ПУЛЬС
HR-ПЛАТФОРМА

УТВЕРЖДЕНО
Приказом №01-КБ от 28.03.2024 г.

ПОЛОЖЕНИЕ
о защите персональных данных

г. Москва,
2024

ООО «Пульс»
pulse-hcm.ru
ОГРН: 1247700255604
ИНН/КПП: 9709108748/770901001

Юридический адрес:
109544, г. Москва, вн.тер.
г. муниципальный округ Таганский,
ул. Большая Андроньевская, д. 6

Фактический адрес:
125284, г. Москва,
Ленинградский пр-кт, д. 35, стр. 1

ПУЛЬС
HR-ПЛАТФОРМА

Оглавление

ПУЛЬС
HR-ПЛАТФОРМА

1. Общие положения

1.1. Настоящее Положение о защите персональных данных Общества с ограниченной ответственностью «Пульс» (далее – Положение) разработано в целях реализации (выполнения) положений Федерального закона Российской Федерации от 27.07.2006 г. №152-ФЗ «О персональных данных» (далее – Закон № 152-ФЗ) и нормативных правовых актов Российской Федерации, которыми установлены требования к обеспечению безопасности ПДн.

1.2. Настоящее Положение определяет требования к правовым, организационным и техническим мерам, реализуемым системой защиты ПДн (далее – СЗПДн) Общества с ограниченной ответственностью «Пульс» (далее – Общество).

1.3. Целями создания СЗПДн в Обществе являются:

– соблюдение требований законодательства и нормативных актов в области защиты ПДн;

– обеспечение защиты конституционных прав и свобод человека и гражданина при обработке ПДн, в том числе с использованием информационных технологий;

– защита деловой репутации Общества;

– снижение до минимального уровня возможности утечки и иных неправомерных действий с ПДн, а также предотвращение нарушений установленных требований законодательства Российской Федерации в области защите ПДн;

– обеспечение непрерывности деятельности Общества, связанной с осуществлением обработки ПДн.

1.4. Требования настоящего Положения обязательны для выполнения всеми работниками Общества при осуществлении обработки ПДн.

1.5. Настоящее Положение доводится до всех лиц, участвующих в обеспечении безопасности ПДн в Обществе, под родпись.

2. Термины и определения

Термины и определения приведены в Приложении 1 Политики обработки персональных данных.

3. Нормативные ссылки

3.1. Перечень нормативных правовых актов Российской Федерации

– Федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных».

– Федеральный закон Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

– Указ Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера».

– Указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».

– Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите ПДн при их обработке в информационных системах ПДн».

– Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки ПДн, осуществляемой без использования средств автоматизации».

– Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в информационных системах ПДн».

– Методика оценки угроз безопасности информации, утверждена ФСТЭК России 05.02.2021.

– Приказ ФСТЭК России от 27.10.2022 № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам ПДн в случае нарушения Федерального закона «О ПДн».

– Приказ ФСТЭК России от 28.10.2022 № 178 «Об утверждении Требований к подтверждению уничтожения ПДн».

– Методические рекомендации по обеспечению с помощью криптосредств безопасности ПДн при их обработке в информационных системах ПДн с использованием средств автоматизации, утвержденные руководством 8 Центра ФСБ России 21.02.2008 № 149/54-144.

– Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности ПДн при их обработке в информационных системах ПДн, утвержденные руководством 8 Центра ФСБ России 21.02.2008 № 149/6/6-622.

3.2. Перечень внутренних нормативных документов, регламентирующих обработку и защиту ПДн в Обществе:

– Политика обработки персональных данных;
– Политика обработки cookie-файлов;
– Положение об обработке персональных данных;
– Положение о защите персональных данных;
– Регламент взаимодействия с третьими лицами
– Регламент проведения внутреннего контроля ПДн
– Порядок работы с обращениями субъектов ПДн
– Порядок проведения регулярного мониторинга изменений законодательства в области ПДн;
– Методика оценки вреда.

4. Организационная структура СЗПДн

4.1. Руководство деятельностью по защите ПДн в Обществе осуществляет Директор по кибербезопасности.

4.2. Функции по обеспечению безопасности ПДн возлагаются приказом Генерального директора на должностное лицо.

4.3. Лицо, ответственное за обеспечение безопасности ПДн обеспечивает выполнение следующих функций:

– разработка и актуализация внутренних нормативных документов по защите ПДн (политики, стандарты, положения, планы, перечни, инструкции или иные виды документов, разрабатываемые для регламентации процедур защиты ПДн в Обществе);

– планирование и контроль выполнения мероприятий по защите ПДн для ИСПДн;

– оценка угроз безопасности ПДн в информационной инфраструктуре Общества;

– разработка и совершенствование организационных и технических мер, реализуемых СЗПДн;

– проведение внутренних аудитов соответствия СЗПДн требованиям законодательства о защите ПДн, внутренним нормативным документам по защите ПДн;

– обнаружение, предупреждение и ликвидация последствий компьютерных атак и реагирование на компьютерные инциденты.

4.4. Обязанности по обеспечению безопасности ПДн, возлагаемые на работников структурных подразделений Общества, в которых осуществляется обработка ПДн, определяются в их должностных инструкциях в соответствии с Приложением 10 к Положению.

5. Мероприятия по созданию СЗПДн

5.1. Создание СЗПДн включает в себя следующие мероприятия:

– определение объектов защиты по результатам проведения инвентаризации информационных ресурсов Общества;

– определение актуальных угроз безопасности ПДн;

– определение требуемого уровня защищенности ПДн при их обработке в ИСПДн Общества;

– разработка проектных решений по созданию СЗПДн с учетом результатов моделирования угроз безопасности ПДн и уровня защищенности ПДн;

– ввод в действие СЗПДн, включающий опытную эксплуатацию и приемо-сдаточные испытания, утверждение внутренних нормативных документов, регламентирующих обработку и защиту ПДн;

– обучение работников правилам и процедурам обеспечения безопасности ПДн;

– оценку эффективности принимаемых мер по обеспечению безопасности ПДн.

6. Определение объектов защиты

6.1. Инвентаризация информационных ресурсов Общества проводится с целью сбора и анализа информации об объектах защиты СЗПДн, к которым относятся:

– компоненты информационной инфраструктуры ИСПДн (сетевое оборудование, серверное оборудование, средства резервного копирования, рабочие станции пользователей и администраторов,);

– компоненты виртуальной инфраструктуры ИСПДн (сетевое оборудование, серверное оборудование, оборудование хранения данных, виртуальные машины, средства резервного копирования компонентов среды виртуализации и средства защиты информации, используемые в рамках виртуальных машин и виртуальной инфраструктуры);

– программные средства информационной и виртуальной инфраструктуры ИСПДн (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение);

– средства защиты информации;

– информация (данные), обрабатываемые в ИСПДн, в том числе категории и состав обрабатываемых ПДн, принадлежность ПДн субъектам ПДн (категории субъектов ПДн), количество субъектов ПДн;

– служебные данные компонентов информационной и виртуальной инфраструктуры (настройки и иные служебные данные);

– машинные носители информации, содержащие защищаемую информацию, аутентификационную информацию;

– сведения о взаимодействии ИСПДн с внешними информационными системами и информационно-телекоммуникационными сетями;

– бумажные носители (документы), содержащие ПДн и хранилища документов;

– помещения, в которых размещаются компоненты информационной инфраструктуры Общества (серверные, помещения подразделений);

– критичные для обеспечения деятельности Общества процессы, реализуемые ИСПДн;

– пользователи и администраторы ИСПДн;

– провайдеры (поставщики услуг).

6.2. По результатам проведения инвентаризации формируется и / или актуализируется описание (схемы) текущей архитектуры информационных систем Общества, а также перечень ИСПДн.

6.3. Перечень информационных систем персональных данных приведен в Приложении 3 к настоящему Положению.

6.4. Перечень ИСПДн утверждается Генеральным директором Общества.

6.5. Информация об объектах защиты используется в ходе проведения оценки угроз безопасности ПДн.

7. Определение актуальных угроз безопасности персональных данных

7.1. Эффективность принимаемых мер защиты ИСПДн Общества зависит от качества определения угроз безопасности информации для конкретной ИСПДн в конкретных условиях ее функционирования.

7.2. Для определения угроз безопасности информации и разработки модели угроз безопасности или ее уточнении должны применяться методические документы ФСТЭК России, ФСБ России.

7.3. Угрозы безопасности информации определяются по результатам оценки возможностей (потенциала) внешних и внутренних нарушителей, анализа возможных уязвимостей информационной системы, возможных способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).

7.4. При определении угроз безопасности информации в ИСПДн, функционирование которой осуществляется или предполагается обеспечить на базе информационно-телекоммуникационной инфраструктуры центра обработки данных, должны учитываться угрозы безопасности информации, актуальные для информационно-телекоммуникационной инфраструктуры центра обработки данных.

7.5. Модель угроз безопасности информации должна содержать описание информационной системы и ее структурно-функциональных характеристик, а также описание угроз безопасности информации, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей информационной системы, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации.

8. Определение уровня защищенности персональных данных

8.1. Под уровнем защищенности ПДн понимается комплексный показатель, характеризующий требования к защите ПДн, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности ПДн при их обработке в ИСПДн.

8.2. Определение уровня защищенности ПДн проводится Комиссией по обеспечению безопасности персональных данных в соответствии с Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите ПДн при их обработке в информационных системах ПДн».

8.3. Для каждой ИСПДн оформлен Акт определения уровня защищенности персональных данных по форме, приведенной в Приложении 6.

8.4. Пересмотр уровней защищенности ПДн при их обработке в ИСПДн Общества должен проводится Комиссией по обеспечению безопасности ПДн ежегодно.

8.5. Определение уровня защищенности ПДн проводится Обществом с целью формирования требований по обеспечению безопасности ПДн при их обработке в ИСПДн в соответствии с Приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в информационных системах ПДн», реализуемых СЗПДн Общества.

9. Разработка, проектирование и внедрение СЗПДн

9.1. Разработка проектных решений по созданию (модернизации) СЗПДн осуществляется на основе:

– сведений о текущей архитектуре информационных систем Общества, используемых мерах и средствах защиты информации в Обществе;

– требований к мерам обеспечения защиты ПДн, установленным Приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в информационных системах ПДн» для соответствующего уровня защищенности ПДн;

– результатов моделирования угроз безопасности ПДн и возможных последствий реализации этих угроз.

9.2. В состав создаваемой СЗПДн, обеспечивающей необходимый уровень защищенности ПДн, должны входить следующие подсистемы, обеспечивающие необходимый уровень защищенности ПДн:

– управление доступом;

– защита машинных носителей информации, на которых хранятся и / или обрабатываются ПДн (далее - машинные носители ПДн);

– регистрация событий безопасности;

– антивирусная защита;

– обнаружение (предотвращение) вторжений;

– контроль (анализ) защищенности ПДн;

– обеспечение целостности информационной системы и ПДн;

– обеспечение доступности ПДн;

– защита среды виртуализации;

– защита технических средств;

– защита ИСПДн, ее средств, систем связи и передачи данных;

– выявление инцидентов, которые могут привести к сбоям или нарушению функционирования ИСПДн и (или) к возникновению угроз безопасности ПДн (далее - инциденты), и реагирование на них;

– управление конфигурацией информационной системы и системы защиты ПДн.

9.3. Проектные решений по созданию (модернизации) СЗПДн должны содержать:

– обоснование структуры создаваемой (модернизируемой) СЗПДн и / или ее отдельных компонентов (подсистем);

– содержание организационных и технических мер по обеспечению безопасности ПДн, подлежащих реализации в ИСПДн в рамках создаваемой (модернизируемой) СЗПДн.

9.4. При разработке проектных решений по созданию (модернизации) СЗПДн в соответствии с ГОСТ 34.201–2020 «Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Виды, комплектность и обозначение документов» формируется документация в объеме,

необходимом для обеспечения выполнения работ по внедрению организационных и технических мер создаваемой СЗПДн, проведения приемо-сдаточных испытаний и эксплуатации СЗПДн в соответствии с принятыми проектными решениями.

9.5. Внедрение СЗПДн включает:

– установку и настройку СЗИ;
– разработку внутренних нормативных документов, регламентирующих порядок обеспечения безопасности ПДн;
– внедрение организационных мер, повышающих эффективность применения СЗИ;
– предварительные испытания системы СЗПДн;
– опытную эксплуатацию и доработку СЗПДн (при необходимости);
– приемо-сдаточные испытания системы СЗПДн;
– проведение оценки эффективности реализованных в рамках СЗПДн мер по обеспечению безопасности ПДн.

9.6. Для разработки, проектирования и внедрения СЗПДн Обществом могут привлекаться на договорной основе юридическое лицо или индивидуальный предприниматель, имеющие лицензию на деятельность по технической защите конфиденциальной информации.

10. Управление доступом

10.1. Доступ к ПДн имеют работники Общества, которые обязаны осуществлять их обработку в связи с исполнением своих должностных обязанностей.

10.2. Перечень структурных подразделений и должностей работников Общества, допущенных к работе с ПДн в ИСПДн и Перечень структурных подразделений и должностей работников Общества, допущенных к работе с ПДн на материальных носителях ПДн (далее – Материальный носитель), приведены в Приложении 5 и Приложении 6.

10.3. Ответственным за разработку и поддержание актуальности перечней структурных подразделений и должностей работников Общества, допущенных к работе с ПДн, является Директор по кибербезопасности.

10.4. Процедура предоставления доступа работника Общества к ПДн предусматривает:

– ознакомление работника под подпись с Политикой Общества в отношении обработки ПДн, настоящим Положением, другими внутренними документами по вопросам обработки и защиты ПДн, а также с требованиями законодательства Российской Федерации в области обработки и защиты ПДн;
– информирование работника о категориях обрабатываемых ПДн, об особенностях и правилах осуществления обработки ПДн в соответствии с требованиями Положения об обработке персональных данных;
– фиксацию в письменной форме обязательства работника о неразглашении конфиденциальной информации (Приложение 7);
– проведение инструктажа и регистрацию HRBP факта проведения инструктажа в соответствии с Приложением 8.

10.5. Инструктаж проводится с целью доведения до работника содержания основных требований Общества в области защиты ПДн и заключается в разъяснении положений, правил, требований, задач, возможных последствий неправомерных действий, ответственности и т.д.

10.6. Работники Общества должны проходить инструктаж по следующим тематикам:

– правила использования персонального компьютера, мобильных устройств, внешних носителей информации;
– корпоративная электронная почта и сервисы «мгновенных» сообщений;
– использование ресурсов сети Интернет;
– правила аутентификации и парольной защиты.

10.7. Доступ к ИСПДн предоставляется по заявке через систему ИТ-услуга с последующим согласованием у непосредственного руководителя.

10.8. Разграничение прав доступа к ИСПДн осуществляется на уровне ролей в соответствии с Матрицей доступа к ИСПДн (Приложение 2).

10.9. Роли, необходимые для выполнения работником своих должностных обязанностей определяются Владельцем ИСПДн и согласуются руководителем подразделения работника.

10.10. Для изменения уровня доступа в ИСПДн, работник должен отправить специальную заявку в системе ИТ-услуга с последующим согласованием руководителем подразделения работника.

10.11. Допуск работников к обработке ПДн до прохождения процедуры предоставления доступа запрещается.

10.12. В ИСПДн Общества выполняется протоколирование следующих событий безопасности:

– все изменения с учетной записью пользователя (изменение пароля, полномочий и т.д.);
– дата и время работы пользователя в информационной системе;
– создание, изменение, удаление данных в информационной системе.

10.13. В случае увольнения, перевода на другую должность или изменения должностных обязанностей работника, допущенного к работе с ПДн, а также изменения организационно-штатной структуры Общества, руководитель осуществляет пересмотр прав доступа работника к ПДн и при необходимости уведомляет об этом Директора по кибербезопасности. Директором по кибербезопасности вносятся соответствующие изменения в Перечень структурных подразделений и должностей работников, допущенных к обработке ПДн в ИСПДн (Приложение 1) и Перечень структурных подразделений и должностей работников, допущенных к обработке ПДн на материальных носителях (Приложение 4 к Положению об обработке ПДн).

10.14. При увольнении работника, имеющего доступ к ПДн, документы и иные носители, содержащие ПДн, передаются другому работнику, имеющему доступ к ПДн по указанию руководителя увольняющегося.

11. Защита материальных носителей персональных данных

11.1. Для обеспечения безопасности материальных носителей должны выполняться следующие меры:

– помещения, где осуществляется хранение материальных носителей, должны оснащаться входными дверьми с замками или оборудованы электромеханическими, электромагнитными устройствами СКУД для исключения несанкционированного доступа третьих лиц и работников, не имеющих доступа к работе с ПДн;

– материальные носители должны храниться в запираемых металлических шкафах, обеспечивающих сохранность материальных носителей. В исключительных случаях (при отсутствии указанных хранилищ) допускается хранение в запираемых ящиках рабочих столов.

11.2. Запрещается хранить материальные носители в не запираемых ящиках рабочих столов и других неприспособленных для этого местах.

11.3. Обществом обеспечивается раздельное хранение материальных носителей, обработка которых осуществляется в различных целях.

11.4. О фактах кражи, утери материальных носителей, либо разглашения содержащихся в них сведений работники Общества должны немедленно сообщать непосредственному руководителю.

11.5. По каждому подобному факту (инциденту) неправомерных действий с материальными носителями проводится расследование в установленном порядке.

12. Защита машинных носителей персональных данных

12.1. Машинные носители могут использоваться в Обществе для решения задач, связанных с временным хранением и передачей (обменом) ПДн в электронном виде.

12.2. Машинные носители, необходимые для выполнения работниками своих служебных обязанностей, являются собственностью Общества и подлежат обязательному учету (Приложение 9).

12.3. Запрещается использование машинных носителей ПДн (далее – машинные носители), не учтенных и не являющихся собственностью Общества.

12.4. Регистрация, выдача и уничтожение машинных носителей осуществляется УКБ. Учет машинных носителей осуществляется в Журнале учета машинных носителей ПДн по форме Приложения 4.

12.5. Обществом обеспечивается раздельное хранение машинных носителей, обработка которых осуществляется в различных целях.

12.6. Уничтожение ПДн с машинных носителей должно осуществляться Комиссией в соответствии с Положением об обработке персональных данных.

12.7. Передача ПДн на машинном носителе третьему лицу должна осуществляться на основании акта приема-передачи, являющегося неотъемлемой частью договора с третьим лицом.

13. Требования к защите персональных данных при взаимодействии с третьими лицами

13.1. Привлечение третьих лиц (контрагентов) для оказания различных услуг Общества, а также предоставление Обществом услуг сторонним организациям является потенциальным источником рисков нарушения безопасности информации.

13.2. Общество, как оператор ПДн, при взаимодействии с третьими лицами должна:

– в договорах с третьими лицами определять обязанности по соблюдению требований к обеспечению конфиденциальности и безопасности ПДн, установленные законодательством Российской Федерации, в случае предоставления доступа к ПДн, передачи ПДн или поручения обработки ПДн третьим лицам;

– соблюдать требования к защите ПДн в соответствии с законодательством Российской Федерации и договором при получении ПДн от третьих лиц или осуществлении обработки ПДн по поручению третьих лиц.

13.3. В случаях передачи ПДн и / или предоставления доступа к ИСПДн Общества, доступ к ПДн третьим лицам предоставляется только после проведения анализа, определения и выполнения требований по защите ПДн при согласовании договора.

13.4. При анализе возможности передачи или предоставления доступа к ПДн третьему лицу должны быть учтены и определены в договоре следующие условия:

– перечень ПДн и / или ИСПДн Общества, к которым будет предоставлен доступ третьей стороне;

– тип доступа, который будет предоставлен третьему лицу (передача ПДн по каналам связи, передача на бумажных носителях, физический доступ и (или) удаленный доступ, тип сетевых соединений);

– порядок определения, утверждения, пересмотра списка представителей третьего лица, которым будут предоставлены (переданы) ПДн или будут иметь доступ к ПДн Общества, а также требования к авторизации представителей третьего лица в ИСПДн Общества;

– порядок, меры и средства защиты информации, которые будут использоваться Обществом и третьей стороной при обработке, хранении и передаче ПДн;

– порядок и процедуры уведомления и расследования инцидентов безопасности ПДн, определения ущерба, а также порядок и условия доступа третьего лица к информации в случае инцидентов безопасности ПДн.

13.5. При заключении договора с третьим лицом, получающим доступ к ПДн Общества, в качестве приложения к договору должно подписываться «Соглашение о неразглашении конфиденциальной информации» или должны быть включены соответствующие требования о неразглашении конфиденциальной информации отдельным пунктом в договор.

13.6. Доступ к ПДн Общества, либо их передача или поручение обработки ПДн третьим лицам, должен осуществляться только на основании заключенных договоров.

13.7. Порядок заключения договоров, предусматривающих передачу, предоставление доступа к ПДн или поручение обработки ПДн третьим лицам определен в Регламенте взаимодействия с третьими лицами.
13.8. Доступ к ПДн Общества третьим лицам разрешается только с начала срока действия договорных отношений и завершается со сроком их окончания.

14. Резервирование и восстановление ИСПДн

14.1. Обязательному резервированию в Обществе должны быть подвергнуты следующие информационные ресурсы и системы:

- серверы и рабочие стации пользователей ИСПДн;
- каналы связи и сетевое оборудование обеспечения выхода в сеть Интернет;
- операционные системы, системы управления базами данных, прикладное программное обеспечение ИСПДн;
- подсистема управления доступом, реализованные средствами операционной системы, системы управления базами данных и встроенными механизмами прикладного программного обеспечения;
- подсистема регистрации и учета событий безопасности, реализованная средствами операционной системы, системы управления базами данных и встроенными механизмами прикладного программного обеспечения;
- подсистема антивирусной защиты;
- подсистема межсетевого экранирования;
- иные подсистемы, реализующие механизмы обеспечения защиты на всех уровнях среды обработки, а также базы данных ИСПДн.

14.2. Для всех ИСПДн и подсистем СЗПДн должен быть определен порядок резервирования, содержащий:

- способ резервирования;
- срок хранения резервных копий ПДн;
- перечень работников, ответственных за резервирование;
- периодичности выполнения работ по резервированию и тестированию функций восстановления.

14.3. При резервировании ПДн на машинный носитель информации такой носитель должен быть учтен в соответствии с п. 12 настоящего Положения.
14.4. Восстановление ИСПДн должно производиться в случае инцидентов безопасности ПДн:

- непреднамеренных действий пользователей;
- преднамеренных действий пользователей и третьих лиц (внешних нарушителей);
- нарушения правил эксплуатации технических средств ИСПДн;
- возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

15. Управление инцидентами безопасности персональных данных

15.1. Инцидентом безопасности ПДн является событие или комбинация событий, указывающие на свершившуюся, предпринимаемую или вероятную реализацию угрозы безопасности ПДн, результатом которой является:

– нарушение требований законодательства в области обработки и защиты ПДн;

– нарушение требований внутренних нормативных документов Общества;

– нарушение договорных обязательств в т.ч. контрагентами Общества (поставщиками услуг);

– нарушение свойств безопасности ПДн (конфиденциальности, целостности, доступности), обрабатываемых в ИСПДн и / или без использования средств автоматизации;

– нанесение вреда (ущерба) Обществу или субъектам ПДн.

15.2. Меры по управлению инцидентами безопасности должны включать:

– систематическое проведение оценки актуальных угроз безопасности ПДн;

– проведение оценки ущерба (вреда) Обществу и субъектам ПДн в случае нарушения законодательства в области обработки и защиты ПДн, внутренних нормативных документов, договорных обязательств;

– внедрение организационных и технических мер, направленных на предотвращение и минимизацию негативных последствий, которые могут наступить от реализации (возникновения) угроз безопасности ПДн;

– проведение мероприятий по информированию работников об актуальных угрозах безопасности информации;

– проведение внутреннего контроля (аудита) и/ или внешнего аудита на соответствие требованиям к защите ПДн.

15.3. Порядок выявления, реагирования, расследования инцидентов безопасности ПДн, а также случаи и порядок уведомления уполномоченных органов об инцидентах безопасности ПДн определяется в соответствии с Регламентом реагирования на инциденты безопасности персональных данных.

16. Мониторинг изменений законодательства в области защиты персональных данных

16.1. Мониторинг изменений законодательства в области защиты ПДн проводится в целях своевременного выявления фактов издания, изменения или отмены нормативных правовых актов, устанавливающих обязанности Общества по обеспечению безопасности ПДн.

16.2. Обязанности проводить регулярный мониторинг изменений федерального законодательства в области обработки и защиты ПДн возлагаются на УКБ.

16.3. Обязанности проводить регулярный мониторинг изменений нормативных правовых актов и методических документов Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, ФСТЭК России, ФСБ России возлагаются на УКБ.

16.4. Мониторинг изменений законодательства в области защиты ПДн проводится ежемесячно.

16.5. Мониторинг изменений законодательства в области обработки и защиты ПДн включает в себя:

– поиск и сбор информации об издании, изменениях или отмене нормативных правовых актов, регулирующих обработку и защиту ПДн, в банках данных правовой информации (например, государственная информационная система «Официальный интернет-портал правовой информации», официальные сайты Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, ФСТЭК России, ФСБ России в сети «Интернет», коммерческие справочные правовые системы и др. информационные источники);

– изучение и обобщение информации об изменениях состава и содержания нормативных правовых актов, регулирующих обработку и защиту ПДн;

– информирование работников Общества об изменениях в нормативных правовых актах и иных документах, регулирующих порядок обработки и защиты ПДн.

16.6. При выявлении фактов издания, изменения или отмены нормативных правовых актов в области обработки и защиты ПДн организуется и проводится анализ таких изменений.

16.7. Анализ нормативных изменений включает:

– оценку применимости правовых норм в текущих процессах обработки и защиты ПДн;

– оценку необходимости внесения изменений в текущие процессы обработки ПДн;

– оценку необходимости реализации (принятии) мер по обеспечению безопасности ПДн;

– определение необходимости внесения изменений во внутренние нормативные документы Общества.

16.8. По результатам анализа изменений законодательства формируется перечень корректирующих действий (мер), направленных на приведение в соответствие процессов обработки и защиты ПДн действующему законодательству.

16.9. Корректирующие действия включают в себя:

– разработку и утверждение новых внутренних нормативных документов, актуализацию внутренних нормативных документов Общества или признание их утратившими силу;

– информирование работников Общества об изменениях внутренних нормативных документов Общества в установленном порядке;

– принятие соответствующих мер по организации обработки и защите ПДн в соответствии с требованиями внутренних нормативных документов.

17. Внутренний контроль (аудит) соответствия обработки и защиты персональных данных

17.1. Внутренний контроль (аудит) соответствия обработки и защиты ПДн проводится в целях:

– оценки соответствия процессов обработки и защиты ПДн законодательству Российской Федерации в области обработки и защиты ПДн, Политике Общества в отношении обработки ПДн и внутренним нормативным документам Общества;

– оценки корректности выполнения СЗПДн установленных требований к защите ПДн;

– проверки работников Общества на предмет знания и соблюдения ими требований внутренних нормативных документов по обработке и защите ПДн.

17.2. Порядок проведения внутреннего контроля, состав и периодичность проведения внутренних контрольных мероприятий определяется Регламентом проведения внутреннего контроля (аудита) соответствия обработки и защиты персональных данных.

17.3. По итогам проведения внутренних контрольных мероприятий должны формироваться отчеты, содержащие результаты:

– сведения о выявленных несоответствиях в процессах обработки и защиты ПДн требованиям законодательства в области ПДн;

– сведения о выявленных несоответствиях внутренним нормативным документам, регламентирующим порядок обработки и защиты ПДн;

– перечень корректирующих действий (мер), направленных на приведение в соответствие процессов обработки и защиты ПДн.

18. Оценка эффективности и совершенствование СЗПДн

18.1. Оценка эффективности реализованных в рамках СЗПДн мер по обеспечению безопасности ПДн проводится Обществом самостоятельно или с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанная оценка проводится не реже 1 (одного) раза в 3 года.

18.2. Оценка эффективности СЗПДн выполняется:

– для подтверждения достаточности (полноты) принятых мер по обеспечению безопасности ПДн;

– для сбора данных, необходимых при принятии и обосновании решений о дальнейшем совершенствовании (модернизации) СЗПДн.

18.3. В случае, если оценка эффективности СЗПДн проводится Обществом самостоятельно, для проведения такой оценки приказом руководителя Общества назначается Комиссия.

18.4. Комиссия проводит анализ следующих документов и сведений о реализованных в рамках СЗПДн мер по обеспечению безопасности ПДн:

– внутренние нормативные документы, регламентирующие порядок обработки и обеспечения безопасности ПДн;

– документы, содержащие информацию о способах и методах защиты ИСПДн, мерах или процедурах их использования, которые реализованы для обеспечения безопасности ПДн;

– результаты оценки угроз безопасности информации (Модель угроз безопасности ПДн);

– документы, содержащие информацию по выявленным инцидентам нарушения безопасности ПДн;

– результаты (отчеты) проведения внутреннего контроля (аудита) соответствия обработки и защиты ПДн;

– результаты (отчеты) о проведении внешних аудитов.

18.5. Анализ документов и сведений о реализованных мерах по обеспечению безопасности ПДн включает, в том числе:

– анализ соответствия внутренних нормативных документов, регламентирующих порядок обработки и обеспечения безопасности ПДн, требованиям законодательства Российской Федерации;

– анализ отсутствия несогласованности реализуемых в рамках СЗПДн мер и установленных внутренними нормативными документами требований к защите ПДн.

18.6. Результаты проведенного анализа должны быть документально зафиксированы и содержать либо выводы (заключение) о соответствии реализованных в рамках СЗПДн мер по обеспечению безопасности ПДн, либо выводы (заключение) о принятии организационных и / или технических мер по совершенствованию СЗПДн.

18.7. Совершенствование (модернизация) СЗПДн проводится с целью устранения выявленных по результатам оценки эффективности недостатков, а также для поддержания эффективности СЗПДн.

19. Ответственность

19.1. Ответственность за сопровождение данного Положения в части организации исполнения и контроля соблюдения положений, а также поддержания его в актуальном состоянии несет Лицо, ответственное за обеспечение безопасности данных.

19.2. Ответственность за реализацию положений Положения в части обеспечения безопасности ИТ-инфраструктуры Общества несут сотрудники УКБ.

19.3. Персональную ответственность за обеспечение безопасности и соблюдение конфиденциальности ПДн несет каждый работник, допущенный к обработке такой информации.

19.4. Лица, разгласившие конфиденциальную информацию, а также лица, нарушившие установленный настоящим Положением порядок доступа к ПДн и обеспечения безопасности ПДн несут дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с действующим законодательством Российской Федерации.

19.5. Работник Общества, который в связи с исполнением трудовых обязанностей получил доступ к ПДн, обладателями которой являются третьи лица (контрагенты Общества), в случае умышленного или неосторожного разглашения этой информации при отсутствии в действиях такого работника состава преступления несет дисциплинарную ответственность в соответствии с действующим законодательством Российской Федерации.

20. Пересмотр и внесение изменений

20.1. Положение поддерживается в актуальном состоянии и соответствует текущим целям и задачам Общества в области защиты ПДн. Для этого ежегодно, а также при каждом изменении законодательства Российской Федерации в области обработки и защиты ПДн, внутренних

процессов обеспечения безопасности ПДн, возникновении инцидентов безопасности ПДн, оказавших негативное влияние на деятельность Общества, пересматриваются и при необходимости обновляются разделы Положения.

20.2. Изменения, вносимые в Положение, согласовываются с Комиссией по обеспечению безопасности ПДн, и утверждаются руководителем Общества в соответствии с установленными в Общества порядками и процедурами, и отражаются в Листе регистрации изменений.

Приложения:

1. Форма Перечня структурных подразделений и должностей работников, допущенных к работе с персональными данными в информационных системах персональных данных;
2. Матрица доступа к информационным системам персональных данных;
3. Форма Перечня информационных систем, в которых осуществляется обработка персональных данных;
4. Форма Журнала учета машинных носителей, предназначенных для обработки персональных данных;
5. Форма Акта определения классов СЗИ/СЗКИ информационной системы персональных данных;
6. Форма Акта определения уровня защищенности персональных данных;
7. Форма Обязательства работника об обеспечении конфиденциальности и безопасности персональных данных, а также о прекращении обработки персональных данных;
8. Форма Модели угроз безопасности персональных данных;
9. Первичный инструктаж по правилам обработки и защиты персональных данных;
10. Обязанности пользователя информационной системы персональных данных по обеспечению безопасности персональных данных.