составляющей коммерческую тайну в ПАО «РусГидро»»

Во исполнение приказа ПАО «РусГидро» от 07.12.2023 № 888 «Об охране конфиденциальности информации, составляющей коммерческую тайну в ПАО «РусГидро», а также во исполнение пункта 9,3 Плана-графика актуализации и разработки локальных нормативных документов (актов) ПАО «РусГидро», регламентирующих бизнес-процессы, на 2023-2024 годы,

Приказываю:

1. Присоединиться к Положению об охране конфиденциальности информации, составляющей коммерческую тайну в ПАО «РусГидро» (далее - Положение) и всем последующим изменениям к нему утвержденным приказом от 07.12.2023 № 888.

2. Считать Положение (Приложение) внутренним документом АО «ХРМК».

3. Начальнику отдела по работе с персоналом Ю.С. Литвиненко:

-обеспечить ознакомление с Положением работников, принимаемых на работу в исполнительный аппарат Общества, до подписания трудового договора;

- обеспечить ознакомление под подпись работников Общества с настоящим приказом в течении 10 рабочих дней с даты его издания;

- обеспечить представление в Департамент безопасности списки работников, которым предоставлен доступ к информации, составляющей коммерческую тайну

4. Контроль за исполнением настоящего приказа оставляю за собой.

И.о. Генерального директора А.Г. Шклярук

Приложение 1
к приказу АО «ХРМК»
от _____ . _____.2024 № _____

ПОЛОЖЕНИЕ
об охране конфиденциальности информации, составляющей коммерческую тайну, в АО «ХРМК»

СОДЕРЖАНИЕ

ГЛОССАРИЙ....3
РАЗДЕЛ I. ОБЩИЕ ПОЛОЖЕНИЯ....6
ГЛАВА 1. ЦЕЛЬ, НАЗНАЧЕНИЕ ПОЛОЖЕНИЯ И ПОРЯДОК ВНЕСЕНИЯ ИЗМЕНЕНИЙ 6
РАЗДЕЛ II. ОБЩЕЕ ОПИСАНИЕ МЕР ПО ОХРАНЕ КОНФИДЕНЦИАЛЬНОСТИ ИКТ 6
ГЛАВА 2. ЦЕЛИ И ЗАДАЧИ ОХРАНЫ КОНФИДЕНЦИАЛЬНОСТИ ИКТ 6
ГЛАВА 3. ПРИНЦИПЫ ОХРАНЫ КОНФИДЕНЦИАЛЬНОСТИ ИКТ 7
ГЛАВА 4. КЛЮЧЕВЫЕ УЧАСТНИКИ ОХРАНЫ КОНФИДЕНЦИАЛЬНОСТИ ИКТ 7
РАЗДЕЛ III. РЕАЛИЗАЦИЯ ПРАВ И ОБЯЗАННОСТЕЙ ОБЩЕСТВОМ И ЕГО РАБОТНИКАМИ ПРИ ОБРАЩЕНИИ С ИКТ 11
ГЛАВА 5. ПРАВА И ОБЯЗАННОСТИ ОБЩЕСТВА 11
ГЛАВА 6. ПРАВА И ОБЯЗАННОСТИ РАБОТНИКА ОБЩЕСТВА 11
РАЗДЕЛ IV. ОПИСАНИЕ СЦЕНАРИЯ «ОХРАНА КОНФИДЕНЦИАЛЬНОСТИ ИКТ», В ГРАНИЦАХ ПРОЦЕССА «УПРАВЛЕНИЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТЬЮ» 13
ГЛАВА 7. СЦЕНАРИЙ «ОХРАНА КОНФИДЕНЦИАЛЬНОСТИ ИКТ» 13
ГЛАВА 8. ЭТАП «РЕАЛИЗАЦИЯ МЕР ПО ОХРАНЕ КОНФИДЕНЦИАЛЬНОСТИ ИКТ» ..14
ГЛАВА 9. ЭТАП «МОНИТОРИНГ СОБЛЮДЕНИЯ МЕР ПО ОХРАНЕ КОНФИДЕНЦИАЛЬНОСТИ ИКТ В ОБЩЕСТВЕ» 20
ГЛАВА 10. ЭТАП «СОВЕРШЕНСТВОВАНИЕ МЕР ПО ОХРАНЕ КОНФИДЕНЦИАЛЬНОСТИ ИКТ» 24
Приложение 1 к Положению 30
Приложение 2 к Положению 33
Приложение 3 к Положению 34
Приложение 4 к Положению 35
Приложение 5 к Положению 36
Приложение 6 к Положению 37

ГЛОССАРИЙ

Термины и определения:

Группа РусГидро	–	Публичное акционерное общество «Федеральная гидрогенерирующая компания – РусГидро» и его подконтрольные организации.
Доступ к информации, составляющей коммерческую тайну	–	ознакомление определенных лиц с информацией, составляющей коммерческую тайну, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации.
Информация, составляющая коммерческую тайну	–	сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны.
Коммерческая тайна	–	режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.
Контрагент	–	сторона гражданско-правового договора, которой Общество передает информацию, составляющую его коммерческую тайну, или от которого такая информация получена.
Конфиденциальность информации	–	обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.
Материальный носитель информации, составляющей коммерческую тайну[1]	–	материальный объект, содержащий сведения, составляющие коммерческую тайну (бумажный носитель информации, составляющей коммерческую тайну (листы, книги, карточки и т.п.), электронный носитель информации, составляющей коммерческую тайну (CD / DVD диски, жесткие диски, съемные носители информации (флэш-память и т.п.)).
Обладатель информации, составляющей коммерческую тайну	–	лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании, ограничило

[1] Далее также по тексту – документ, содержащий ИКТ

		доступ к этой информации и установило в отношении ее режим коммерческой тайны.
Общество	–	акционерное общество «Хабаровская ремонтно-монтажная компания» (АО «ХРМК»).
Передача информации, составляющей коммерческую тайну	–	передача информации, составляющей коммерческую тайну, зафиксированной на материальном носителе, ее обладателем Контрагенту на основании договора в объеме и на условиях, которые предусмотрены договором, включая условие о принятии Контрагентом установленных договором мер по охране ее конфиденциальности.
Предоставление информации, составляющей коммерческую тайну	–	передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем органам государственной власти, иным государственным органам, органам местного самоуправления[2] в целях выполнения их функций.
Работник	–	физическое лицо, вступившее трудовые отношения с Обществом.
Работодатель	–	Общество, вступившее в трудовые отношения с работником.
Разглашение информации, составляющей коммерческую тайну	–	действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.
Режим коммерческой тайны	–	правовые, организационные, технические и иные, принимаемые обладателем информации, составляющей коммерческую тайну, меры по охране ее конфиденциальности[3].
Третьи лица	–	физические и юридические лица, не связанные гражданско-правовыми отношениями с Обществом или его Контрагентами в рамках заключенных договоров (соглашений о конфиденциальности).

Сокращения:

---

[2] Далее – государственные органы, органы местного самоуправления.

[3] Перечень обязательных мер по охране конфиденциальности информации, составляющей коммерческую тайну, определен ст. 10 Федерального закона от 29.07.2004 № 98-ФЗ «О коммерческой тайне».

ИКТ – информация, составляющая коммерческую тайну.

КТ – коммерческая тайна.

КСД – корпоративная система документооборота.

ЛНД (А) – локальный нормативный документ (акт).

РАЗДЕЛ I. ОБЩИЕ ПОЛОЖЕНИЯ

ГЛАВА 1. ЦЕЛЬ, НАЗНАЧЕНИЕ ПОЛОЖЕНИЯ И ПОРЯДОК ВНЕСЕНИЯ ИЗМЕНЕНИЙ

1.1. Положение об охране конфиденциальности информации, составляющей коммерческую тайну, в АО «ХРМК» (далее – Положение) определяет требования к организации процесса «Управление экономической безопасностью» в части сценария «Охрана конфиденциальности информации, составляющей коммерческую тайну, в АО «ХРМК» (далее бизнес-процесс).

1.2. Целью Положения является:

– определение целей и задач охраны конфиденциальности ИКТ в Обществе;

– определение принципов охраны конфиденциальности ИКТ в Обществе;

– определение ключевых участников процедур охраны конфиденциальности ИКТ в Обществе;

– установление прав и обязанностей Общества и его работников при обращении с ИКТ;

– определение мер по охране конфиденциальности ИКТ в Обществе.

1.3. Положение основывается на:

– Конституции Российской Федерации;

– Гражданском кодексе Российской Федерации;

– Трудовом кодексе Российской Федерации;

– Федеральном законе от 29.07.2004 № 98-ФЗ «О коммерческой тайне»;

– Федеральном законе от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации».

1.4. Отдельные нормы, не вошедшие в Положение и относящиеся к компетенции структурных подразделений и должностных лиц Общества, участвующих в пределах своих полномочий в процедурах обработки ИКТ, подлежат определению в иных ЛНД (А) Общества, издаваемых в развитие Положения[4].

1.5. Положение и изменения к нему утверждаются приказом Генерального директора Общества по представлению заместителя Генерального директора Общества по представлению специалиста по безопасности.

РАЗДЕЛ II. ОБЩЕЕ ОПИСАНИЕ МЕР ПО ОХРАНЕ КОНФИДЕНЦИАЛЬНОСТИ ИКТ

ГЛАВА 2. ЦЕЛИ И ЗАДАЧИ ОХРАНЫ КОНФИДЕНЦИАЛЬНОСТИ ИКТ

---

[4] Действие Положения не распространяется на информацию:

– отнесенную в установленном порядке к государственной тайне Российской Федерации, а также на сведения, являющиеся персональными данными физических лиц (субъектов персональных данных);

– подлежащую обязательному раскрытию в соответствии с законодательством о рынке ценных бумаг Российской Федерации.

2.1. Целью охраны конфиденциальности ИКТ является предотвращение возможного нанесения ущерба экономической безопасности Общества и его Контрагентам вследствие неправомерного использования (утраты, хищения, разглашения или фальсификации) ИКТ.

2.2. Для достижения цели охраны конфиденциальности ИКТ требуется решение следующих задач:

– определение перечня информации, составляющей коммерческую тайну АО «ХРМК» (далее – Перечень ИКТ);

– ограничение доступа к ИКТ;

– учет лиц, получивших доступ к ИКТ, и / или лиц, которым такая информация была предоставлена или передана;

– установление ответственности лиц, получивших доступ к ИКТ, за нарушение порядка обращения с ИКТ;

– принятие мер по охране конфиденциальности ИКТ.

ГЛАВА 3. ПРИНЦИПЫ ОХРАНЫ КОНФИДЕНЦИАЛЬНОСТИ ИКТ

3.1. Охрана конфиденциальности ИКТ основывается на следующих ключевых принципах.

3.1.1. Законность.

Требования к охране конфиденциальности ИКТ полностью соответствуют нормам законодательства Российской Федерации, не противоречат Уставу и иным ЛНД(А) Общества. Режим КТ не может быть использован в целях, противоречащих требованиям защиты нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства, для сокрытия фактов бесхозяйственности, недобросовестной конкуренции и других негативных явлений в деятельности Общества.

3.1.2. Разумная достаточность.

Меры, принимаемые в целях охраны конфиденциальности ИКТ, должны быть соразмерны ценности информационных ресурсов и величине возможного ущерба от нарушения конфиденциальности охраняемых сведений.

3.1.3. Ценность информации.

При выработке мер по охране конфиденциальности ИКТ учитывается ее действительная или потенциальная коммерческая ценность в силу неизвестности ее третьим лицам.

3.1.4. Актуальность.

При отнесении информации к КТ учитывается жизненный цикл относимых сведений.

ГЛАВА 4. КЛЮЧЕВЫЕ УЧАСТНИКИ ОХРАНЫ КОНФИДЕНЦИАЛЬНОСТИ ИКТ

4.1. Генеральный директор Общества:

– утверждает Перечень ИКТ Общества;

– утверждает ЛНД (А) Общества, устанавливающие меры, направленные на охрану конфиденциальности ИКТ.

4.2. Заместители Генерального директора Общества:

– представляют предложения в рамках компетенций в Перечень ИКТ.

4.3. Комиссия по соблюдению режима коммерческой тайны (далее – Комиссия):

– представляет Перечень ИКТ и изменения в него на утверждение Генеральному директору Общества;

– определяет меры (административные, технические, экономические, правовые), направленные на ограничение доступа к ИКТ, путем установления, изменения либо прекращения режима КТ в отношении информации, обладателем которой является Общество, а также контроля за соблюдением режима КТ в Обществе с учетом требований законодательства Российской Федерации и ЛНД (А) Общества.

4.4. Специалист по безопасности:

– организовывает и контролирует соблюдение режима КТ в Обществе;

– координирует деятельность структурных подразделений Общества по вопросам охраны конфиденциальности ИКТ;

– организовывает взаимодействие с государственными органами, наделенными полномочиями по осуществлению государственного контроля (надзора) в части, касающейся вопросов обеспечения безопасности;

– инициирует и контролирует проведение предварительных проверочных мероприятий / служебных проверок / расследований по фактам (признакам) нарушения режима КТ, в том числе своевременность и объективность их проведения.

– организовывает деятельность по обеспечению защиты ИКТ, при ее обработке в информационных системах Общества;

– организовывает и контролирует процессы защиты ИКТ от неправомерного доступа и использования, а также процессы передачи ИКТ третьим лицам;

– согласовывает проведение предварительных проверочных мероприятий / служебных проверок / расследований по фактам (признакам) нарушения режима КТ в части разглашения / утечки ИКТ, произошедших при ее обработке и передаче с использованием средств автоматизации (в информационных системах).

– организовывает деятельность по соблюдению режима КТ в Обществе и его мониторингу;

– обеспечивает разработку (поддержание в актуальном состоянии) Перечня ИКТ;

– планирует мероприятия по охране конфиденциальности ИКТ, организует их выполнение и осуществляет контроль за их эффективностью;

– организовывает разработку и внесение изменений в ЛНД (А) Общества, регламентирующие порядок обращения с ИКТ и охрану ее конфиденциальности;

– организовывает и осуществляет проведение контрольных мероприятий за соблюдением режима КТ в Обществе;

– осуществляет проведение предварительных проверочных мероприятий, служебных проверок и служебных расследований по признакам нарушений режима КТ в Обществе;

– организовывает ведение учета работников Общества, которым предоставлен доступ к ИКТ;

– выносит на рассмотрение вопросы, касающиеся реализации и изменения мер по охране конфиденциальности ИКТ.

4.5. Начальник отдела по работе с персоналом:

– обеспечивает внесение в трудовые договоры с работниками положений об охране конфиденциальности ИКТ;

– организовывает ознакомление с Положением и Перечнем ИКТ работников, принимаемых на работу в Общество.

4.6. Начальник отдела корпоративно-правового сопровождения:

– организовывает оказание поддержки и консультирования по правовым вопросам, связанным с охраной конфиденциальности ИКТ.

4.7. Начальник группы информационных технологий связи:

– обеспечивает защиту ИКТ при ее обработке с использованием средств автоматизации (в информационных системах);

– обеспечивает поддержание технических средств информационных систем и средств защиты информации, используемых при обработке ИКТ, в работоспособном состоянии;

– обеспечивает проведение мониторинга соблюдения режима КТ при обработке ИКТ с использованием средств автоматизации (в информационных системах);

– осуществляет руководство деятельностью по внедрению, настройке и вводу в эксплуатацию технических средств защиты ИКТ;

– инициирует проведение предварительных проверочных мероприятий, служебных проверок и расследований по фактам разглашения или утечки ИКТ, произошедших при ее обработке и передаче с использованием средств автоматизации (в информационных системах).

4.8. Начальник группы управления делами:

– организовывает прием и первичную обработку входящей документированной информации, содержащей КТ (гриф «Коммерческая тайна»).

4.9. Секретарь совета директоров Общества:

– представляет предложения в рамках компетенций в Перечень ИКТ.

4.10. Руководители структурных подразделений Общества, в которых осуществляется обработка ИКТ:

– обеспечивают создание необходимых условий для соблюдения режима КТ подчиненными работниками;

– представляют предложения в рамках компетенций по поддержанию в актуальном состоянии Перечня ИКТ;

– при выявлении фактов утраты (хищения, разглашения или фальсификации) ИКТ информируют специалиста по безопасности;

– определяют круг лиц (работников структурного подразделения) Общества, которым предоставляется доступ к ИКТ.

4.11. Директор филиала Общества:

– руководит деятельностью по соблюдению режима КТ в филиале;

– организовывает подготовку и направление в Комиссию предложений по актуализации Перечня ИКТ;

– утверждает список работников филиала, которым предоставлен доступ к ИКТ.

– обеспечивает соблюдение режима КТ в филиале;

– организовывает выполнение мероприятий по обеспечению информационной безопасности в филиале, в том числе по защите ИКТ при ее обработке с использованием средств автоматизации (в информационных системах);

– разрабатывает предложения по актуализации Перечня ИКТ;

– организовывает ведение учета работников филиала, которым предоставлен доступ к ИКТ;

– организовывает и принимает участие в проведении предварительных проверочных мероприятий / служебных проверок / расследований по фактам (признакам) нарушений режима КТ в филиале.

– обеспечивает внесение в трудовые договора с работниками филиала положений о соблюдении режима КТ;

– организовывает ознакомление с Положением и Перечнем ИКТ работников, принимаемых на работу в филиал Общества;

– осуществляет прием и первичную обработку входящей документированной ИКТ;

– организовывает оказание поддержки и консультирования в филиале по правовым вопросам, связанным с охраной конфиденциальности ИКТ;

– обеспечивают создание необходимых условий для соблюдения режима КТ подчиненными работниками;

– представляют предложения в рамках компетенций по поддержанию в актуальном состоянии Перечня ИКТ;

– при выявлении фактов утраты (хищения, разглашения или фальсификации) ИКТ информируют специалиста по безопасности;

– определяют круг лиц (работников структурного подразделения) в филиале, которым предоставляется доступ ИКТ.

4.12. Работники Общества, которым предоставлен доступ к ИКТ:

– осуществляют обработку ИКТ с соблюдением требований по охране ее конфиденциальности в соответствии со своими должностными обязанностями, а также с учетом прав и обязанностей, закрепленных в главе 6 Положения.

4.13. Контрагенты, государственные органы, органы местного самоуправления.

Регулирование отношений, связанных с обращением с ИКТ в ходе взаимодействия с Контрагентами, государственными органами, органами местного самоуправления осуществляется в соответствии с п. 8.4.3 Положения.

РАЗДЕЛ III. РЕАЛИЗАЦИЯ ПРАВ И ОБЯЗАННОСТЕЙ ОБЩЕСТВОМ И ЕГО РАБОТНИКАМИ ПРИ ОБРАЩЕНИИ С ИКТ

ГЛАВА 5. ПРАВА И ОБЯЗАННОСТИ ОБЩЕСТВА

5.1. Общество имеет право:

– использовать ИКТ Общества по собственному усмотрению любым способом, не противоречащим законодательству Российской Федерации;

– разрешать или запрещать доступ к ИКТ, определять порядок и условия доступа к этой информации;

– вводить в гражданский оборот ИКТ на основании договоров, предусматривающих условия об охране ее конфиденциальности;

– требовать от юридических и физических лиц, государственных органов, органов местного самоуправления, которым предоставлена ИКТ, соблюдения обязанностей по охране ее конфиденциальности;

– требовать от лиц, получивших доступ к ИКТ случайно или по ошибке, охраны ее конфиденциальности;

– защищать в установленном законом порядке права в случае разглашения, незаконного получения или незаконного использования третьими лицами ИКТ, в том числе требовать возмещения убытков, причиненных в связи с нарушением его прав.

5.2. В целях предотвращения разглашения ИКТ и / или создания предпосылок к этому Общество:

– оставляет за собой право, но не принимает каких-либо обязательств контролировать надлежащие использование работниками технических средств хранения, обработки и передачи информации, соблюдение ими установленных режимных мер по охране конфиденциальности ИКТ в соответствии с ЛНД (А) Общества;

– оставляет за собой право проводить контрольные мероприятия в отношении использования работником средств хранения, обработки и передачи информации. В случае несогласия работника с проведением указанных мероприятий Общество вправе не предоставлять ему в пользование соответствующие технические средства;

– при наличии в действиях лица, разгласившего ИКТ, признаков административного правонарушения или преступления руководство Общества вправе обратиться в правоохранительные органы для привлечения такого лица к ответственности в соответствии с законодательством Российской Федерации;

– при причинении лицом, разгласившим ИКТ, ущерба Обществу и при отказе добровольно возместить его, Общество вправе обратиться в суд за защитой своих интересов.

ГЛАВА 6. ПРАВА И ОБЯЗАННОСТИ РАБОТНИКА ОБЩЕСТВА

6.1. Работник Общества, имеющий доступ к ИКТ, обязан:

– знать и выполнять установленный работодателем режим КТ, требования Положения и иных ЛНД (А) Общества, регулирующие отношения в сфере защиты информации, знать Перечень ИКТ Общества;

– не разглашать ИКТ, обладателями которой являются Общество и его Контрагенты, и без их согласия не использовать ИКТ, а также не использовать ИКТ в личных целях;

– информировать непосредственного руководителя или лицо, его замещающего о фактах разглашения ИКТ или нарушения порядка обращения с документами, содержащими ИКТ, о попытках несанкционированного доступа к ИКТ лиц, не имеющих на то права, о фактах утраты или недостачи документов, содержащих ИКТ, ключей от служебных помещений, сейфов, шкафов и рабочих столов, где хранятся документы, содержащие ИКТ, личных печатей и других событиях, создающих предпосылки для несанкционированного доступа к ИКТ;

– препятствовать попыткам работников Общества или иных лиц, имеющих доступ к ИКТ, совершать действия, которые могут привести к разглашению ИКТ (оставлять документы, содержащие ИКТ, без контроля, сообщать сведения, отнесенные к ИКТ, в личной беседе, на совещаниях, по телефону лицам, не имеющим права доступа к ИКТ и т.п.);

– соблюдать правила пользования документами, содержащими ИКТ, обеспечивать в процессе работы охрану конфиденциальности ИКТ и предотвращать попытки доступа к ней посторонних лиц в соответствии с Положением и иными ЛНД (А) Общества;

– знакомиться только с той информацией, к которой получен доступ в силу исполнения должностных обязанностей;

– представлять по требованию специалиста по безопасности или директора (в филиалах) письменные объяснения о допущенных нарушениях установленного порядка обращения с ИКТ, а также о фактах разглашения ИКТ;

– оказывать помощь и содействие при проведении предварительных проверочных мероприятий, служебных проверок / расследований по фактам нарушения режима КТ, попыток его нарушения или подготовки к нарушению;

– в случае установления виновности работника в разглашении ИКТ, возместить ущерб, причиненный нарушением права Общества на ИКТ.

6.2. При прекращении / расторжении трудового договора работник, которому был предоставлен доступ к ИКТ, обязан:

– передать уполномоченному работнику своего структурного подразделения или непосредственному руководителю все имеющиеся у него материальные носители ИКТ, полученные и / или созданные им в рамках выполнения трудовых обязанностей и / или взаимодействия с Контрагентами, государственными органами и органами местного самоуправления;

– не разглашать ИКТ, обладателем которой являются Общество и Контрагенты, ставшую известной в период срока действия трудового договора и после его прекращения / расторжения (в течение срока, установленного Перечнем ИКТ), не использовать ИКТ в личных целях.

6.3. Работнику, имеющему доступ к ИКТ, запрещается:

– передавать документы, содержащие ИКТ, без документального оформления факта передачи, а также передавать их работникам Общества, которым не положен доступ к работе с ИКТ, или знакомить их с ИКТ в любой форме;

– передавать ИКТ в электронном виде по любым техническим каналам связи без использования средств защиты информации, принятых Обществом в эксплуатацию в установленном порядке[5];

– использовать ИКТ при осуществлении научной и педагогической деятельности, в открытой переписке, публикациях в СМИ, различного рода публичных выступлениях, в личных интересах, а также для занятия иными видами деятельности, не связанными с выполнением трудовых обязанностей в Обществе;

– снимать копии с документов, содержащих ИКТ, или производить выписки из них, а также использовать различные технические средства (фотоаппараты, видео и звукозаписывающую аппаратуру) для их записи, без письменного распоряжения соответствующего руководителя;

– сохранять ИКТ в электронном виде на материальные носители, не учтенные предварительно в установленном порядке в качестве материальных носителей ИКТ;

– выносить документы, содержащие ИКТ, из зданий Общества, а также выполнять какие-либо работы, связанные с ИКТ, вне служебных помещений (в исключительных случаях, с разрешения руководителя структурного подразделения возможен вынос документов, содержащих ИКТ, из служебного помещения, в котором они хранятся, для их обсуждения, согласования или подписания в сторонних организациях[6]).

6.4. Ответственность за разглашение ИКТ несет работник Общества, получивший доступ к таким сведениям и допустивший их утечку (разглашение, утрату материального носителя).

6.5. Невыполнение работником Общества требований Положения и причинение Обществу ущерба вследствие разглашения ИКТ или ее неправомерного использования влечет дисциплинарную, материальную, гражданско-правовую, административную и уголовную ответственность в соответствии с законодательством Российской Федерации.

РАЗДЕЛ IV. ОПИСАНИЕ СЦЕНАРИЯ «ОХРАНА КОНФИДЕНЦИАЛЬНОСТИ ИКТ», В ГРАНИЦАХ ПРОЦЕССА «УПРАВЛЕНИЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТЬЮ»

ГЛАВА 7. СЦЕНАРИЙ «ОХРАНА КОНФИДЕНЦИАЛЬНОСТИ ИКТ»

---

[5] Допускается использование возможности шифрованного обмена сообщениями внутри сегмента корпоративной электронной почты с соблюдением требований Политики информационной безопасности ПАО «РусГидро», АО «ХРМК». Обмен ИКТ с Контрагентами осуществляется в соответствии с правилами, оговоренными в Соглашениях о конфиденциальности.

[6] К сторонним организациям.

7.1. Целевыми результатами Сценария являются:

– обеспечение охраны конфиденциальности ИКТ в Обществе;

– недопущение неправомерного использования конфиденциальной информации, ее утраты, хищения, разглашения или фальсификации.

7.2. Сценарий инициируется установлением в Обществе режима КТ в целях обеспечения соблюдения требований нормативных правовых актов Российской Федерации, регулирующих отношения, связанные с обращением с ИКТ.

7.3. Сценарий состоит из следующих этапов:

– реализация мер по охране конфиденциальности ИКТ;

– мониторинг соблюдения мер по охране конфиденциальности ИКТ в Обществе;

– совершенствование мер по охране конфиденциальности ИКТ.

ГЛАВА 8. ЭТАП «РЕАЛИЗАЦИЯ МЕР ПО ОХРАНЕ КОНФИДЕНЦИАЛЬНОСТИ ИКТ»

8.1. Целью Этапа является обеспечение соблюдения требований законодательства Российской Федерации и ЛНД (А) Общества при обращении с ИКТ, исключение доступа к ИКТ Общества любых лиц без согласия обладателя ИКТ, а также обеспечение возможности использования ИКТ Общества работниками и передачи ее Контрагентам / государственным органам, органам местного самоуправления без нарушения режима КТ.

8.2. Входящими данными (видами инициирующих событий) Этапа являются:

– утверждение Положения;

– утверждение (актуализация) Перечня ИКТ;

– утвержденные ЛНД (А) Общества, определяющие (уточняющие) меры по охране конфиденциальности ИКТ в Обществе;

– подтверждение актуальности действующих ограничений в отношении ИКТ;

– подтверждение выполнения мер по охране конфиденциальности ИКТ в Обществе, либо информация об их корректировке.

8.3. Результатом Этапа являются:

– регистрация (постановка на учет) поступивших в работу документов, содержащих ИКТ;

– обеспечение условий для соблюдения работниками Общества мер по охране конфиденциальности ИКТ;

– заключение соглашений (договоров) о конфиденциальности с Контрагентами;

– исполнение Обществом обязанностей по предоставлению ИКТ государственным органам, органам местного самоуправления.

8.4. Этап состоит из следующих процедур:

– учет документов, содержащих ИКТ;

– охрана конфиденциальности ИКТ в рамках трудовых отношений;

– охрана конфиденциальности ИКТ при ее предоставлении.

8.4.1. Процедура «Учет документов, содержащих ИКТ»:

– инициируется (в дополнение к событиям, указанным в п. 8.2 Положения) поступлением в работу документов, содержащих ИКТ;

– результатом выполнения Процедуры является регистрация документов, содержащих ИКТ, в «Журнале регистрации и учета входящих документов / носителей ИКТ» либо в КСД (путь: Документы/Журналы регистрации/ИА.КТ. Входящие документы).

8.4.1.1. На все документы, содержащие ИКТ, специалист по безопасности / директор (в филиале Общества) наносится гриф «Коммерческая тайна».

Форма грифа представлена в приложении 2 к Положению.

8.4.1.2. За организацию учета документов, содержащих ИКТ, и их материальных носителей в структурных подразделениях отвечают руководители структурных подразделений ИА и филиалов Общества, в которых осуществляется обработка ИКТ, с документальной фиксацией в соответствующих журналах учета (типовые формы Журналов приведены в приложениях 3 – 5 к Положению) либо в КСД.

8.4.1.3. Контроль за ведением учета документов, содержащих ИКТ, и их материальных носителей в ИА Общества осуществляет группа управления делами, специалист по безопасности и группа информационных технологий и связи (в части касающейся машинных носителей информации), в филиалах Общества – директора.

8.4.2. Процедура «Охрана конфиденциальности ИКТ в рамках трудовых отношений»:

– инициируется (в дополнение к событиям, указанным в п. 8.2 Положения) заключением трудового договора с работником и возникновением необходимости привлечения работника к работе с ИКТ;

– результатом процедуры является обеспечение Обществом условий для соблюдения работником мер по охране конфиденциальности ИКТ, предусмотренных трудовым договором.

8.4.2.1. Обязанности всех работников Общества по обеспечению сохранности ИКТ предусмотрены положениями заключенных с ними трудовых договоров, а также Положением.

8.4.2.2. При приеме на работу ознакомление работника с Положением и Перечнем ИКТ осуществляется наряду с иными ЛНД (А) Общества до подписания трудового договора в соответствии с требованиями ст. 68 ТК РФ.

Лист ознакомления с ЛНД (А) Общества при приеме на работу работника хранится в отделе по работе с персоналом.

Ознакомление работников с ЛНД (А) Общества, которые вносят изменения в Положение и Перечень ИКТ, осуществляется посредством КСД в установленном порядке.

Обязательства по обеспечению работником сохранности конфиденциальности ИКТ Общества включаются в соответствующий раздел трудового договора.

8.4.2.3. Предоставляя доступ работникам к ИКТ, в целях соблюдения работниками режима КТ, Общество:

– обеспечивает работников автоматизированными рабочими местами (далее – АРМ), соответствующими требованиям по исключению несанкционированного доступа к обрабатываемой информации, с учетом расположения АРМ, исключающего случайное ознакомление с ИКТ работников, которым доступ к ИКТ не требуется;

– предоставляет доступ работникам к КСД и иным информационным системам, посредством которых осуществляется обработка ИКТ;

– предоставляет работникам рабочие места, оборудованные запираемыми на ключ ящиками стола (сейфом, шкафом и т.п.).

8.4.2.4. Доступ к ИКТ в полном объеме предоставляется членам Совета директоров Общества, Генеральному директору Общества, заместителям Генерального директора, специалисту по безопасности, начальнику отдела корпоративно-правового сопровождения, начальнику группы управления делами, секретарю Совета директоров Общества.

В филиалах Общества доступ к ИКТ в полном объеме предоставляется директорам филиалов.

8.4.2.5. Работникам Общества, кроме указанных в п. 8.4.2.4 непосредственный доступ к ИКТ предоставляется, если данная информация необходима для выполнения их трудовых обязанностей[7].

Предоставление им доступа инициируется руководителями структурных подразделений в отношении своих подчиненных и оформляется следующим образом:

8.4.2.5.1. Руководители структурных подразделений, в которых предполагается, либо осуществляется обработка ИКТ, формируют списки работников, которым предоставляется доступ к ИКТ (рекомендуемая форма списка приведена в приложении 6 к Положению).

8.4.2.5.2. Списки работников Общества, которым предоставляется доступ к ИКТ, утверждаются по каждому структурному подразделению отдельно, либо по Блоку (на усмотрение руководства) организационно-распорядительными документами заместителя Генерального директора, директора по направлению деятельности, руководителя структурного подразделения прямого подчинения Председателю Правления – Генеральному директору.

8.4.2.5.3. Списки работников филиалов Общества, которым предоставляется доступ к ИКТ, утверждаются организационно-распорядительным документом директора филиала.

8.4.2.5.4. После подписания организационно - распорядительных документов, указанных в пунктах 8.4.2.5.2 и 8.4.2.5.3 Положения, списки работников, которым предоставлен доступ к ИКТ, направляются:

– Специалисту по безопасности – в отношении работников структурных подразделений Общества;

---

[7] Доступ работника к ИКТ осуществляется с его согласия, если это не предусмотрено его трудовыми обязанностями

– Директору филиала – в отношении работников структурных подразделений филиала.

8.4.2.5.5. Актуализация списков работников, которым предоставлен доступ к ИКТ, осуществляется по мере необходимости, но не реже 1 (одного) раза в год. Изменения вносятся в порядке, установленном в п. 8.4.2.5.1 – 8.4.2.5.4 Положения.

8.4.2.6. Сводный учет работников, которым предоставлен доступ к ИКТ, осуществляется специалист по безопасности.

8.4.2.7. Доступ работника к ИКТ прекращается, в следующих случаях:

– прекращение / расторжение трудового (гражданско-правового) договора (независимо от причин прекращения / расторжения);

– нарушение работником условий трудового (гражданско-правового) договора или ЛНД (А) Общества, связанных с неразглашением и обеспечением конфиденциальности ИКТ;

– перевода работника на должность, не требующую доступа к ИКТ, и / или изменения трудовых обязанностей.

8.4.2.8. Сведения о работниках, доступ к ИКТ которым прекращен, предоставляются в специалисту по безопасности руководителем соответствующего структурного подразделения с последующим внесением изменений в список работников.

8.4.3. Процедура «Охрана конфиденциальности ИКТ при ее предоставлении»:

– инициируется (в дополнение к событиям, указанным в п. 8.2 Положения) возникновением договорных отношений, связанных с обращением с ИКТ и / или возникновением у Общества обязательств по предоставлению ИКТ государственным органам, органам местного самоуправления;

– результатами процедуры являются заключение соглашений (договора) о конфиденциальности с Контрагентами и / или предоставлением ИКТ государственным органам, органам местного самоуправления.

8.4.3.1. Отношения Общества с Контрагентами, которым Обществом передается ИКТ или от которого ИКТ получена, регулируются гражданско-правовыми договорами.

8.4.3.2. Общество вправе требовать охрану конфиденциальности ИКТ Общества и / или Контрагентов от лиц, получивших доступ к этой информации в результате действий, осуществленных случайно или по ошибке.

8.4.3.3. Обязательства Контрагента по обеспечению сохранности КТ перед Обществом, могут закрепляться отдельным соглашением.

8.4.3.4. Требования к порядку подготовки (разработки), согласования, оформления, подписания, изменения, прекращения (расторжения), регистрации, учета и хранения, а также исполнения договоров, заключаемых от имени Общества, и соглашений о конфиденциальности к ним устанавливаются отдельным ЛНД (А) Общества[8].

---

[8] Приказ Общества от 30.06.2020 № 515 «Об утверждении Положения о договорной работе в ПАО «РусГидро».

8.4.3.5. Ответственность за принятие решения о составе, объеме, порядке передачи и использования ИКТ, предоставляемой Контрагенту, возлагается на лицо, подписавшее соответствующий гражданско-правовой договор.

8.4.3.6. Передача ИКТ Общества Контрагентам в соответствии с заключенными договорами производится только на материальных носителях, на которые нанесен гриф «Коммерческая тайна», с регистрацией факта передачи.

8.4.3.7. Предоставление Контрагенту ИКТ на материальных носителях, не имеющих грифа «Коммерческая тайна», а также направление документов, содержащих ИКТ, третьим лицам запрещается.

8.4.3.8. Документы, содержащие ИКТ на материальных носителях, могут направляться Контрагентам следующими способами:

- фельдъегерской связью;
- заказными или ценными почтовыми отправлениями;
- нарочно.

8.4.3.9. Направление Контрагентам ИКТ в электронном виде с использованием средств связи общего пользования и глобальной информационной сети интернет (по электронной почте) допускается только при условии использования криптографических средств защиты информации, принятых Обществом и Контрагентом в эксплуатацию в установленном порядке, а также наличия соглашения между Обществом и Контрагентом о ведении электронного документооборота, в котором регулируются вопросы охраны конфиденциальности, подтверждения подлинности документов и неотказуемости от авторства.

Во всех остальных случаях использование незащищенных каналов связи для передачи ИКТ Контрагентам запрещается.

8.4.3.10. Предоставление ИКТ государственным органам, органам местного самоуправления в целях выполнения ими своих функций производится Обществом по мотивированному требованию соответствующего органа власти, контрольного (надзорного) органа. Мотивированное требование должно быть подписано уполномоченным должностным лицом, содержать указание цели и правовое основание затребования ИКТ, срок предоставления этой информации, если иное не установлено законодательством Российской Федерации. Общество обязано предоставлять ИКТ по запросам судов, органов прокуратуры, органов предварительного следствия, органов дознания по делам, находящимся в их производстве, и другим контрольным (надзорным) органам в порядке и на основаниях, которые предусмотрены законодательством Российской Федерации.

Предоставление ИКТ государственным органам, органам местного самоуправления без запроса от них производится в случаях, когда такое предоставление обязательно и необходимо для совершения действий в интересах Общества (оформление паспорта внешнеторговой сделки, получение лицензий, обращение в суд и др.).

8.4.3.11. Запросы государственных органов, органов местного самоуправления на предоставление ИКТ принимаются в письменном виде

или в форме электронного документа. Устные запросы на предоставление ИКТ, в том числе полученные по телефону, рассмотрению не подлежат.

Запросы в форме электронного документа должны быть подписаны усиленной квалифицированной электронной подписью соответствующего руководителя и соответствовать требованиям законодательства Российской Федерации в сфере использования электронных подписей.

При получении запроса в форме электронного документа (по электронной почте) работник Общества, которому поручена подготовка ответа по запросу, проверяет, принадлежность адреса электронной почты или телефонного номера, указанного в запросе, органу власти, направившему запрос, а также удостоверяется, что должностное лицо, указанное в качестве инициатора запроса, занимает соответствующую должность в данном органе власти.

Запросы на предоставление ИКТ по электронной почте принимаются к рассмотрению только в том случае, если доменный адрес почтовой системы принадлежит соответствующему государственному органу, органу местного самоуправления. В случаях, когда адрес электронной почты отправителя запроса получен в общедоступной почтовой системе (mail.ru, rambler.ru, gmail.com, aol.com и им подобных), запрос рассмотрению не подлежит, о чем уведомляется отправитель запроса на указанный им электронный адрес. После получения запроса лицо, ответственное за подготовку ответа, удостоверяется в том, что правообладателем запрашиваемой информации является Общество, запрашиваемая информация находится в ведении соответствующего государственного органа, органа местного самоуправления, а возможность ее предоставления предусмотрена законодательством Российской Федерации. Ответы на запросы, содержащие ИКТ Общества, направляются в письменном виде, с использованием специальной связи.

Предоставление ИКТ государственным органам, органам местного самоуправления в электронном виде с использованием средств связи общего пользования и сети интернет (по электронной почте) запрещается, кроме случаев, указанных в п. 8.4.3.12 Положения.

8.4.3.12. Направление ответов, содержащих ИКТ Общества, на запросы государственных органов, органов местного самоуправления в электронном виде возможно только в случае наличия с ними каналов связи, закрытых с использованием сертифицированных ФСБ России средств криптографической защиты информации (например, предназначенных для сдачи налоговой, пенсионной и иной отчетности), организованных соответствующим органом, при наличии у Общества необходимых сертификатов соответствия, ключей шифрования и средств электронной подписи, необходимых программных средств и выполнении иных условий охраны конфиденциальности ИКТ.

8.4.3.13. Если в формах электронной отчетности государственных органов, органов местного самоуправления отсутствуют поля (графы), позволяющие указать, что предоставляемые сведения относятся к ИКТ Общества, об этом сообщается в соответствующий орган любым документируемым способом

(почтой, электронной почтой), имеющим систему подтверждения доставки корреспонденции, или письмом, доставляемым курьером.

8.4.3.14. На всех материальных носителях ИКТ, предоставляемых по запросу, проставляется гриф «Коммерческая тайна».

8.4.3.15. Направление документов, содержащих ИКТ, на материальных носителях, не имеющих грифа «Коммерческая тайна», запрещается.

8.4.3.16. В ответе на запрос государственного органа, органа местного самоуправления о предоставлении информации (в сопроводительном письме) в обязательном порядке сообщается о наличии в предоставляемых материалах ИКТ Общества (с указанием наименований и иных реквизитов их материальных носителей ИКТ), а также делается отметка о необходимости охраны конфиденциальности предоставляемой ИКТ.

8.4.3.17. Ответы на запросы государственных органов, органов местного самоуправления о предоставлении ИКТ Общества подписываются Генеральным директором Общества, либо лицом, действующим по доверенности.

В филиалах Общества ответы на запросы подписываются директором филиала.

ГЛАВА 9. ЭТАП «МОНИТОРИНГ СОБЛЮДЕНИЯ МЕР ПО ОХРАНЕ КОНФИДЕНЦИАЛЬНОСТИ ИКТ В ОБЩЕСТВЕ»

9.1. Целью Этапа является систематическая оценка соответствия принимаемых в Обществе мер по охране конфиденциальности ИКТ требованиям законодательства Российской Федерации во взаимосвязи с коммерческими интересами Общества, выявление потребностей в их актуализации, а также принятие мер реагирования по фактам нарушений порядка обращения с ИКТ в Обществе, приведшим (создавшим предпосылки) к ее разглашению (утрате).

9.2. Входящими данными (видами инициирующих событий) Этапа являются:

– регистрация (постановка на учет) поступивших в работу документов, содержащих ИКТ;

– обеспечение условий для соблюдения работниками Общества мер по охране конфиденциальности ИКТ;

– заключение соглашений (договоров) о конфиденциальности с Контрагентами;

– исполнение Обществом обязанностей по предоставлению ИКТ государственным органам, органам местного самоуправления.

9.3. Результатами Этапа являются:

– подтверждение результативности мер по охране конфиденциальности ИКТ в Обществе;

– подтверждение актуальности действующих ограничений в отношении ИКТ;

– окончание срока действия ограничения доступа к ИКТ;

– наступление событий, позволяющих отменить режим КТ в отношении определенных сведений;

– утрата коммерческой ценности сведениями, ранее отнесенными к ИКТ;

– получение от ключевых участников сценария предложений о внесении изменений в Перечень ИКТ;

– решение о необходимости принятия мер воздействия к лицам, допустившим нарушения мер по охране конфиденциальности ИКТ;

– принятие решения о необходимости корректировки мер по охране конфиденциальности ИКТ;

9.4. Этап состоит из следующих процедур:

– мониторинг соблюдения мер по охране конфиденциальности ИКТ;

– оценка актуальности действующих ограничений в отношении ИКТ;

– комплексный анализ соблюдения мер по охране конфиденциальности ИКТ.

9.4.1. Процедура «Мониторинг соблюдения мер по охране конфиденциальности ИКТ»:

– инициируется наступлением событий, указанных в п. 9.2. настоящего Положения;

– результатом процедуры является подтверждение результативности мер по охране конфиденциальности ИКТ в Обществе либо выявленные факты их нарушения.

9.4.1.1. Мониторинг соблюдения мер по охране конфиденциальности ИКТ осуществляется на всем протяжении действия режима КТ в отношении информации, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам.

9.4.1.2. Мониторинг осуществляется руководителями структурных подразделений ИА и филиалов Общества, работники которых осуществляют обработку ИКТ в рамках своих полномочий.

9.4.1.3. В рамках мониторинга оценивается:

– порядок обращения с документами, содержащим ИКТ;

– достаточность принимаемых мер по охране конфиденциальности ИКТ работниками Общества и их соблюдение;

– порядок заключения соглашений (договоров) о конфиденциальности с Контрагентами и их соблюдение;

– полнота исполнения обязанностей по предоставлению ИКТ государственным органам, органам местного самоуправления.

9.4.1.4. Специалист по безопасности в рамках мониторинга организовывает проведение контрольных мероприятий за соблюдением режима КТ в Обществе.

9.4.1.5. В случаях обработки ИКТ с использованием средств автоматизации (в информационных системах) мониторинг их использования осуществляется с привлечением группы информационных технологий и связи, в том числе с использованием средств контроля утечки конфиденциальной информации (DLP – систем).

9.4.1.6. При выявлении фактов нарушения мер по охране конфиденциальности ИКТ, приведшим (способствующим) к ее утрате (хищения,

разглашения или фальсификации) руководители соответствующих структурных подразделений информируют специалиста по безопасности.

Специалист по безопасности информирует о выявленных нарушениях заместителя Генерального директора по безопасности и по его указанию проводит предварительные проверочные мероприятия, служебные проверки / расследования по выявленным нарушениям.

9.4.1.7. Предварительные проверочные мероприятия, служебные проверки / расследования проводятся в соответствии с требованиями Положения о порядке проведения в АО «ХРМК» служебных проверок / расследований по потенциальным / реализованным рискам экономической, внутренней и информационной безопасности[9].

9.4.1.8. В рамках проведения предварительных проверочных мероприятий, служебных проверок / расследований должны быть:

– установлены обстоятельства разглашения ИКТ или утраты ее материальных носителей, а также способствовавшие этому условия;

– выявлены причины, цели и мотивы разглашения ИКТ;

– определены характер и размер ущерба, причиненного Обществу;

– сформированы предложения по совершенствованию мер по охране конфиденциальности ИКТ в Обществе.

9.4.1.9. Выводы по результатам проведения проверочных мероприятий, служебных проверок / расследований являются основой для комплексного анализа соблюдения мер по охране конфиденциальности ИКТ в Обществе.

9.4.1.10.На основе полученной в результате мониторинга информации специалистом по безопасности формируются выводы о соблюдении в Обществе мер по охране конфиденциальности ИКТ.

9.4.2. Процедура «Оценка актуальности действующих ограничений в отношении ИКТ»:

– инициируется наступлением событий, указанных в п. 9.2 Положения;

– результатом процедуры является окончание срока действия ограничения доступа к ИКТ; наступление событий, позволяющих отменить режим КТ в отношении определенных сведений; утрата коммерческой ценности сведений, ранее отнесенных к ИКТ; получение от ключевых участников сценария предложений о внесении изменений в Перечень ИКТ; подтверждение актуальности действующих ограничений в отношении ИКТ.

9.4.2.1. Оценка актуальности условий действия ограничений в отношении ИКТ проводится в целях обеспечения оперативного реагирования на изменения свойств ИКТ, оказывающих влияние на ее коммерческую ценность.

9.4.2.2. Оценка актуальности условий действия ограничений в отношении ИКТ осуществляется обладателем ИКТ на основе сведений, содержащихся в Перечне ИКТ, либо в соответствии с бизнес-процессами, участниками которых они являются.

---

[9] Приказ по присоединении к Приказу ПАО «РусГидро» от 30.11.2021 № 1095 «Об утверждении Положения о порядке проведения в Группе РусГидро служебных проверок/расследований по потенциальным/реализованным рискам экономической, внутренней и информационной безопасности».

9.4.2.3. На основании оценки принимаются решения о возможности снятия ограничений доступа к документу, ранее содержащему ИКТ, и формируются предложения о внесении изменений в Перечень ИКТ. Кроме того, на основании оценки возможно получение подтверждения актуальности условий действия ограничений в отношении ИКТ.

9.4.3. Процедура «Комплексный анализ соблюдения мер по охране конфиденциальности ИКТ»:

– инициируется выявлением фактов нарушения мер по охране конфиденциальности ИКТ;

– результатом процедуры являются управленческие решения о необходимости корректировки мер по охране конфиденциальности ИКТ в Обществе и / или необходимости принятия мер воздействия к лицам, допустившим нарушения данных мер.

9.4.3.1. Целью проведения комплексного анализа является определение степени соответствия ЛНД (А) Общества, регулирующих отношения, связанные с установлением, изменением и прекращением режима КТ в Обществе, требованиям законодательства Российской Федерации, а также достаточности принимаемых мер по охране конфиденциальности ИКТ.

9.4.3.2. Комплексный анализ проводится специалистом по безопасности.

9.4.3.3. В рамках комплексного анализа проводится:

– анализ действующих нормативных правовых актов Российской Федерации, регулирующих отношения, связанные с установлением, изменением и прекращением режима КТ в отношении информации, которая имеет действительную или потенциальную ценность в силу неизвестности ее третьим лицам;

– анализ имевших место фактов (предпосылок) нарушения мер по охране конфиденциальности ИКТ;

– анализ соответствия применяемых для обеспечения охраны конфиденциальности ИКТ средств защиты информации требованиям политики по информационной безопасности Общества.

9.4.3.4. Результаты комплексного анализа обобщаются специалистом по безопасности для их последующего направления для рассмотрения Комиссией.

9.4.3.5. Комиссия по итогам рассмотрения результатов комплексного анализа формирует предложения о необходимости корректировки мер по охране конфиденциальности ИКТ.

9.4.3.6. На основе принятого Комиссией решения специалист по безопасности организовывает разработку ЛНД (А) Общества, целью которого является уточнение мер по охране конфиденциальности ИКТ в Обществе.

9.4.3.7. В случае выявления вины работника Общества в нарушении мер по охране конфиденциальности ИКТ, повлекших причинение ущерба вследствие разглашения ИКТ или ее неправомерного использования, работник может быть привлечен к дисциплинарной, материальной, гражданско-правовой, административной и уголовной ответственности в соответствии с законодательством Российской Федерации.

ГЛАВА 10. ЭТАП «СОВЕРШЕНСТВОВАНИЕ МЕР ПО ОХРАНЕ КОНФИДЕНЦИАЛЬНОСТИ ИКТ»

10.1.Целью Этапа является предупреждение нарушений режима КТ в Обществе, устранение (недопущение повторения) выявленных в ходе мониторинга нарушений мер по охране конфиденциальности ИКТ и причин их возникновения, реализация решений по совершенствованию мер по охране конфиденциальности ИКТ.

10.2.Входящими данными (инициирующими событиями) Этапа являются:

– решения о необходимости корректировки мер по охране конфиденциальности ИКТ;

– информация об окончании срока действия ограничения доступа к ИКТ;

– информация о наступлении событий, позволяющих отменить режим КТ в отношении определенных сведений;

– информация об утрате коммерческой ценности сведений, ранее отнесенных к ИКТ;

– предложения от ключевых участников сценария о внесении изменений в Перечень ИКТ.

10.3.Результатами Этапа являются:

– сформированный (актуализированный) Перечень ИКТ, утвержденный ЛНД (А) Общества;

– принятые ЛНД (А) Общества, определяющие (уточняющие) меры по охране конфиденциальности ИКТ в Обществе;

– снятие ограничений доступа к документу, ранее содержащему ИКТ.

10.4.Этап состоит из следующих процедур:

– определение (уточнение) Перечня ИКТ Общества;

– совершенствование мер по охране конфиденциальности ИКТ;

– снятие ограничений доступа к информации, в отношении которой установлен режим КТ.

10.4.1. Процедура «Определение (уточнение) Перечня ИКТ Общества»:

– инициируется поступлением предложений о внесении изменений в Перечень ИКТ;

– результатом процедуры является сформированный (актуализированный) Перечень ИКТ, утвержденный ЛНД (А) Общества.

10.4.1.1.В целях принятия коллегиальных решений по вопросам определения (актуализации) Перечня ИКТ, соблюдения режима КТ, а также установления, изменения либо прекращения режима КТ в отношении информации, обладателем которой является Общество, приказом Общества создана Комиссия.

10.4.1.2.На основании решения о необходимости установления (уточнения) режима КТ в отношении информации, которая имеет действительную или потенциальную коммерческую ценность для Общества, специалист по безопасности инициирует сбор и обобщение предложений по формированию (актуализации) Перечня ИКТ.

10.4.1.3.Обобщенные предложения по формированию (актуализации) Перечня ИКТ выносятся специалистом по безопасности на рассмотрение Комиссией.

10.4.1.4.При рассмотрении Перечня ИКТ Комиссией устанавливаются сроки действия ограничений на доступ к содержащейся в нем информации или условия прекращения таких ограничений.

10.4.1.5.После одобрения Комиссией поступивших предложений специалист по безопасности формирует проект Перечня ИКТ, который представляется на утверждение Генеральному директору Общества.

10.4.1.6.Режим КТ не может быть установлен в отношении сведений:

– содержащихся в учредительных документах Общества, документах, подтверждающих факт внесения записей об Обществе в соответствующие государственные реестры;

– содержащихся в документах, дающих право на осуществление определенных видов предпринимательской деятельности, в том числе в лицензиях;

– о состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение безопасного функционирования производственных объектов Общества, безопасности каждого гражданина и безопасности населения в целом;

– о численности, о составе работников Общества, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости и о наличии свободных рабочих мест;

– о задолженности Общества по выплате заработной платы и по иным социальным выплатам;

– о нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений;

– о перечне лиц, имеющих право действовать без доверенности от имени Общества;

– о проспектах ценных бумаг, отчетах эмитента и иных документах, содержащих информацию, подлежащую опубликованию или раскрытию иным способом в соответствии с Федеральным законом от 22.04.1996 № 39-ФЗ «О рынке ценных бумаг», Положением Банка России от 27.03.2020 № 714-П «О раскрытии информации эмитентами эмиссионных ценных бумаг», а также в соответствии с другими применимыми требованиями регуляторов рынка ценных бумаг и торговых площадок;

– об аффилированных лицах Общества;

– об информации, защищенной патентным правом;

– о состоянии окружающей среды;

– иных сведений, обязательность раскрытия или опубликования которых, а также недопустимость ограничения доступа, к которым установлена федеральными законами.

10.4.1.7.При определении возможности, необходимости и целесообразности отнесения тех или иных сведений, указанных в Перечне ИКТ, к КТ, обладатель ИКТ исходит из оценки содержания конкретной информации и особенностей ее обращения, учитывая, в частности, следующие факторы и условия:

– коммерческую ценность информации и наличие к ней потенциального интереса третьих лиц;

– важность сведений с точки зрения получения прибыли в условиях конкуренции с другими субъектами рынка;

– возможность использования сведений конкурентами в случае их получения, в том числе в формах недобросовестной конкуренции, а также возможные последствия такого использования для Общества;

– возможность использования информации в бизнес-процессах в условиях ограничения доступа к ней и введения режимных мер;

– наличие других факторов и условий, которые могут представлять угрозу экономическим интересам Общества;

– оценка последствий обязательного раскрытия ИКТ акционерам.

10.4.2. Процедура «Совершенствование мер по охране конфиденциальности ИКТ»:

– инициируется решением о необходимости корректировки мер по охране конфиденциальности ИКТ в Обществе;

– результатом процедуры являются принятые ЛНД (А) Общества, определяющие (уточняющие) меры по охране конфиденциальности ИКТ.

10.4.2.1. Меры по охране конфиденциальности ИКТ должны обеспечивать выполнение следующих требований:

– возможность ознакомления с документами, содержащими ИКТ, работниками, в рамках предоставленных полномочий;

– документальное фиксирование всех фактов передачи документов, содержащих ИКТ, между работниками Общества, передачи их Контрагентам и предоставления государственным органам и органам местного самоуправления;

– обеспечение ответственности за сохранность документов, содержащих ИКТ;

– обеспечение возможности установить место нахождения документов, содержащих ИКТ, и лиц, осуществляющих их хранение, для любого промежутка времени;

– возможность изготовления копий документов, содержащих ИКТ, только при наличии письменного распоряжения соответствующего руководителя структурного подразделения;

– хранение документов, содержащих ИКТ только в местах, исключающих несанкционированный доступ к ним лиц, не имеющих на то прав;

– утверждение перечня отобранных к уничтожению документов, содержащих ИКТ, и документальное оформление актом уничтожения таких документов комиссиями, назначенными ЛНД (А) Общества.

– Уничтожение документов, содержащих ИКТ, осуществляется способом, исключающим или существенно затрудняющим их восстановление способом с

учетом зависимости стоимости затрат на их восстановление от размера возможного потенциального ущерба.

– Обработка ИКТ с использованием средств автоматизации (в информационных системах (далее – ИС)) должна предусматривать реализацию комплекса организационных, программных, технических мер, направленных на предотвращение несанкционированного доступа к хранящейся и обрабатываемой информации, защиту ее от модификации и уничтожения.

10.4.2.2. С учетом принципов обеспечения информационной безопасности ИС, обрабатывающих ИКТ, в ее состав должны быть включены следующие средства:

– средства идентификации и аутентификации пользователей и элементов автоматизированной системы (серверов, рабочих станций, сетевого оборудования, процессов, программ и т.п.);

– средства авторизации (предоставления прав пользователям ИС) и разграничения доступа к данным;

– средства защиты от программно-математических воздействий, в том числе вредоносного кода (антивирусная защита);

– средства криптографической защиты информации, передаваемой по открытым каналам связи, в том числе сети интернет (защищенный удаленный доступ);

– средства регистрации обращения и контроля за использованием ИКТ в ИС.

10.4.2.3. Работа с документами ИКТ в корпоративной системе документооборота допускается с обязательным установлением персонифицированного доступа работникам, которым данные документы адресованы.

10.4.2.4. При обработке ИКТ в ИС Общества должно обеспечиваться выполнение следующих общих требований:

– учет и документальная фиксация всех информационных ресурсов, содержащих ИКТ, назначение лица, ответственного за каждый такой ресурс;

– предоставление доступа работникам только к тем информационным ресурсам, которые необходимы им для выполнения трудовых обязанностей, с минимальными правами, обеспечивающими выполнение этих обязанностей;

– учет в соответствии с установленным порядком всех бумажных носителей (документов), содержащих ИКТ, выведенных на печать из ИС (с применением DLP – систем);

– запрет на передачу по каналам связи, не защищенным средствами криптографической защиты, принятыми в эксплуатацию установленным порядком, в том числе, с использованием незащищенной электронной почты.

10.4.2.5. Уничтожение ИКТ, обрабатываемой с использованием средств автоматизации (в ИС), осуществляется в соответствии с руководством пользователя соответствующей ИС.

10.4.2.6. В случаях, требующих передачи ИКТ Общества принимающей стороне в рамках заключенных договоров (соглашений о конфиденциальности)

для ее последующей обработки в ИС принимающей стороны, такая передача должна осуществляться с соблюдением требований по защите конфиденциальности ИКТ. При этом, принимающая сторона должна представить передающей стороне – Обществу, документы, подтверждающие соответствие ИС, в которой предполагается обработка ИКТ, требованиям защиты информации и информационной безопасности (в форме Аттестата соответствия).

10.4.3. Процедура «Снятие ограничений доступа к информации, в отношении которой установлен режим КТ»:

– инициируется окончанием срока действия ограничения доступа к ИКТ; наступлением событий, позволяющих отменить режим КТ в отношении определенных сведений; утратой коммерческой ценности сведений, ранее отнесенных к ИКТ;

– результатом процедуры является снятие ограничений доступа к документу, ранее содержащему ИКТ.

10.4.3.1.Срок действия ограничений доступа к ИКТ определяется Перечнем ИКТ как конкретный срок или «до заключения контракта / договора», или «до раскрытия в установленном порядке решения органа управления», или «до публикации в открытом доступе» или «бессрочно». Требование об обеспечении охраны конфиденциальности ИКТ устанавливается также в соглашениях о конфиденциальности в течение срока их действия / определенного периода после прекращения их действия.

10.4.3.2.Прекращение действия режима КТ в отношении сведений, ранее отнесенных к КТ, до истечения срока действия режима КТ / наступления события, прекращающего режим КТ или при установлении бессрочного действия, осуществляется на основании решения обладателя ИКТ, в компетенции которого находилась такая ИКТ.

10.4.3.3.При принятии решения о снятии ограничений доступа к документам, содержащих ИКТ обладатель ИКТ учитывает основания утраты коммерческой ценности данной информации и / или ее конфиденциальности и удостоверяется в том, что снятие с информации грифа «Коммерческая тайна» не наносит ущерба Обществу.

10.4.3.4.В случае принятия решения о раскрытии (опубликовании) информации, потери ее актуальности и / или истечения срока установления ограничений доступа к ней, в отношении таких сведений прекращается режим КТ. С документа, содержащего такие сведения, удаляется гриф «Коммерческая тайна».

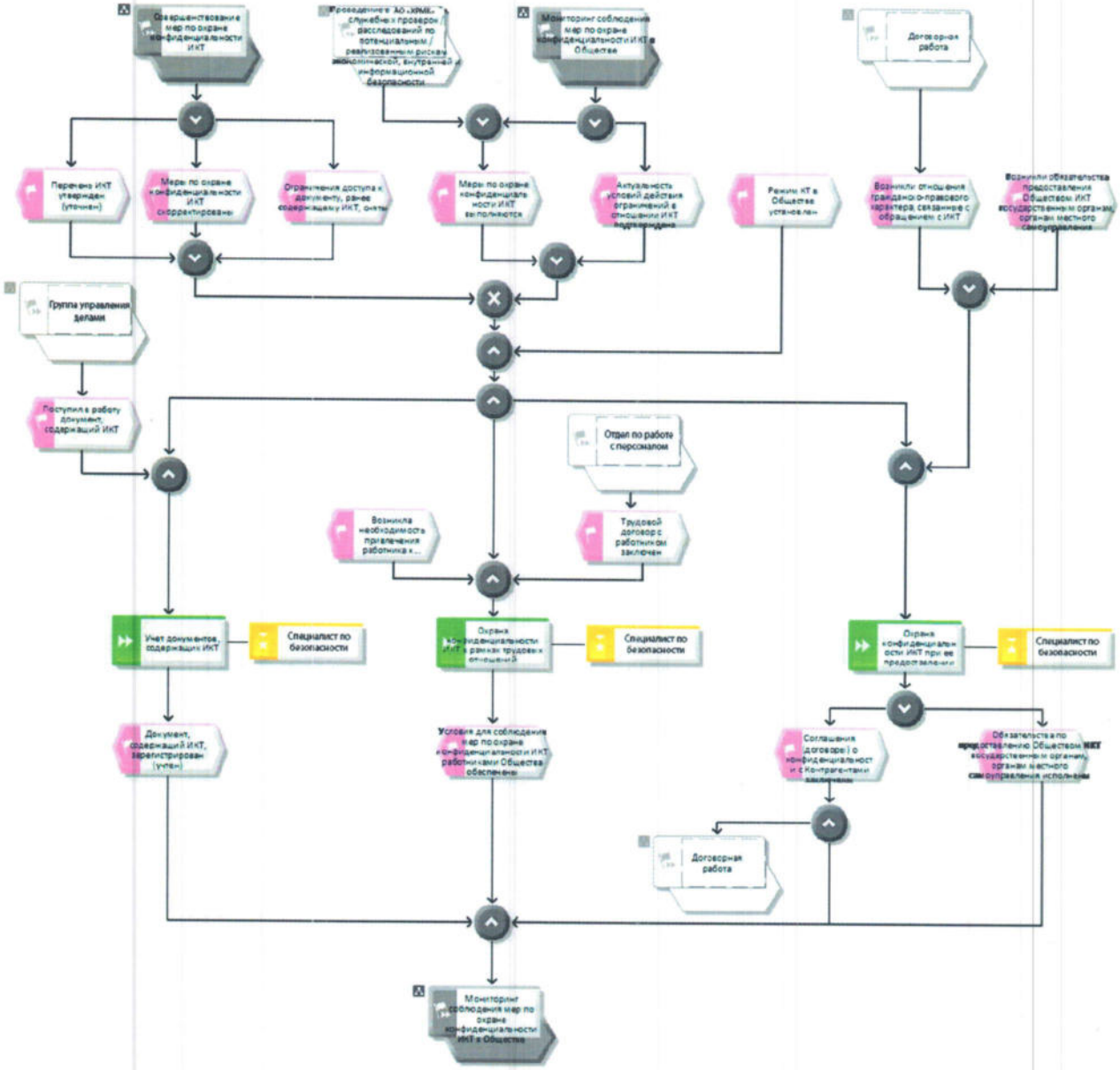
С отчуждаемых материальных носителей, содержащих в электронном виде такие сведения, удаляется гриф «Коммерческая тайна», а сами сведения удаляются с машинного носителя информации.

10.4.3.5.Факт несанкционированного получения ИКТ лицами, не имеющими на то законного права, в том числе в устной форме, не может служить безусловным основанием для прекращения отнесения информации к КТ.

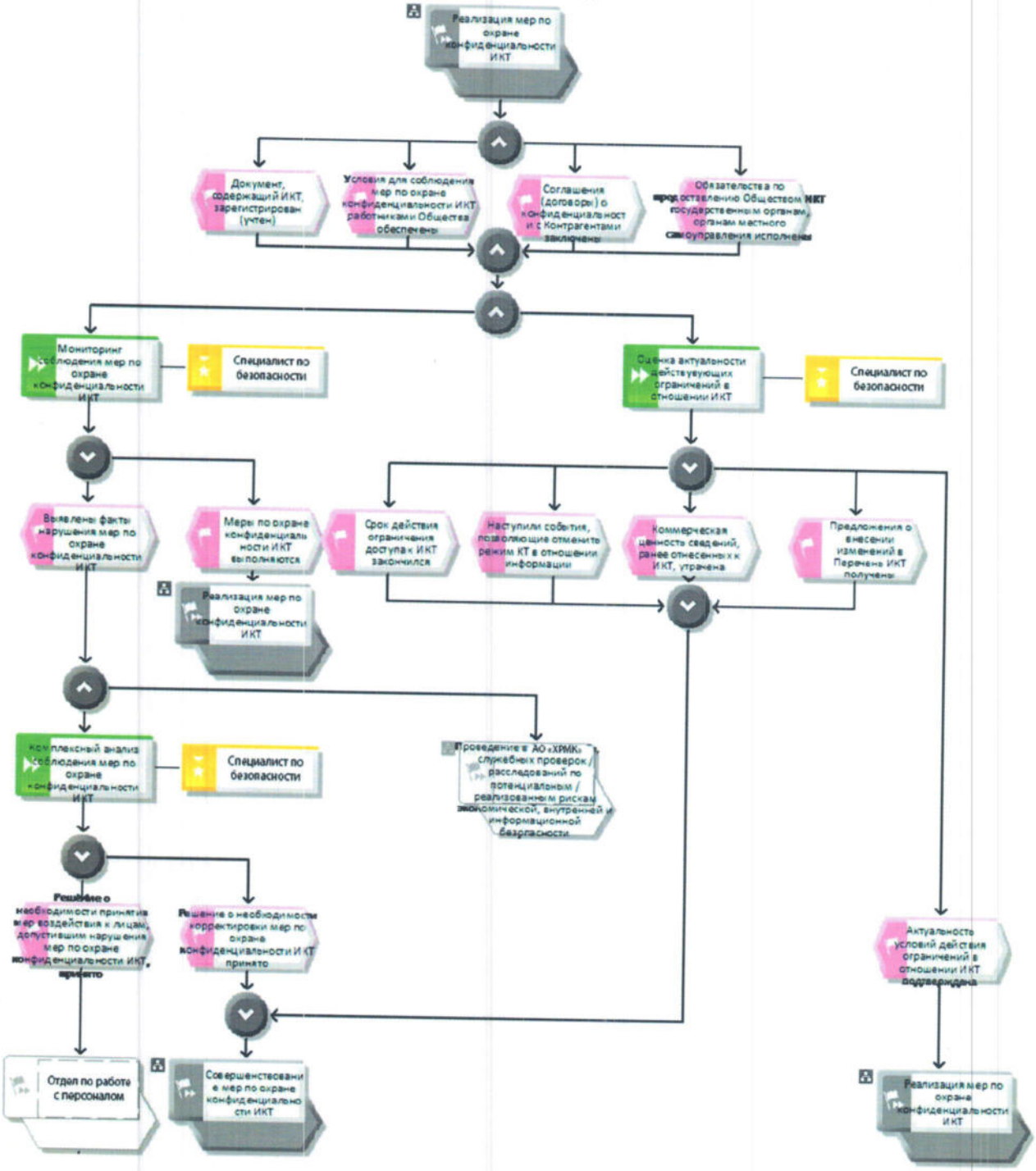
Решение о прекращении отнесения информации к КТ принимается с учетом оценки возможности сохранения конфиденциальности таких сведений, в том числе лицом, получившим такие сведения в результате ошибки или случайности.

Приложение 1 к Положению

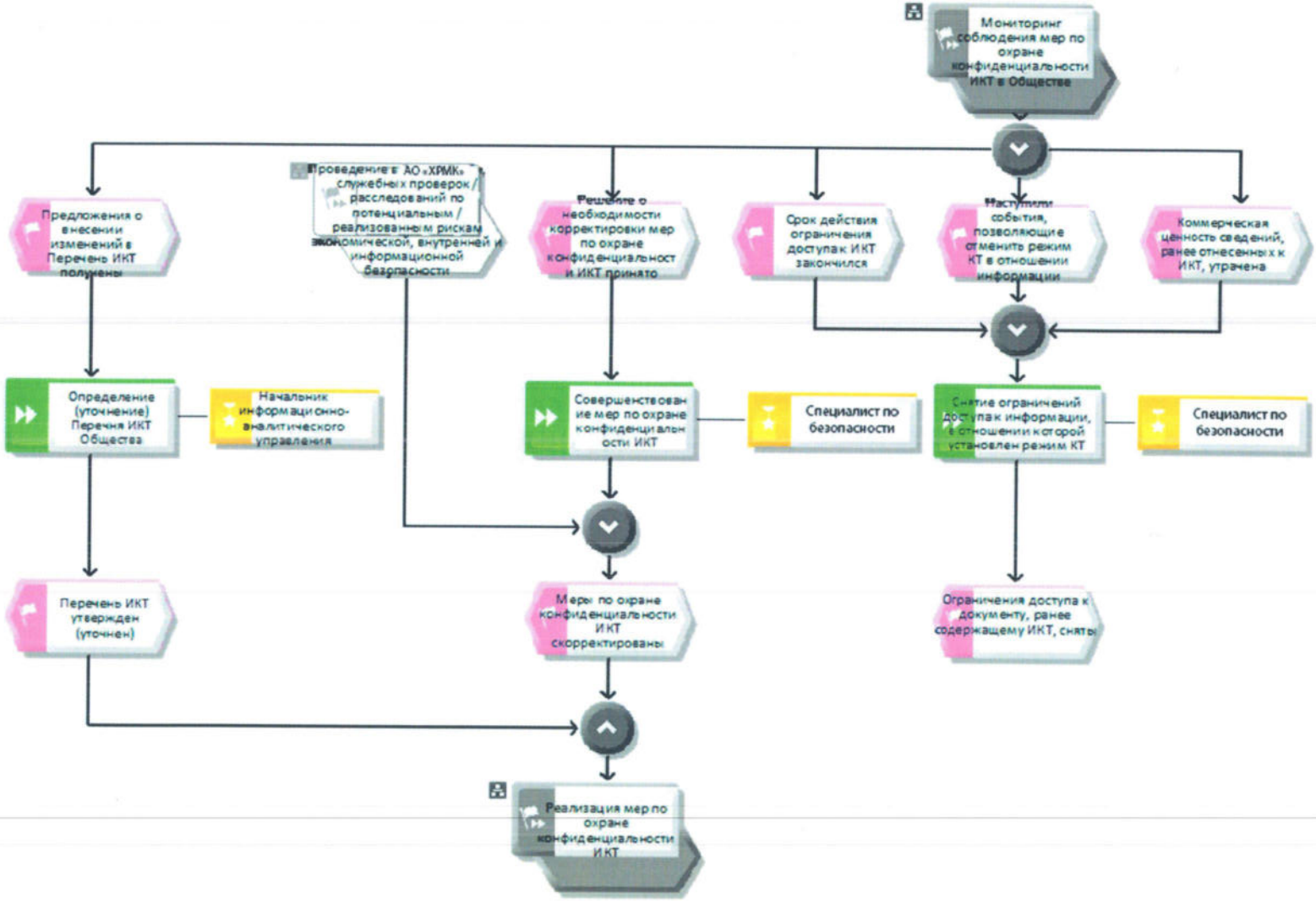
МОДЕЛЬ 3-ГО УРОВНЯ ДЕКОМПОЗИЦИИ ЭТАПА «РЕАЛИЗЦИЯ МЕР ПО ОХРАНЕ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ, СОСТАВЛЯЮЩЕЙ КОММЕРЧЕСКУЮ ТАЙНУ» В ГРАНИЦАХ СЦЕНАРИЯ «ОХРАНА КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ, СОСТАВЛЯЮЩЕЙ КОММЕРЧЕСКУЮ ТАЙНУ» ПРОЦЕССА «УПРАВЛЕНИЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТЬЮ» (ЛОГИКА ПРОЦЕДУР)»



МОДЕЛЬ 3-ГО УРОВНЯ ДЕКОМПОЗИЦИИ ЭТАПА «МОНИТОРИНГ СОБЛЮДЕНИЯ МЕР ПО ОХРАНЕ КОНФИДЕНЦИАЛЬНОСТИ ИКТ В ОБЩЕСТВЕ» В ГРАНИЦАХ СЦЕНАРИЯ «ОХРАНА КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ, СОСТАВЛЯЮЩЕЙ КОММЕРЧЕСКУЮ ТАЙНУ» ПРОЦЕССА «УПРАВЛЕНИЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТЬЮ» (ЛОГИКА ПРОЦЕДУР)»



МОДЕЛЬ 3-ГО УРОВНЯ ДЕКОМПОЗИЦИИ ЭТАПА «СОВЕРШЕНСТВОВАНИЕ МЕР ПО ОХРАНЕ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ, СОСТАВЛЯЮЩЕЙ КОММЕРЧЕСКУЮ ТАЙНУ» В ГРАНИЦАХ СЦЕНАРИЯ «ОХРАНА КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ, СОСТАВЛЯЮЩЕЙ КОММЕРЧЕСКУЮ ТАЙНУ» ПРОЦЕССА «УПРАВЛЕНИЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТЬЮ» (ЛОГИКА ПРОЦЕДУР)»



Приложение 2 к Положению

Форма грифа «Коммерческая тайна»

Коммерческая тайна
Экз. № _____
Акционерное общество
«Хабаровская ремонтно-монтажная
компания»
(АО «ХРМК»)
680033, Хабаровский край, г. Хабаровск,
ул. Адмиральская, д. 10

Приложение 3 к Положению

Типовая форма Журнала регистрации и учета входящих документов/носителей ИКТ (вариант)*

№ п/п	Входящий регистрационный номер	Дата регистрации (поступления)	Адресант (от кого поступил)	Исх. номер и дата документа	Тип носителя	Заголовок или краткое содержание	Количество листов, приложений	Номер экземпляра	Адресат (получатель)	Исполнитель по резолюции (структурное подразделение, ФИО)	Дата получения документа исполнителем	Подпись исполнителя о получении документа	Расписка в обратном приеме документа от исполнителя	Примечание
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

* Форма Журнала может быть скорректирована под конкретные задачи

Приложение 4 к Положению

Типовая форма Журнала регистрации и учета исходящих документов/носителей ИКТ (вариант)*

№ п/п	Исходящий регистрационный номер	Дата регистрации	Тип носителя	Заголовок или краткое содержание	Количество листов, количество приложений	Количество экземпляров	Адресат (получатель)	Исполнитель документа (структурное подразделение, ФИО)	ФИО получившего документ от исполнителя	Подпись получившего документ от исполнителя	Примечание
1	2	3	4	5	6	7	8	9	10	11	12

* Форма Журнала может быть скорректирована под конкретные задачи

Приложение 5 к Положению

Типовая форма Журнала регистрации и учета внутренних документов/носителей ИКТ (вариант)*

№ п/п	Регистрационный номер	Дата регистрации	Тип носителя	Заголовок или краткое содержание	Количество листов, количество приложений	Количество экземпляров	Разработчик (исполнитель) документа (структурное подразделение, ФИО)	Подпись разработчика (исполнителя) документа	ФИО получившего документ	Подпись получившего документ	Примечание
1	2	3	4	5	6	7	8	9	10	11	12

* Форма Журнала может быть скорректирована под конкретные задачи

Приложение 6 к Положению

Список работников _____, которым предоставлен
(наименование структурного подразделения)
доступ к информации, содержащей коммерческую тайну АО «ХРМК»

№ п/п	Наименование должности	Фамилия, Имя, Отчество	Номер пункта Перечня ИКТ	Дата, с которой предоставлен доступ к ИКТ	Дата ознакомления с ЛНД (А) Общества	Примечание