УТВЕРЖДЕН
Решением Совета директоров
ОАО «Содружество»
(Протокол от «12» декабря 2016г.
№ 09-2016)
Председатель совета директоров

_____/В.С. Тюленев

ПОЛОЖЕНИЕ
об организации контроля за соблюдением режима защиты персональных данных в ОАО «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 ОАО «Содружество» по обработке и защите персональных данных, иными нормативными правовыми актами Российской Федерации и нормативными документами ОАО «Содружество», определяет порядок организации контроля за соблюдением режима защиты персональных данных в подразделении аппарата управления, и структурных подразделениях ОАО «Содружество».

2. В настоящем Положении используются следующие термины и понятия:

1) информационная безопасность - состояние защищенности информации, при котором обеспечиваются такие ее характеристики, как конфиденциальность, целостность и доступность;

2) инциденты, связанные с нарушениями режима защиты персональных данных - одно или ряд нежелательных или непредвиденных событий, которые могут нарушить режим защиты персональных данных;

3) контроль процедур, связанных с компьютерной обработкой информации и информационными системами (компьютерный контроль) - контроль доступа, целостности, внесения изменений в информационные системы, обрабатывающие персональные данные, уровня защищенности персональных данных;

4) режим защиты персональных данных - нормативно установленные правила, определяющие ограничения доступа к персональным данным, порядок передачи и условия их хранения;

5) событие информационной безопасности - определенное проявление состояния системы, информационной службы (сервиса) или информационного ресурса, указывающее на возможные недостатки в политике информационной безопасности или недостатки мер защиты, или

ранее неизвестную ситуацию, которая может повлиять на безопасность персональных данных;

6) средства защиты информации - технические, программные, программно-технические средства, предназначенные или используемые для защиты информации.

3. Контроль за соблюдением режима защиты персональных данных осуществляется путем мониторинга и проверок, организуемых ответственными за организацию обработки персональных данных в структурных подразделениях ОАО «Содружество».

Контроль и координацию работы ответственных за организацию обработки персональных данных в структурных подразделениях ОАО «Содружество» осуществляет специально созданная комиссия по защите персональных данных (далее - комиссия).

4. Ответственные за организацию обработки персональных данных в структурных подразделениях ОАО «Содружество» представляют в комиссию аналитическую справку, содержащую результаты мониторинга режима защиты персональных данных, с выводами о состоянии защищенности персональных данных и предложениями по повышению уровня их безопасности и совершенствованию режима защиты персональных данных, а также статистический отчет о контроле за соблюдением режима защиты персональных данных с пояснительной запиской к нему по форме согласно приложению №1.

Указанные документы за первое полугодие направляются в комиссию до 15 июля текущего года, за второе полугодие - до 15 января следующего года.

5. Комиссия для проведения проверок и контроля процедур, связанных с компьютерной обработкой информации и информационными системами, оценки причиненного (возможного) материального или иного вреда субъекту персональных данных, а также ущерба коммерческим интересам и минимизации имиджевых рисков ОАО «Содружество» может в установленном ОАО «Содружество» порядке привлекать своих сотрудников с учетом специфики их деятельности, а также на договорной основе юридических лиц и индивидуальных предпринимателей.

6. Контроль процедур, связанных с компьютерной обработкой информации и информационными системами, осуществляется в соответствии с пунктом 17 требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 г. №1119, регулярно, не реже 1 раза в 3 года.

7. Целью контроля за соблюдением режима защиты персональных данных является оценка соответствия обработки персональных данных

требованиям законодательства Российской Федерации в области обработки и защиты персональных данных, требованиям к защите персональных данных, политике ОАО «Содружество» по обработке и защите персональных данных и другим нормативным документам ОАО «Содружество».

8. Задачами контроля за соблюдением режима защиты персональных данных являются:

1) проверка выполнения требований законодательства Российской Федерации и нормативных документов ОАО «Содружество» в области обработки и защиты персональных данных;

2) проверка соблюдения прав субъектов персональных данных;

3) выявление недостатков и нарушений режима защиты персональных данных, установление причин их возникновения, а также выработка предложений, направленных на их устранение и предотвращение;

4) проверка уровня защищенности персональных данных;

5) проверка порядка и условий применения средств защиты информации, используемых в информационных системах, обрабатывающих персональные данные;

6) проверка порядка организации доступа к персональным данным;

7) проверка соблюдения требований конфиденциальности при обработке персональных данных;

8) проверка организации учета, хранения и использования материальных носителей персональных данных.

II. Мониторинг соблюдения режима защиты персональных данных

9. Мониторинг соблюдения режима защиты персональных данных (далее - мониторинг) представляет собой постоянное наблюдение за процессом обработки и защиты персональных данных в структурных подразделениях ОАО «Содружество», а также сбор, анализ и обобщение результатов наблюдения с целью определения его текущего состояния и соответствия законодательству Российской Федерации и нормативным документам ОАО «Содружество».

10. Мониторингу подлежат:

1) своевременность назначения ответственного за организацию обработки персональных данных;

2) актуальность списков работников, уполномоченных на обработку персональных данных;

3) включение обязанностей ответственных за организацию обработки персональных данных, а также уполномоченных на обработку персональных данных в их должностные инструкции;

4) актуальность перечней помещений, в которых хранятся материальные носители персональных данных;

5) учет машинных носителей персональных данных;

6) порядок организации доступа к персональным данным;

7) порядок и условия применения средств защиты информации, используемых в информационных системах, обрабатывающих персональные данные;

8) соблюдение требований конфиденциальности при обработке персональных данных;

9) рассмотрение обращений субъектов персональных данных по вопросам нарушений обработки персональных данных;

10) иные события информационной безопасности, которые могут повлиять на соблюдение режима защиты персональных данных.

11. По факту выявленных в процессе мониторинга инцидентов, связанных с нарушениями режима защиты персональных данных, проводится проверка и принимаются меры к их устранению.

По результатам проверки осуществляется анализ причин возникновения инцидентов и проводятся мероприятия по их недопущению в дальнейшем.

12. Мониторинг соблюдения режима защиты персональных данных, обрабатываемых в информационных системах, проводится с помощью программного обеспечения, применяемого в этих информационных системах.

По согласованию с ответственным за организацию обработки персональных данных в ОАО «Содружество» для проведения мониторинга могут использоваться специальные программно-технические средства сбора, анализа событий информационной безопасности и уведомления об их возникновении.

13. Ответственные за организацию обработки персональных данных в подразделениях ОАО «Содружество» информируют комиссию не позднее чем за месяц:

1) об определении уровня защищенности персональных данных при их обработке во вводимых в эксплуатацию новых информационных системах;

2) о вводе в эксплуатацию новых и модернизации эксплуатируемых информационных систем, обрабатывающих персональные данные в ОАО «Содружество»;

3) об изменении уровня защищенности персональных данных, обрабатываемых в информационной системе, в случае изменения состава, категорий, объема персональных данных, принадлежности персональных данных работникам ОАО «Содружество» или иным субъектам персональных данных;

4) об изменении состава средств защиты информации, применяемых в информационных системах, обрабатывающих персональные данные;

5) об аттестации по требованиям безопасности информации вводимых в эксплуатацию информационных систем, в которых планируется обработка персональных данных;

6) о переаттестации по требованиям безопасности информации информационных систем, обрабатывающих персональные данные, в случае окончания срока действия аттестата соответствия или модернизации информационных систем, вызывающей необходимость переаттестации.

III. Организация и проведение проверок соблюдения режима защиты персональных данных

14. Проверке соблюдения режима защиты персональных данных (далее - проверка) подлежат структурные подразделения ОАО «Содружество», в которых осуществляется обработка персональных данных.

15. Проверки могут организовываться:

1) в структурных подразделениях ОАО «Содружество» - комиссией;

2) ответственным за организацию обработки персональных данных в ОАО «Содружество» проводятся проверки в бухгалтерии и отделах по управлению делами и персоналом, труда и заработной платы.

16. Для проведения проверки приказом генерального директора ОАО «Содружество» образуется комиссия численностью не менее 3 человек.

17. Основанием для проверки является предписание о ее проведении, составленное в 2 экземплярах по форме согласно приложению № 2, которое подписывается ответственным за организацию обработки персональных данных в ОАО «Содружество».

Председатель комиссии представляет предписание о проведении проверки руководителю проверяемого подразделения, который подписывает его. Второй экземпляр предписания остается у председателя комиссии.

18. Проверки подразделяются на плановые, внеплановые и контрольные. Длительность проверки не может превышать 20 календарных дней.

19. План проверок на следующий год, проводимых комиссией, утверждается ответственным за организацию обработки персональных данных в ОАО «Содружество». Выписка из плана направляется руководителям проверяемых подразделений.

20. План проверок на следующий год, проводимых в бухгалтерии, отделе по управлению делами и персоналом, отделе труда и заработной платы утверждается руководителями этих подразделений. Копия плана

направляется в комиссию до 1 декабря текущего года, выписка из плана направляется руководителям проверяемых подразделений.

21. Руководитель проверяемого подразделения: бухгалтерии, отдела по управлению делами и персоналом, отдела труда и заработной платы письменно уведомляется о плановой проверке не менее чем за 10 календарных дней до ее начала. В уведомлении указываются сроки проведения проверки, перечень вопросов, которые будут рассматриваться в ходе проверки, а также требования к организации и проведению проверки.

22. Внеплановая проверка в структурных подразделениях ОАО «Содружество» проводится по указанию генерального директора ОАО «Содружество» в случае наличия инцидента, связанного с нарушениями режима защиты персональных данных.

23. Контрольная проверка проводится для оценки полноты устранения нарушений, выявленных в ходе плановой или внеплановой проверки, после завершения мероприятий, предусмотренных планом устранения нарушений, но не позднее одного года с даты завершения проверки.

24. При проведении проверок федеральными органами исполнительной власти, осуществляющими контроль и надзор в области обработки и защиты персональных данных (Роскомнадзор, ФСТЭК России, ФСБ России), руководителям подразделений ОАО «Содружество» необходимо руководствоваться федеральным законодательством в области защиты персональных данных и внутренними документами ОАО «Содружество».

При получении от указанных федеральных органов уведомления о планируемой проверке руководитель проверяемого подразделения в 3-дневный срок направляет в комиссию копию уведомления, а после завершения проверки - копию акта проверки с соответствующим предписанием (при наличии).

IV. Права, обязанности и ответственность комиссии

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

26. Председатель комиссии:

1) организует взаимодействие с руководителем проверяемого подразделения по вопросам, рассматриваемым в ходе проверки;

2) устанавливает по согласованию с руководителем проверяемого подразделения время ежедневного пребывания членов комиссии в

служебных помещениях в течение срока проверки с учетом режима работы подразделения;

3) по согласованию с генеральным директором ОАО «Содружество», может ознакомить руководителя проверяемого подразделения с проектом акта проверки и иными материалами проверки до ее завершения.

27. Члены комиссии имеют право:

1) входить в служебные помещения проверяемого подразделения в сопровождении работников проверяемого 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 используемые проверяемым подразделением автоматизированные рабочие места и информационные системы, обрабатывающие персональные данные;

7) запрашивать от работников проверяемого подразделения информацию о функционировании автоматизированных рабочих мест и информационных систем, обрабатывающих персональные данные;

8) требовать от работников проверяемого подразделения демонстрации своей работы на автоматизированных рабочих местах с информационными системами, обрабатывающими персональные данные, включая выборку необходимой информации;

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

28. Члены комиссии несут ответственность в соответствии с законодательством Российской Федерации за разглашение полученных в ходе проверки сведений конфиденциального характера.

V. Обязанности руководителя и работников проверяемого подразделения

29. Руководитель проверяемого подразделения:

1) информирует работников о цели и характере проверки;

2) определяет работников подразделения, в число которых должен входить ответственный за организацию обработки персональных данных, для работы с членами комиссии;

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

30. 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.

В случае отсутствия документов (сведений), необходимых для проведения проверки, и (или) возникновения обстоятельств, препятствующих их предоставлению, руководитель проверяемого подразделения представляет председателю комиссии письменное объяснение о невозможности выполнения требований настоящего подпункта с указанием причин.

VI. Оформление результатов проверки

31. Результаты проверки подразделения отражаются в акте проверки, который составляется в 2 экземплярах по форме согласно приложению № 3 на бумажном носителе.

32. Аналитическая часть акта проверки содержит сведения:

1) о документах (сведениях), предоставленных и не предоставленных проверяемым подразделением в ходе проведения проверки;

2) о выполнении проверяемым подразделением требований законодательства Российской Федерации и нормативных документов ОАО «Содружество» в области обработки и защиты персональных данных, о принятых мерах по защите персональных данных;

3) о выявленных нарушениях режима защиты персональных данных с указанием места и времени совершения нарушений;

4) о невыполнении требований нормативных правовых актов Российской Федерации и нормативных документов ОАО «Содружество» в области обработки и защиты персональных данных;

5) об устранении проверяемым подразделением выявленных нарушений на дату завершения проверки.

Выявленные нарушения отражаются в акте проверки с учетом их значимости для оценки состояния режима защиты персональных данных.

33. Заключительная часть акта проверки содержит обобщенную информацию об основных результатах проверки и выводы комиссии по результатам ее проведения.

34. Акт проверки составляется не позднее 10 календарных 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 и иные объективные причины) председатель комиссии делает в акте соответствующую отметку.

35. Экземпляр акта проверки направляется руководителю проверяемого подразделения не позднее 10 календарных дней с даты окончания проверки.

36. Руководитель проверяемого подразделения не позднее 10 рабочих дней с даты получения акта проверки утверждает план устранения нарушений, который направляется в комиссию (ответственному в ОАО «Содружество», подписавшему предписание о проведении проверки).

37. Сведения о проверке отражаются в журнале учета проверок соблюдения режима защиты персональных данных в ОАО «Содружество», который ведется в комиссии (и структурном подразделении ОАО «Содружество») по форме согласно приложению №4.

38. По результатам проверки председатель комиссии представляет руководителю структурного подразделения ОАО «Содружество» докладную записку с приложением акта проверки.

39. Председатель комиссии информирует в установленном порядке ответственного за организацию обработки персональных данных в ОАО «Содружество» о результатах проведения проверки.

Приложение № 1
к Положению об
организации контроля за
соблюдением режима
защиты персональных
данных в ОАО «Содружество»

СТАТИСТИЧЕСКИЙ ОТЧЕТ

о контроле за соблюдением режима защиты персональных данных

в ОАО «Содружество»

за _____

(период)

№ п/п	Сведения	Количество
1.	Проверки, проводимые контролирующими и надзирающими органами	
1.1.	Роскомнадзор	
1.2.	ФСБ России	
1.3.	ФСТЭК России	
1.4.	Прокуратура	
1.5.	Другие	
2.	Получено предписаний об устранении нарушений, выявленных контролирующими и надзирающими органами	
2.1.	Роскомнадзор	
2.2.	ФСБ России	
2.3.	ФСТЭК России	
2.4.	Прокуратура	
2.5.	Другие	
3.	Получено протоколов об административных правонарушениях от контролирующих и надзирающих органов	
3.1.	Роскомнадзор	
3.2.	ФСБ России	
3.3.	ФСТЭК России	

3.4.	Прокуратура	
3.5.	Другие	
4.	Проведено внутренних проверок	
№ п/п	**Сведения**	**Количество**
5.	Рассмотрено обращений (запросов) субъектов персональных данных или уполномоченного органа по защите прав субъектов персональных данных о нарушениях обработки персональных данных	
6.	Выявлено нарушений режима защиты персональных данных	
7.	Проведено служебных расследований	
7.1.	По фактам утраты материальных носителей персональных данных	
7.2.	По фактам разглашения персональных данных	
7.3.	По фактам неправомерной обработки персональных данных	
8.	Привлечено к дисциплинарной и(или) материальной ответственности	
9.	Направлено обращений в правоохранительные органы в отношении лиц, допустивших утрату материальных носителей персональных данных, разглашение либо неправомерную обработку персональных данных субъектов персональных данных	
10.	Заключено договоров с третьими лицами на обработку персональных данных	

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
к статистическому отчету о контроле за соблюдением режима защиты персональных данных

К статистическому отчету прилагается пояснительная записка, содержащая следующую информацию:

по пункту 1 - указывается общее количество проверок, проведенных контролирующими и надзирающими органами;

по подпунктам 1.1. - 1.5 - указывается количество, вид, период проверок, мероприятия по контролю, проведенные в ходе проверок, информация об отсутствии или наличии нарушений с названием вида нарушения и нарушенных нормативно-правовых актов;

по подпунктам 2.1. - 2.5. указывается количество полученных предписаний об устранении выявленных нарушений с содержанием нарушения и предписания, сроки устранения;

по подпунктам 3.1. - 3.5. указывается количество полученных протоколов об административных правонарушениях, кем, в отношении кого составлен протокол, событие административного правонарушения со ссылкой на нарушенные нормы законодательства, результаты рассмотрения дела;

по пункту 4 - указывается количество, вид, период проверок, перечень вопросов рассмотренных в ходе проверки, результаты проверки;

по пункту 5 - излагается суть и результаты рассмотренных обращений (запросов) субъектов персональных данных или уполномоченного органа по защите прав субъектов персональных данных о нарушениях обработки персональных данных;

по пункту 6 - дается краткое описание выявленных нарушений режима защиты персональных данных как при автоматизированной, так и неавтоматизированной обработке персональных данных, с указанием со ссылкой на нарушенные нормы законодательства и нормативные документы ОАО «Содружество» в области обработки и защиты персональных данных, а также результаты проверки;

по подпунктам 7.1 - 7.3 - указываются сведения, содержащиеся в заключении о результатах проведенного служебного расследования по фактам утраты материальных носителей, разглашения персональных данных либо неправомерной обработки персональных данных;

по пункту 8 - указываются сведения о привлечении виновных работников ОАО «Содружество» к дисциплинарной и (или) материальной ответственности по результатам служебного расследования;

по пункту 9 - дается краткое описание материалов, направленных по инициативе руководителя ОАО «Содружество» в правоохранительные и контролирующие органы, в отношении лиц, допустивших утрату материальных носителей персональных данных, разглашение либо неправомерную обработку персональных данных субъектов персональных данных и требующих уголовно-правового, административного или иного преследования уполномоченными органами государства. Указываются также принятые по ним решения;

по пункту 10 - указываются сведения о договорах, заключенных с третьими лицами на обработку персональных данных, в том числе состав персональных данных субъектов персональных данных, перечень действий (операций) с персональными данными и цели обработки;

Ответственный за организацию
Обработки персональных данных
ОАО «Содружество» _____ _____
(подпись) (расшифровка подписи)

«_____» _____20____г.

Приложение № 2
к Положению об
организации контроля за
соблюдением режима
защиты персональных
данных в ОАО «Содружество»

Открытое Акционерное Общество
«СОДРУЖЕСТВО»
(ОАО «Содружество»)

ПРЕДПИСАНИЕ
о проведении проверки

от «___»_____20___г. № _____
В соответствии с _____
(основание для проведения проверки)
_____

комиссии в составе:
председатель комиссии _____
(должность, ФИО)
и члены комиссии: _____
(должность, ФИО)

поручается провести проверку _____
(наименование подразделения)
_____

Вопросы, рассматриваемые в ходе проверки: _____

_____

Предписание действительно с «__»_____20__ г. до «___»_____ 20__ г.

_____ _____ _____
(должность) (подпись) (расшифровка подписи)
«___»_____20___г.

Печать

Предписание получено «____»_____ 20____г.

_____ _____ _____
(должность) (подпись) (расшифровка подписи)

Приложение № 3
к Положению об
организации контроля за
соблюдением режима
защиты персональных
данных в ОАО «Содружество»

Экз. № _____

Открытое Акционерное Общество
«СОДРУЖЕСТВО»
(ОАО «Содружество»)

АКТ ПРОВЕРКИ

Дата начала проверки «____»_____20___г.
Дата окончания проверки «____»_____ 20___г.

Место проведения проверки _____
(адрес проверяемого подразделения)

Настоящий акт составлен по результатам проверки _____

Проведенной на основании _____
_____
_____
(аналитическая и заключительная части 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 подразделения ознакомлен:

_____ _____ _____
(должность) (подпись) (расшифровка подписи)

«___»_____20___г.

Приложение № 4
к Положению об
организации контроля за
соблюдением режима
защиты персональных
данных в ОАО «Содружество»

ЖУРНАЛ
Учета проверок соблюдения режима защиты персональных данных в ОАО «Содружество»

№ п/п	Наименование проверяемого подразделения	Адрес места нахождения объекта проверки	№ и дата предписания о проведении проверки	Должность, фамилия, инициалы председателя комиссии	№ и дата составления акта проверки	Дата вручения (направления) акта проверки	№ дела, где хранятся документы