Приложение № 3
к приказу ректора
Самарского университета
от 03.10.2017 № 770-О

Правила
осуществления внутреннего контроля соответствия обработки и защиты персональных данных требованиям законодательства в федеральном государственном автономном образовательном учреждении высшего образования «Самарский национальный исследовательский университет имени академика С.П. Королева»

Самара, 2017 г.

1. Настоящие правила осуществления внутреннего контроля соответствия обработки и защиты персональных данных требованиям к защите персональных данных (далее - правила), установленным Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и правовыми актами федерального государственного автономного образовательного учреждения высшего образования «Самарский национальный исследовательский университет имени академика С.П. Королева» (далее – университет), определяют процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки и защиты персональных данных (далее – ПД) требованиям законодательства.

2. В настоящих правилах используются следующие основные понятия:

1) **персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных – работнику, обучающемуся и иному физическому лицу);

2) **лицо, уполномоченное на получение, обработку, хранение, передачу и другое использование персональных данных** – работник, организующий и (или) осуществляющий обработку персональных данных, а также определяющий цели и содержание обработки персональных данных;

3) **лицо, ответственное за обработку и защиту персональных данных в структурном подразделении** – работник, контролирующий обработку персональных данных в подразделении, организующий правовое информирование работников подразделения (обучающихся в подразделении) и обеспечивающий информационное взаимодействие по данным вопросам с уполномоченными должностными лицами университета;

4) **обработка персональных данных** – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

5) **автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники;

6) **распространение персональных данных** - действия, направленные на раскрытие персональных данных неопределенному кругу лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление

доступа к персональным данным неопределенному кругу лиц каким-либо иным способом;

7) **предоставление персональных данных** - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

8) **блокирование персональных данных** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

9) **уничтожение персональных данных** - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

10) **обезличивание персональных данных** - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

11) **информационная система персональных данных** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

12) **трансграничная передача персональных данных** - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

13) **сбор персональных данных** – сбор информации, содержащей ПД на материальных носителях и (или) в автоматизированных информационных системах;

14) **накопление и систематизация персональных данных** – организация размещения ПД, которое обеспечивает быстрый поиск и отбор нужных сведений, обновление данных, защиту их от искажений, потери;

15) **хранение персональных данных** – комплекс мероприятий, направленный на обеспечение сохранности полноты и целостности сформированных массивов ПД, создание и поддержание надлежащих условий для их использования, а также предупреждение несанкционированного доступа, распространения и использования;

16) **уточнение персональных данных** – процесс поддержания ПД в актуальном состоянии;

17) **использование персональных данных** – действия (операции) с ПД, совершаемые лицом, уполномоченным на получение, обработку, хранение, передачу и другое использование ПД в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц, либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;

18) **материальный носитель** – бумажный и машиночитаемый носители информации (в том числе магнитный и электронный), на которых осуществляются запись и хранение ПД;

19) **доступ к персональным данным** – возможность получения ПД и их использования;

20) **конфиденциальность персональных данных** – обязательное для соблюдения лицом, уполномоченным на получение, обработку, хранение, передачу и другое использование персональных данных или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания;

21) **общедоступные персональные данные** – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности;

22) **третья сторона** – любое физическое или юридическое лицо, орган государственной власти или местного самоуправления, кроме субъекта персональных данных, университета (оператора) и лиц, уполномоченных на получение, обработку, хранение, передачу и другое использование персональных данных на законных основаниях;

23) **защита персональных данных** – технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и обеспечивающий безопасность информации в процессе деятельности университета;

24) **технические средства, позволяющие осуществлять обработку персональных данных** – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы

управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах;

3. Правила разработаны в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Постановлением Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Постановлением Правительства РФ «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации» № 687 от 15.09.2008, и локальными нормативно-правовыми актами университета.

4. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям законодательства к обработке и защите персональных данных университет организует проведение проверок соответствия обработки персональных данных установленным требованиям законодательства к обработке и защите персональных данных (далее - проверки) в структурных подразделениях университета.

5. Проверки осуществляются членами постоянно действующей комиссии по контролю соответствия обработки и защиты персональных данных установленным требованиям законодательства в структурных подразделениях университета (далее - Комиссия), состав которой утверждается приказом ректора университета. При необходимости к проверке могут привлекаться специалисты и иные должностные лица университета.

6. Проверки проводятся на основании:

- утвержденного ректором университета плана-графика осуществления внутреннего контроля соответствия обработки персональных данных требованиям законодательства к обработке и защите персональных данных в структурных подразделениях и календарного плана проведения проверок, составленного в соответствии с план-графиком и утвержденного председателем Комиссии (плановые проверки). Плановые проверки могут проводиться не чаще одного раза в три года;

- поступившего в университет заявления о нарушении требований законодательства к обработке и защите персональных данных или предписания (указания, запроса и т.п.) контрольно-надзорного органа исполнительной власти (внеплановые проверки). Проведение внеплановой проверки организуется в течение 7 рабочих дней со дня регистрации соответствующего заявления.

7. В ходе проверки проводится полная, объективная и всесторонняя оценка:

7.1. Наличия и актуальности правовых и организационно-распорядительных документов, утверждаемых в соответствии с правовыми актами университета в области обработки и защиты персональных данных.

7.2. Информирования лиц, осуществляющих обработку персональных данных, о положениях законодательства Российской Федерации, правовых актах университета о порядке обработки персональных данных и требованиях к обеспечению безопасности персональных данных.

7.3. Соответствия утвержденного перечня помещений университета (структурного подразделения), в которых ведется обработка персональных данных (автоматизированная и неавтоматизированная), фактическому использованию помещений для обработки персональных данных.

7.4. Соответствия утвержденного перечня должностных лиц университета (структурного подразделения), замещение должностей которых предусматривает осуществление обработки персональных данных, либо осуществление доступа к персональным данным, фактическому составу должностных лиц, осуществляющих обработку персональных данных, либо имеющих доступ к персональным данным.

7.5. Соответствия утвержденного перечня используемых материальных носителей персональных данных (бумажных и электронных) университета (структурного подразделения), фактическому составу материальных носителей персональных данных (бумажных и электронных) университета (структурного подразделения).

7.7. Соответствия утвержденного перечня используемых технических средств и программного обеспечения (баз данных) для обработки и защиты персональных данных университета (структурного подразделения), фактическому использованию технических средств и программного обеспечения (баз данных) для обработки и защиты персональных данных университета (структурного подразделения).

7.7. Соблюдения установленного порядка доступа должностных лиц структурных подразделений университета в помещения, в которых ведется обработка персональных данных.

7.8. Соблюдения сроков обработки и хранения персональных данных.

7.9. Соответствия утвержденного перечня обрабатываемых персональных данных, фактическому перечню персональных данных, обрабатываемых в университете (структурном подразделении) в связи с реализацией трудовых отношений, а также в связи с оказанием образовательных услуг, осуществлением функций и исполнением отдельных полномочий.

7.10. Соблюдения правил обработки персональных данных, осуществляемой без использования средств автоматизации, в том числе:

- раздельного хранения персональных данных, обработка которых осуществляется в разных целях;

- соответствия фактических мест хранения материальных носителей персональных данных местам хранения материальных носителей персональных данных, утвержденным правовым актом университета (списком мест хранения материальных носителей персональных данных в структурном подразделении);

- соответствия использования типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, установленным требованиям законодательства;

- информирование должностных лиц, осуществляющих обработку персональных данных без использования средств автоматизации о факте обработки ими персональных данных, обработка которых осуществляется без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами, а также локальными правовыми актами университета;

- состояния учета машинных съемных носителей информации.

7.11. Соблюдения правил обработки персональных данных в информационных системах для выполнения требований законодательства к обработке и защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных, в том числе:

- порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

- состав, порядок и условия применения программных и технических средств обработки и защиты персональных данных, использование которых обеспечивает установленные уровни защищенности персональных данных;

- использования сертифицированных средств защиты информации и соблюдения условий их использования лицами, осуществляющими обработку персональных данных;

- эффективность принимаемых мер по обеспечению безопасности персональных данных при эксплуатации информационной системы персональных данных;

- наличия возможности незамедлительного восстановления персональных данных, модифицированных или уничтоженных в случае несанкционированного доступа;

- соблюдение должностными лицами требований инструкций, регламентирующих обработку и защиту персональных данных.

7.12. Уровня осведомленности и знаний должностных лиц, допущенных к обработке персональных данных, в области обработки и защиты персональных данных.

8. Информация о сроках проведения плановых проверок доводится до руководителей структурных подразделений путем рассылки приказа ректора университета об утверждении план-графика проведения внутреннего контроля соответствия обработки персональных данных требованиям законодательства к обработке и защите персональных данных в структурных подразделениях университета.

9. Персональный состав должностных лиц, проводящих плановую или внеплановую проверку (не менее двух должностных лиц), и конкретные сроки её проведения оформляются указанием (Приложения №1,№2) ответственного за организацию обработки персональных данных университета (председателя Комиссии) о проведении проверки (далее – указание) и доводятся до руководителя структурного подразделения не позднее чем за три рабочих дня до начала ее проведения.

10. Руководитель структурного подразделения, в котором проводится проверка должен обеспечить необходимые условия для проведения проверки и обязан по требованию членов Комиссии, проводящих проверку, организовать доступ к оборудованию и документам, в помещения, где осуществляется обработка персональных данных, предоставить необходимую информацию и документацию для достижения целей проверки.

11. Члены Комиссии и должностные лица, привлекаемые к проведению проверки, имеют право:

- запрашивать и получать у должностных лиц структурного подразделения информацию и документы (копии документов), необходимые для реализации полномочий;

- получать доступ к техническим и программным средствам, используемым для обработки и защиты ПД должностными лицами структурного подразделения, просматривать и фиксировать на материальных носителях (бумажных и электронных) перечни и характеристики данных средств и состав ПД (копии экранов с ПД, структура баз данных и т.п.);

- требовать от должностных лиц, уполномоченных на обработку персональных данных уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

- привлекать к проведению проверки (включать в состав должностных лиц, проводящих проверку) специалистов и должностных лиц университета, не входящих в состав Комиссии;

- принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;

- вносить предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;

- вносить предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

12. Срок проведения проверки не более 10 рабочих дней. При необходимости срок проведения проверки может быть продлен, но не более, чем на 10 рабочих дней.

13. По результатам проведенной проверки составляется акт проверки (Приложение №3). Акт подписывается должностными лицами, проводившими проверку и руководителем структурного подразделения (должностным лицом, замещающим руководителя структурного подразделения на момент подписания акта), утверждается председателем Комиссии и хранится у секретаря Комиссии. Копия акта направляется руководителю структурного подразделения университета, в котором проводилась проверка.

14. Акт должен содержать описание нарушений, срок устранения выявленных нарушений (в случае их наличия) и, при необходимости, рекомендации по их устранению.

15. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений (в случае их наличия), ректору университета докладывает ответственный за организацию обработки персональных данных университета (председатель Комиссии).

16. На основании результатов проведенной проверки при обнаружении фактов осуществления обработки персональных данных с нарушением требований законодательства Российской Федерации, ответственный за организацию обработки персональных данных университета (председатель Комиссии) принимает решение о приостановлении или прекращении обработки персональных данных в структурных подразделениях университета, либо, в случае невозможности устранения нарушений (обеспечения правомерности обработки), об уничтожении таких персональных данных.

17. Члены Комиссии и должностные лица, привлекаемые к проведению проверки обязаны соблюдать конфиденциальность информации ограниченного доступа (персональных данных), ставшей известной им в ходе проведения проверки.

Приложение № 1
к Правилам осуществления внутреннего контроля соответствия
обработки и защиты персональных данных требованиям
законодательства в Самарском университете

Указание (образец)

ответственного за организацию обработки персональных данных университета о проведении внеплановой проверки

О проведении внеплановой
проверки в отношении Института ...

Во исполнение приказа ректора Самарского университета от _____ № _____и в связи с поступлением заявления о нарушении требований законодательства к обработке и защите персональных данных в Институте ...

ПРЕДЛАГАЮ

1. В соответствии с правилами осуществления внутреннего контроля соответствия обработки и защиты персональных данных требованиям законодательства, утвержденными приказом ректора Самарского университета от _____ № _____в период с 16 сентября 2017 г. по 26 сентября 2017 г. провести внеплановую проверку в отношении Института ....

2. В состав должностных лиц, осуществляющих проверку включить: главного специалиста по защите информации, Никитина Александра Михайловича – председатель, инженеров НИЛ-55, Иванова Семен Викторовича и Петрова Дмитрия Анатольевича.

3. Директору Института ... обеспечить необходимые условия для проведения проверки, организовать доступ к оборудованию, в помещения, где осуществляется обработка персональных данных, предоставить необходимую информацию и документацию для достижения целей проверки.

Проректор по общим вопросам Ковалёв М.А.

Приложение № 2
к Правилам осуществления внутреннего контроля соответствия
обработки и защиты персональных данных требованиям
законодательства в Самарском университете

Указание (образец)

ответственного за организацию обработки персональных данных университета о проведении плановых проверок в период с …. по ….

О проведении плановых проверок соответствия обработки и защиты персональных данных в структурных подразделениях университета требованиям законодательства в период с октября 2017 года по декабрь 2017 года

Во исполнение приказа ректора Самарского университета от _____ № _____

ПРЕДЛАГАЮ

1. Утвердить План внутренних проверок соответствия обработки и защиты персональных данных требованиям законодательства в структурных подразделениях университета в период с октября по декабрь 2017 года (Приложение №1 к настоящему указанию).

2. Назначить лицами, уполномоченными на проведение проверок: главного специалиста по защите информации Никитина А.М. - председатель, инженера НИЛ-55 Иванова С.А.

3. Должностным лицам, уполномоченным на проведение проверок, провести внутренние проверки подразделений университета в соответствии с Планом (см. Приложение № 1 к настоящему указанию).

4. Руководителям проверяемых структурных подразделений университета со своей стороны предоставить доступ проверяющих в подразделение согласно Плану (см. Приложение № 1 к настоящему указанию) и обеспечить проведение проверок в соответствии с п.10 правил осуществления внутреннего контроля соответствия обработки и защиты персональных данных требованиям законодательства, утвержденных приказом ректора Самарского университета от _____ № _____. В случае невозможности проведения проверки в назначенное время руководителю структурного подразделения необходимо не менее чем за 3 рабочих дня до утвержденной даты проверки согласовать с председателем комиссии, утвердившем план, новое время проверки.

5. Руководителям подразделений, прошедших проверку, подготовить планы устранения выявленных нарушений по результатам проверки не позднее 15 рабочих дней со дня окончания проверки.

6. Возложить на руководителей подразделений ответственность за устранение выявленных нарушений в установленные планами сроки.

7. Заведующей канцелярией Елистратовой Л.Е. довести приказ до сведения руководителей структурных подразделений, указанных в Плане (см. Приложение № 1 к настоящему указанию).

Проректор по общим вопросам Ковалёв М.А.

Приложение № 1 к указанию от _____ № _____

«Утверждаю»
Председатель комиссии по контролю
соответствия обработки и защиты персональных данных
установленным требованиям законодательства

_____ М.А. Ковалев

«___» _____ 2017 г.

План (образец)
проведения внутренних проверок соответствия обработки и защиты персональных данных в структурных подразделениях Самарского университета требованиям законодательства на октябрь – декабрь 2017 года

№№ п/п	Наименование	Срок проведения проверки	
		Дата начала	Дата окончания
1	Управление по работе с персоналом	02.10.2017	16.10.2017
2	Студенческий отдел кадров	09.10.2017	23.10.2017
3	Управление бухгалтерского учета	16.10.2017	30.10.2017
...	...	...	...
12	Планово-финансовое управление	18.12.2017	29.12.2017
13	Управление по формированию контингента	25.12.2017	29.12.2017

Секретарь Комиссии

А.М.Никитин

Приложение № 3
к Правилам осуществления внутреннего контроля соответствия
обработки и защиты персональных данных требованиям
законодательства в Самарском университете

«Утверждаю»
Председатель комиссии по контролю
соответствия обработки и защиты персональных данных
установленным требованиям законодательства

_____ М.А. Ковалев

«___» _____ 2017 г.

АКТ (образец)

проверки соответствия обработки и защиты персональных данных установленным требованиям законодательства в отношении Института …

№ хх

г. Самара *«10 » октября 2017г.*

По адресу/адресам: *443086, г. Самара, Московское шоссе, 34, корпус № 15, ауд. 404, 411; Академика Павлова, д.1, корпус 22, ауд. 216*

В соответствии с: *Планом-графиком внутренних проверок соответствия обработки и защиты персональных данных установленным требованиям законодательства, утвержденным приказом ректора Самарского университета № хх-О от __ июня 2017 года*

была проведена *плановая проверка* **в отношении:**
Института …

Дата и время проведения проверки: *с «06» октября 2017 г. по «20» октября 2017 г.*

Общая продолжительность проверки: *10 рабочих дней*

Лицо(а), проводившие проверку:
Никитин Александр Михайлович – главный специалист по защите информации - председатель;

Петров Семен Викторович – инженер НИЛ-55;

Иванов Дмитрий Анатольевич – инженер НИЛ-55.

При проведении проверки присутствовали:
Крылов Виктор Анатольевич – ведущий специалист Института ….

В ходе проведения проверки:

выявлены следующие нарушения :

1) *Несоответствие (отсутствие) перечня помещений структурного подразделения, в которых ведется обработка персональных данных (автоматизированная и неавтоматизированная), фактическому использованию помещений для обработки персональных данных;*
2) *Несоответствие (отсутствие) перечня должностных лиц структурного подразделения, замещение должностей которых предусматривает осуществление обработки персональных данных, либо осуществление доступа к персональным данным, фактическому составу должностных лиц, осуществляющих обработку персональных данных, либо имеющих доступ к персональным данным;*
3) *Несоответствие (отсутствие) перечня используемых материальных носителей персональных данных (бумажных и электронных), фактическому составу материальных носителей персональных данных (бумажных и электронных) структурного подразделения;*
4) *Несоответствие (отсутствие) перечня используемого в структурном подразделении программного обеспечения (баз данных) для обработки и защиты персональных данных, фактическому использованию программного обеспечения (баз данных) для обработки и защиты персональных данных;*
5) *Несоответствие (отсутствие) перечня обрабатываемых персональных данных, фактическому перечню персональных данных, обрабатываемых в структурном подразделении в связи с реализацией трудовых отношений, а также в связи с оказанием образовательных услуг, осуществлением функций и исполнением отдельных полномочий;*
6) *Несоответствие (отсутствие) перечня мест хранения материальных носителей персональных данных, фактическим местам хранения материальных носителей персональных данных;*
7) *Несоблюдение требований по информированию лиц, осуществляющих обработку персональных данных без использования средств автоматизации;*
8) *Несоответствие типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, требованиям законодательства Российской Федерации;*
9) *Несоблюдение требований в части обеспечения раздельного хранения, персональных данных (материальных носителей), обработка которых осуществляется в различных целях без использования средств автоматизации;*
10) *Несоблюдение порядка и правил применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;*
11) *Использование не сертифицированных средств защиты информации и не соблюдение условий их использования должностными лицами, осуществляющими обработку персональных данных;*
12) *Недостаточный уровень осведомленности и знаний должностных лиц, допущенных к обработке персональных данных, в области обработки и защиты персональных данных;*
13) *Нарушение установленного законом права субъекта персональных данных на получение информации, касающейся обработки его персональных данных;*
14) *Обработка биометрических и специальных категорий персональных данных без письменного согласия субъекта персональных данных;*
15) *Неисполнение обязательств по устранению нарушений, допущенных при обработке персональных данных, а также по уточнению, блокированию и уничтожению персональных данных;*
16) *Неисполнение требований по прекращению и уничтожению персональных данных в*

случае отзыва субъектом персональных данных согласия на обработку своих персональных данных;

17) *Нарушение требований конфиденциальности при обработке персональных данных;*
18) *Поручение иному лицу осуществлять обработку персональных данных без согласия субъекта персональных данных;*
19) *Несоблюдение установленных требований по ознакомлению должностных лиц, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных и локальными актами по вопросам обработки персональных данных;*

Срок устранения нарушений: 20.12.2017 г.

Прилагаемые документы:

1. Материалы, подтверждающие нарушения:

   Приложение № 1 к акту проверки от 20.10.2017

   № хх на 5 листах в 1 экз.

2. Рекомендации по устранению нарушений:

   Приложение № 2 к акту проверки от 20.10.2017

   № хх на 2 листах в 1 экз.

Подписи лиц, проводивших проверку:

А.М. Никитин

С.В. Петров

Д.А. Иванов

С актом проверки ознакомлен(а):

_____

(ФИО, должность)

«____» _____2017 г.

_____

(подпись)