УТВЕРЖДЕНО
решением Совета директоров
АО «Содружество»
Протокол № 02-2020 от 26.02.2020
Председатель совета директоров
_____ В.С. Тюленев

ПОЛОЖЕНИЕ
о контроле за соблюдением режима защиты персональных данных в АО «Содружество»

I. Общие положения

1. Настоящее Положение, разработанное в соответствии с федеральными законами «О персональных данных» и «Об информации, информационных технологиях и о защите информации», политикой АО «Содружество» по обработке и защите персональных данных, иными нормативными правовыми актами Российской Федерации и нормативными документами АО «Содружество», определяет цель, задачи и порядок контроля за соблюдением режима защиты персональных данных в АО «Содружество».

2. В настоящем Положении используются следующие понятия:

1) защита персональных данных – деятельность АО «Содружество», включающая принятие правовых, организационных и технических мер, направленных на обеспечение защиты от неправомерных действий в отношении персональных данных;

2) инцидент, связанный с нарушением режима защиты персональных данных, – одно или ряд нежелательных или непредвиденных событий, которые могут нарушить режим защиты персональных данных;

3) контроль за соблюдением режима защиты персональных данных – совокупность действий и операций по мониторингу и проверке соблюдения требований законодательства Российской Федерации и нормативных документов АО «Содружество» в области персональных данных;

4) мониторинг соблюдения режима защиты персональных данных – постоянное наблюдение за процессами обработки и обеспечения безопасности персональных данных, включая рассмотрение поступающей (выявляемой) информации о рисках, связанных с нарушениями режима защиты персональных данных, а также сбор, анализ и обобщение результатов наблюдения.

5) персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

6) режим защиты персональных данных – нормативно установленные правила, определяющие ограничение доступа к персональным данным и процессам их обработки, а также порядок их передачи и условия хранения;

7) риск, связанный с нарушением режима защиты персональных данных, – потенциальная опасность нанесения ущерба АО «Содружество» финансового и/или репутационного характера в результате нарушения требований законодательства Российской Федерации и нормативных документов АО «Содружество» в области персональных данных;

3. Целью контроля за соблюдением режима защиты персональных данных (далее – контроль) является оценка в рамках риск-ориентированного подхода соответствия обработки и обеспечения безопасности персональных данных требованиям законодательства Российской Федерации и нормативных документов АО «Содружество» в области персональных данных.

4. Задачи контроля:

1) анализ выполнения требований законодательства Российской Федерации и нормативных документов АО «Содружество» в области обработки и обеспечения безопасности персональных данных;

2) выявление рисков, связанных с нарушениями режима защиты персональных данных, установление причин их возникновения;

3) разработка мероприятий по воздействию на выявленные риски для их минимизации (устранения), а также предотвращения их повторного возникновения и реализации.

5. Контроль за соблюдением режима защиты персональных данных и обеспечением их безопасности осуществляется в АО «Содружество», ответственным за организацию обработки персональных данных в АО «Содружество» и ответственным за обеспечение безопасности персональных данных в информационных системах АО «Содружество».

6. Контроль за выполнением требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119, проводится не реже 1 раза в 3 года ответственным за организацию обработки персональных данных в АО «Содружество».

II. Мониторинг соблюдения режима защиты персональных данных

7. Ответственный за организацию обработки персональных данных в АО «Содружество» по кругу ведения осуществляет мониторинг в части:

1) соблюдения порядка организации доступа к персональным данным;

2) соблюдения требований конфиденциальности при обработке персональных данных;

3) своевременности назначения и установления обязанностей ответственного за обеспечение безопасности персональных данных в информационных системах АО «Содружество»;

4) актуальности списков работников, уполномоченных на обработку персональных данных;

5) включения обязанностей уполномоченных на обработку персональных данных в их должностные инструкции;

6) ознакомления под подпись работников, уполномоченных на обработку персональных данных, с нормативными документами АО «Содружество» в области персональных данных;

7) наличия письменных обязательств о неразглашении персональных данных от работников, уполномоченных на обработку персональных данных;

8) актуальности перечней помещений, в которых хранятся материальные носители персональных данных;

9) учета машинных носителей персональных данных;

10) актуальности сведений, содержащихся в паспорте оператора персональных данных АО «Содружество» и его соответствия форме, утвержденной распоряжением АО «Содружество» от 25 апреля 2018 г. № 816/р;

11) организации работы с обращениями субъектов персональных данных, их представителей и юридических лиц по вопросам обработки персональных данных.

8. Ответственный за организацию обработки персональных данных в АО «Содружество осуществляет мониторинг правомерности доступа работников и сторонних организаций к информационным системам АО «Содружество», а также оценки эффективности реализованных мер по обеспечению безопасности обрабатываемых в ней персональных данных в соответствии с требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119.

9. Ответственный за организацию обработки персональных данных в АО «Содружество» незамедлительно информирует генерального директора АО «Содружество» об утечке персональных данных субъектов персональных данных, которая может серьезно отразиться на правах и основных свободах субъектов персональных данных в АО «Содружество».

10. Ответственным за организацию обработки персональных данных в АО «Содружество» для проведения мониторинга информационных систем могут использоваться специальные программно-технические средства сбора,

записи и хранения событий информационной безопасности с возможностью их анализа и уведомления об их возникновении в АО «Содружество».

11. По факту выявленных в процессе мониторинга рисков, связанных с нарушениями режима защиты персональных данных и обеспечения их безопасности, принимаются меры по их минимизации (устранению), в том числе работы по приведению информационной системы обработки персональных данных в соответствие с требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119.

При необходимости проводится внеплановая проверка соблюдения режима защиты персональных данных.

III. Организация и проведение проверок соблюдения режима защиты персональных данных

12. Проверки соблюдения режима защиты персональных данных (далее также – проверки) организует ответственный за организацию обработки персональных данных в АО «Содружество».

13. Для проведения проверок и контроля процедур, в том числе связанных с автоматизированной обработкой персональных данных, оценки причиненного (возможного) материального и (или) иного вреда субъекту персональных данных, а также ущерба коммерческим интересам АО «Содружество» и минимизации имиджевых рисков в соответствии с установленным в АО «Содружество» порядке могут на договорной основе привлекаться юридические лица и индивидуальные предприниматели.

14. Проверки подразделяются на плановые, внеплановые и контрольные. Длительность проверки не может превышать 20 календарных дней. При необходимости срок проверки может быть продлен ответственным за организацию обработки персональных данных в АО «Содружество» или руководителем АО «Содружество» на срок не более 20 дней.

15. Допускается проведение проверки одновременно в нескольких подразделениях АО «Содружество».

16. Плановая проверка проводится не реже чем один раз в полгода.

17. Для проведения проверки издается приказ по форме согласно приложению № 1, в соответствии с которым образуется комиссия по проведению проверки соблюдения режима защиты персональных данных (далее также – комиссия) численностью не менее 3 человек.

18. Основанием для проведения проверки соблюдения режима защиты персональных данных является приказ о проведении проверки (приложение № 1).

19. Руководитель подразделения АО «Содружество», в котором запланировано проведение проверки, уведомляется о проверке не менее, чем за 1 рабочий день до ее начала, путем ознакомления с приказом о проведении проверки.

20. Внеплановая проверка в подразделениях АО «Содружество» проводится по указанию генерального директора АО «Содружество» либо ответственного за обработку персональных данных в АО «Содружество». Контрольная проверка в подразделениях АО «Содружество» проводится для оценки полноты устранения нарушений, выявленных в ходе плановой или внеплановой проверки, после завершения мероприятий, по устранению выявленных нарушений, но не позднее одного года с даты завершения проверки.

21. В случае выявления в ходе проверки фактов утраты материальных носителей персональных данных, распространения либо неправомерной обработки персональных данных субъектов персональных данных проводится служебное расследование.

IV. Права, обязанности и ответственность комиссии по проведению проверки соблюдения режима защиты персональных данных

22. Члены комиссии руководствуются при проведении проверки настоящим Положением и другими нормативными и методическими документами АО «Содружество».

23. Председатель комиссии:

1) в день начала проверки представляет руководителю подразделения АО «Содружество», в котором будет проведена проверка, членов комиссии, доводит информацию о порядке проведения;

2) организует взаимодействие с руководителем проверяемого подразделения;

3) устанавливает по согласованию с руководителем проверяемого подразделения время ежедневного пребывания членов комиссии в служебных помещениях в течение срока проверки с учетом режима работы этого подразделения;

4) может ознакомить руководителя проверяемого подразделения с проектом акта проверки и иными материалами проверки до ее завершения.

24. Члены комиссии имеют право:

1) входить в служебные помещения проверяемого подразделения в сопровождении работников этого подразделения;

2) пользоваться необходимыми для проведения проверки техническими средствами;

3) запрашивать в проверяемом подразделении необходимые для проведения проверки документы (сведения);

4) проводить беседы и консультации с работниками проверяемого подразделения, требовать предоставления письменных справок, отчетов по вопросам, рассматриваемым в ходе проверки;

5) снимать копии с документов проверяемого подразделения для приобщения к материалам проверки;

6) знакомиться с документацией на автоматизированные рабочие места и информационные системы, используемые при обработке персональных данных, проверяемым подразделением;

7) запрашивать от работников проверяемого подразделения информацию о функционировании автоматизированных рабочих мест и информационных систем, используемых при обработке персональных данных;

8) требовать от работников проверяемого подразделения демонстрации своей работы на автоматизированных рабочих местах с информационными системами при обработке персональных данных и производить выборку необходимой информации;

9) направлять запросы в другие подразделения АО «Содружество» с целью получения дополнительной информации по вопросам, рассматриваемым в ходе проверки.

25. Члены комиссии несут ответственность в соответствии с законодательством Российской Федерации за разглашение полученных в ходе проверки сведений, содержащих персональные данные и иной информации ограниченного доступа.

V. Обязанности руководителя и работников подразделений АО «Содружество», в которых проводится проверка

26. Руководитель подразделения АО «Содружество», в котором проводится проверка:

1) информирует работников подразделения о цели и характере проверки;

2) определяет работников подразделения для работы с членами комиссии;

3) обеспечивает доступ к документам (сведениям) в ходе проведения проверки, а также иные условия для проведения проверки.

27. Руководитель и работники проверяемого подразделения в период проверки обязаны:

1) содействовать комиссии в проведении проверки;

2) обеспечивать беспрепятственный доступ членов комиссии в служебные помещения проверяемого подразделения;

3) предоставлять при необходимости членам комиссии рабочие места в служебном помещении проверяемого подразделения;

4) демонстрировать членам комиссии свою работу на автоматизированных рабочих местах с информационными системами, содержащими персональные данные, включая выборку необходимой информации;

5) предоставлять документы (сведения), необходимые для проведения проверки, в сроки, установленные председателем комиссии.

28. В случае отсутствия документов (сведений), необходимых для проведения проверки, и (или) возникновения обстоятельств, препятствующих их предоставлению, руководитель подразделения АО «Содружество», в котором проводится проверка, представляет председателю комиссии письменное объяснение с указанием причин.

VI. Оформление результатов проверки соблюдения режима защиты персональных данных, порядок разработки, утверждения и исполнения плана устранения нарушений

29. По результатам проведения проверки составляется в двух экземплярах акт, по форме согласно приложению № 2.

Сведения о проверке отражаются в журнале учета проверок соблюдения режима защиты персональных данных по форме согласно приложению № 3.

30. Основная часть акта проверки содержит информацию о рассмотренных в ходе проверки вопросах с обязательным отражением по каждому из них следующих сведений:

1) о выполнении в проверяемом подразделении АО «Содружество» требований законодательства Российской Федерации и нормативных документов АО «Содружество» в области обработки и обеспечении безопасности персональных данных, принятых мерах по обеспечению безопасности персональных данных;

2) о выявленных нарушениях режима защиты персональных данных;

31. Заключительная часть акта проверки содержит выводы комиссии по результатам проведения проверки.

Документы, подтверждающие выявленные в ходе проверки нарушения, при необходимости приобщаются к акту.

32. Акт проверки составляется не позднее 10 рабочих дней с даты окончания проверки и подписывается председателем и членами комиссии.

В случае невозможности подписания акта проверки каким-либо членом комиссии (болезнь, отпуск, служебная командировка, иные объективные причины) председатель комиссии делает в акте соответствующую отметку.

33. По результатам проверки председатель комиссии представляет генеральному директору отчет о проведенной проверке согласно приложению № 5.

34. Руководитель подразделения АО «Содружество» не позднее 10 рабочих дней с даты проведения проверки, разрабатывает и предлагает на утверждение план устранения выявленных нарушений по форме согласно приложению № 4.

35. Мероприятия, предусмотренные планом по устранению нарушений, не влекущие за собой дополнительного финансирования, должны быть исполнены подразделением АО «Содружество», в котором проводилась проверка, в течение одного месяца с даты ознакомления с актом проверки.

36. Отчет подразделения об исполнении плана устранения нарушений предоставляется ответственному за организацию обработки персональных данных в АО «Содружество» не позднее 5 рабочих дней со дня истечения срока, предусмотренного указанным планом в АО «Содружество».

Приложение № 1
к Положению о контроле
за соблюдением режима
защиты персональных
данных в АО
«Содружество»

АКЦИОНЕРНОЕ ОБЩЕСТВО
«Содружество»

ПРИКАЗ

«_____»_____20__ г. №____

О проведении внутренней проверки по обеспечению безопасности персональных данных в АО «Содружество»

В целях проверки соблюдения режима защиты и обработки персональных данных, обеспечения безопасности хранения и обработки персональных данных и приведения информационной системы обработки и хранения персональных данных в соответствие с ФЗ-152 «О персональных данных», п р и к а з ы в а ю:

1. В срок с ___ по __ провести в АО «Содружество» внутреннюю проверку по вопросу обеспечения безопасности персональных данных.
2. Определить рабочую группу в следующем составе:

Фамилия И.О. – _____ (председатель комиссии)
(должность, Ф.И.О.)

Фамилия И.О. – _____
(должность, Ф.И.О.)

Фамилия И.О. – _____
(должность, Ф.И.О.)

3. Утвердить план внутренней проверки по обеспечению безопасности персональных данных работников АО «Содружество», представленный в приложении к настоящему приказу.
4. В срок до _____по результатам проведенной проверки представить отчет о проведенной проверки и план устранения выявленных нарушений.
5. Контроль за исполнением настоящего приказа возложить на _____

Генеральный директор _____

Приложение
К приказу №____от
«О проведении внутренней проверки по обеспечению безопасности персональных данных в АО «Содружество»

№п/п	Наименование подразделения	№ кабинета	Срок проведения	Цель проведения проверки

Приложение № 2
к Положению о контроле за
соблюдением режима
защиты персональных
данных в АО«Содружество»

АКЦИОНЕРНОЕ ОБЩЕСТВО
«Содружество»

АКТ ПРОВЕРКИ

Дата начала проверки «___»_____ 20___ г.
Дата окончания проверки «___»_____ 20___ г.

Место проведения проверки _____.
(адрес проверяемого подразделения АО «Содружество»)

Настоящий акт составлен по результатам проверки соблюдения режима защиты персональных данных в _____,
(наименование подразделения АО «Содружество»)
проведенной комиссией в составе:

Фамилия И.О. – _____ (председатель комиссии)
(должность)
Фамилия И.О. – _____
(должность)
Фамилия И.О. – _____
(должность)
на основании _____.

В ходе проверки рассмотрены следующие вопросы:
_____

Выводы по результатам проверки
_____.

Приложение:_____ на _____ л.
(с указанием прилагаемых документов и их копий)
Настоящий акт составлен в двух экземплярах.
Председатель комиссии _____ _____
(подпись) (расшифровка подписи)
Члены комиссии: _____ _____
(подпись) (расшифровка подписи)

«___»_____ 20___ г.

С актом проверки ознакомлен:

_____ _____ _____
(должность) (подпись) (расшифровка подписи)
«___»_____ 20___ г.

Приложение № 3
к Положению о контроле за
соблюдением режима защиты
персональных данных в
АО«Содружество»

Ж У Р Н А Л
учета проверок соблюдения режима защиты персональных данных

п/п	Наименование проверяемого подразделения	Адрес места нахождения объекта проверки	№ и дата составления акта проверки	№ и дата Плана устранения нарушений	№ дела, где хранятся материалы проверки
1	2	3	4	5	6

Приложение № 4
к Положению о контроле за соблюдением режима защиты персональных данных в АО «Содружество»

УТВЕРЖДАЮ

_____
Руководитель АО «Содружество»

(подпись) И.О.Фамилия
(дата)

ПЛАН
устранения нарушений, выявленных в ходе проверки соблюдения режима защиты персональных данных в АО «Содружество»

№ п/п	Нарушение	Мероприятия по устранению нарушений	Ответственный	Срок исполнения

Должность (подпись) ФИО

Приложение № 5
к Положению о контроле
за соблюдением режима
защиты персональных
данных в АО
«Содружество»

УТВЕРЖДАЮ
Председатель комиссии по
проведению внутренней проверки
по обеспечению безопасности
персональных данных
в АО «Содружество»

И.О. Фамилия_____

Дата

Отчет
о проведении внутренней проверки по обеспечению безопасности персональных данных в АО «Содружество»

Члены комиссии внутренней проверки:

ФИО - должность

1. Перечень подразделений в которых проводилась проверка

_____
_

2. Нарушения, выявленные в ходе проверки

_____

По результатам проверки подготовлен и представлен на утверждение план по устранению недостатков выявленных в ходе проверки обеспечения безопасности персональных данных АО «Содружество».