



ПРАВИТЕЛЬСТВО САНКТ-ПЕТЕРБУРГА
КОМИТЕТ ПО ИНФОРМАТИЗАЦИИ И СВЯЗИ

П Р И К А З

ОКУД 0251151

№ 31-17

**О мерах, направленных на обеспечение
выполнения обязанностей, предусмотренных
Федеральным законом Российской Федерации
«О персональных данных» в Комитете
по информатизации и связи**

В соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации», Федеральным законом «О персональных данных», Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановлением Правительства Российской Федерации от 21.03.2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», Постановлением Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

П Р И К А З Ы В А Ю:

1. Утвердить:

1.1. Правила обработки персональных данных в Комитете по информатизации и связи согласно приложению № 1.

1.2. Порядок доступа государственных гражданских служащих и работников, замещающих должности, не являющиеся должностями государственной гражданской службы, Комитета по информатизации и связи в помещения, в которых ведется обработка персональных данных, согласно приложению № 2.

1.3. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленных Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами Российской Федерации и организационно-распорядительными актами Комитета по информатизации и связи, согласно приложению № 3.

1.4. Правила работы с обезличенными данными согласно приложению № 4.

1.5. Правила рассмотрения запросов субъектов персональных данных или их представителей согласно приложению № 5.

1.6. Инструкцию о действиях лиц, допущенных к информации, содержащей персональные данные, в случае возникновения нештатных ситуаций в Комитете по информатизации и связи согласно приложению № 6.

1.7. Инструкцию по порядку учета и хранению съемных машинных носителей информации, доступ к которой ограничен в соответствии с федеральными законами, в Комитете по информатизации и связи согласно приложению № 7.

1.8. Инструкцию о порядке резервного копирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации информационных систем персональных данных в Комитете по информатизации и связи согласно приложению № 8.

1.9. Инструкцию ответственного за организацию обработки персональных данных в Комитете по информатизации и связи согласно приложению № 9.

1.10. Инструкцию пользователя персонального компьютера при работе в локальной вычислительной сети Смольного в Комитете по информатизации и связи согласно приложению № 10.

1.11. Инструкцию пользователя автоматизированной системы обработки конфиденциальной информации и персональных данных в Комитете по информатизации и связи согласно приложению № 11.

1.12. Инструкцию по организации антивирусной защиты в Комитете по информатизации и связи согласно приложению № 12.

1.13. Перечень информационных систем персональных данных Комитета по информатизации и связи, в которых должна быть обеспечена безопасность информации, согласно приложению № 13.

1.14. Перечень должностей государственных гражданских служащих и работников, замещающих должности, не являющиеся должностями государственной гражданской службы, Комитета по информатизации и связи, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных в Комитете по информатизации и связи, согласно приложению № 14.

1.15. Перечень сведений конфиденциального характера, подлежащих защите в Комитете по информатизации и связи, согласно приложению № 15.

1.16. Перечень государственных гражданских служащих и работников, замещающих должности, не являющиеся должностями государственной гражданской службы, Комитета по информатизации и связи, допущенных к работе с персональными данными, обрабатываемыми в Комитете по информатизации и связи, согласно приложению № 16.

1.17. Форму согласия на обработку персональных данных согласно приложению № 17.

1.18. Форму обязательства государственного гражданского служащего и работника, замещающего должность, не являющуюся должностью государственной гражданской службы, Комитета по информатизации и связи, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним служебного контракта (трудового договора) прекратить обработку персональных данных, ставших известными ему в связи исполнения должностных обязанностей, согласно приложению № 18.

1.19. Форму разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные в связи

с поступлением на государственную гражданскую службу в Комитет по информатизации и связи, ее прохождением согласно приложению № 19.

2. Назначить ответственным за организацию обработки персональных данных в Комитете по информатизации и связи главного специалиста отдела информационно-компьютерной безопасности Управления информационной безопасности и технической защиты информации Цыулева С.В.

3. Контроль за выполнением настоящего приказа возложить на первого заместителя председателя Комитета по информатизации и связи Чамару Д.П.

Председатель Комитета
по информатизации и связи



И.А.Громов

ПРАВИЛА

обработки персональных данных в Комитете по информатизации и связи

1. Общие положения

1.1. Настоящие Правила обработки персональных данных в Комитете по информатизации и связи (далее – Правила) определяют порядок обработки персональных данных в Комитете по информатизации и связи (далее – Комитет) в связи с реализацией служебных или трудовых отношений, а также в связи с осуществлением государственных функций и оказанием государственных услуг.

1.2. Персональные данные, обрабатываемые в Комитете, являются информацией, доступ к которой ограничен в соответствии с федеральными законами за исключением сведений, подлежащих распространению в средствах массовой информации в соответствии с действующим законодательством Российской Федерации.

1.3. Целью данных Правил является защита информации, содержащей персональные данные, доступ к которой ограничен в соответствии с законодательством Российской Федерации, от несанкционированного доступа, неправомерного их использования или утраты.

2. Используемые понятия

Для целей настоящих Правил используются следующие основные понятия:

оператор – Комитет, самостоятельно или совместно с другими лицами организующий и (или) осуществляющий обработку персональных данных, а также определяющий цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом;

информация – сведения (сообщения, данные) независимо от формы их предоставления;

Закон – Федеральный закон «О персональных данных».

3. Категории субъектов персональных данных

3.1. В качестве субъектов персональных данных, персональные данные которых могут обрабатываться в Комитете с использованием средств автоматизации или без использования таковых, понимаются нижеперечисленные категории лиц:

государственные гражданские служащие (далее – сотрудники) и работники, замещающие должности, не являющиеся должностями государственной гражданской службы (далее – работники), Комитета по информатизации и связи (далее – сотрудники);

руководители подведомственных Комитету предприятий и учреждений; граждане, претендующие на замещение вакантных должностей государственной гражданской службы и должностей, не являющихся должностями государственной гражданской службы, Комитета;

граждане и организации, обратившиеся в Комитет по вопросам, находящимся в ведении Комитета

4. Обработка персональных данных в Комитете в связи с осуществлением государственных функций и оказанием государственных услуг

4.1. Общие правила обработки персональных данных в Комитете в связи с осуществлением государственных функций и оказанием государственных услуг.

4.1.1. Обработка персональных данных в Комитете должна осуществляться в соответствии с действующим законодательством Российской Федерации.

4.1.2. Целью обработки персональных данных в Комитете является осуществление государственных функций и оказание государственных услуг.

4.1.3. Обработка персональных данных в Комитете должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

4.1.4. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

4.1.5. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

4.1.6. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

4.1.7. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных.

Главный специалист отдела информационно-компьютерной безопасности, Управления информационной безопасности и технической защиты информации Комитета, ответственный за организацию обработки персональных данных в Комитете, должен принимать решения и организовывать необходимые меры по удалению или уточнению неполных или неточных персональных данных.

4.1.8. Мерами, направленными на защиту сведений, содержащих персональные данные, являются:

- осуществление внутреннего контроля соответствия обработки персональных данных нормам Закона и принятым в соответствии с ним правовыми актами;

- оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Закона, соотношение указанного вреда и принимаемых Комитетом мер, направленных на обеспечение выполнения обязанностей, предусмотренных Законом;

- ознакомление сотрудников (работников), непосредственно осуществляющих обработку персональных данных, с нормами законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, и (или) обучение сотрудников (работников), подписанием обязательства сотрудника (работника) о соблюдении конфиденциальности персональных данных и соблюдении правил их обработки.

4.1.9. Обеспечение безопасности персональных данных достигается, в частности:

- определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

- применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

- проведением, в установленном порядке, процедуры оценки соответствия средств защиты информации, содержащей персональные данные;

- оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

- учетом машинных носителей с информацией, содержащей персональные данные;

- обнаружением фактов несанкционированного доступа к персональным данным и принятием мер по их недопущению;

- восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных.

4.1.10. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъект персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен Законом, договором, стороной которого является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено Законом.

4.1.11. В случае выявления неправомерной обработки персональных данных, осуществляемой сотрудником (работником), в срок, не превышающий три рабочих дней с даты выявления данного факта, он обязан прекратить неправомерную обработку персональных данных.

В случае если обеспечить правомерность обработки персональных данных невозможно, сотрудник (работник) в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные.

Об устранении допущенных нарушений или об уничтожении персональных данных сотрудник (работник) обязан уведомить субъекта персональных данных или его представителя, а в случае если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

4.1.12. В случае достижения цели обработки персональных данных сотрудник (работник) обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого является субъект персональных данных, иным соглашением между Комитетом и субъектом персональных данных.

4.1.13. В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных сотрудник (работник) обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между Комитетом и субъектом персональных данных.

Об уничтожении персональных данных сотрудник (работник) обязан уведомить субъекта персональных данных не позднее трех рабочих дней со дня уничтожения.

4.1.14. В случае отсутствия возможности уничтожения персональных данных в течение сроков, указанных выше, сотрудник (работник) осуществляет блокирование таких персональных данных и обеспечивает уничтожение персональных данных в срок, не превышающий шесть месяцев, если иной срок не установлен Закон и иными федеральными законами Российской Федерации.

4.1.15. Доступ к персональным данным имеют сотрудники (работники), которым персональные данные необходимы в связи с исполнением ими служебных (трудовых) обязанностей и занимающие должности согласно Перечню государственных гражданских служащих и работников, замещающих должности, не являющиеся должностями государственной гражданской службы, Комитета по информатизации и связи, допущенных к работе с персональными данными, обрабатываемыми в Комитете.

Доступ к персональным данным может быть предоставлен иному сотруднику (работнику), должность которого не включена в Перечень государственных гражданских служащих и работников, замещающих должности, не являющиеся должностями государственной гражданской службы, Комитета по информатизации и связи, допущенных к работе с персональными данными, обрабатываемыми в Комитете, на основании служебной записки от руководителя

структурного подразделения Комитета на имя первого заместителя председателя Комитета.

5. Обработка персональных данных сотрудников (работников) Комитета в связи с реализацией служебных (трудовых) отношений

5.1. Обработка персональных данных осуществляется для обеспечения соблюдения законов и иных нормативных правовых актов.

5.2. Сотрудники Сектора по вопросам государственной службы и кадров Комитета (далее – уполномоченные специалисты) не имеют права получать и обрабатывать персональные данные сотрудника (работника) Комитета о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации уполномоченные специалисты вправе получать и обрабатывать данные о частной жизни сотрудника (работника) только с его письменного согласия.

Уполномоченные специалисты не имеют права получать и обрабатывать персональные данные сотрудника (работника) о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных Законом.

При принятии решений, затрагивающих интересы сотрудника (работника), уполномоченные специалисты не имеют права основываться на персональных данных сотрудника (работника), полученных исключительно в результате их автоматизированной обработки или в электронном виде по техническим каналам связи.

5.3. В соответствии с Трудовым кодексом Российской Федерации, а также исходя из положений Закона, обработка персональных данных сотрудников (работников) осуществляется Комитетом в связи с реализацией служебных и трудовых отношений в качестве работодателя без письменного согласия сотрудника (работника), за исключением случаев, предусмотренных Законом.

5.4. Все персональные данные о сотруднике (работнике) Комитет может и должен получить от него самого.

5.5. Сотрудник (работник) обязан предоставлять в Комитет достоверные сведения о себе и своевременно сообщать об изменении своих персональных данных. Комитет имеет право проверять достоверность сведений, предоставленных сотрудником (работником), сверяя представленные данные с оригиналами документов.

5.6. В случаях, когда Комитет может получить необходимые персональные данные сотрудника (работника) только у третьего лица, Комитет должен уведомить об этом сотрудника (работника) и получить от него письменное согласие (приложение № 1).

Комитет обязан сообщить сотруднику (работнику) о целях, способах и источниках получения персональных данных, а также о характере подлежащих получению персональных данных и возможных последствиях отказа сотрудника (работника) дать письменное согласие на их получение.

5.7. Персональные данные сотрудника (работника) хранятся в Секторе по вопросам государственной службы и кадров Комитета в личном деле

сотрудника (работника). Личные дела хранятся в бумажном виде в папках и находятся в сейфе или в негорючем шкафу.

Персональные данные сотрудника (работника) в Секторе по вопросам государственной службы и кадров Комитета хранятся также в электронном виде на выделенной электронно-вычислительной машине, не подключенной к вычислительной сети Комитета. Доступ к электронным базам данных, содержащим персональные данные сотрудников (работников), обеспечивается системой паролей. Пароли устанавливаются начальником Сектора по вопросам государственной службы и кадров Комитета и сообщаются индивидуально уполномоченным специалистам, имеющим доступ к персональным данным сотрудников (работников).

Хранение персональных данных сотрудников (работников) в Финансово-бухгалтерском отделе Комитета, осуществляется на электронно-вычислительных машинах, подключенных в защищенный сегмент вычислительной сети Комитета, с выполнением всех требований по защите информации.

5.8. Сотрудник (работник), имеющий доступ к персональным данным сотрудников (работников) в связи с исполнением служебных (трудовых) обязанностей, обеспечивает хранение информации, содержащей персональные данные сотрудников (работников), исключая доступ к ней третьих лиц.

В отсутствие сотрудника (работника) на его рабочем месте не должно быть документов, содержащих персональные данные сотрудников (работников).

При уходе в отпуск, убытии в служебную командировку и иных случаях длительного отсутствия сотрудника (работника) на своем служебном месте, он обязан передать документы и носители, содержащие персональные данные сотрудников (работников) лицу, на которое приказом Комитета будет возложено исполнение его служебных обязанностей.

В случае если такое лицо не назначено, то документы и носители, содержащие персональные данные, передаются другому сотруднику (работнику), имеющему доступ к персональным данным сотрудников (работников) по указанию руководителя структурного подразделения Комитета.

При увольнении сотрудника (работника), имеющего доступ к персональным данным сотрудников (работников), документы и носители, содержащие персональные данные сотрудников (работников) Комитета, передаются другому сотруднику (работнику), имеющему соответствующий доступ к персональным данным сотрудников (работников) по указанию руководителя структурного подразделения Комитета.

5.9. В случае если Комитету оказывают услуги юридические и физические лица на основании заключенных договоров (либо иных оснований) и в силу данных договоров они должны иметь доступ к персональным данным сотрудников (работников), то соответствующие данные предоставляются Комитетом только после подписания с ними соглашения о неразглашении конфиденциальной информации (приложение № 2).

В исключительных случаях, исходя из существа договорных отношений Комитета с контрагентом, допускается наличие в договорах пунктов о неразглашении конфиденциальной информации, в том числе предусматривающих защиту переданных персональных данных сотрудников (работников).

5.10. Процедура оформления доступа к персональным данным сотрудников Комитета включает в себя:

ознакомление сотрудника (работника) под роспись с настоящими Правилами;

получение от сотрудника (работника) письменного обязательства о соблюдении конфиденциальности персональных данных и соблюдении правил их обработки;

При наличии иных нормативных актов (приказы, распоряжения, инструкции и т.п.), регулирующих обработку и защиту персональных данных сотрудников (работников), также производится ознакомление под роспись.

5.11. Сотрудники (работники), имеющие доступ к персональным данным, имеют право получать только те персональные данные сотрудников (работников), которые необходимы им для выполнения конкретных служебных обязанностей.

5.12. Сотрудник (работник) имеет право на свободный доступ к своим персональным данным, включая право на получение копии любой записи (за исключением случаев, предусмотренных Законом), содержащей его персональные данные. Сотрудник (работник) имеет право вносить предложения по внесению изменений в свои данные в случае обнаружения в них неточностей.

Представителю сотрудника (работника) персональные данные сотрудника (работника) передаются на основании заявления и при наличии нотариально удостоверенной доверенности или доверенности, приравненной к нотариально удостоверенной. Доверенности и заявления хранятся в Секторе по вопросам государственной службы и кадров Комитета в личном деле сотрудника (работника).

5.13. Сектор по вопросам государственной службы и кадров Комитета вправе передавать персональные данные сотрудников (работников) в иные структурные подразделения Комитета в случае необходимости исполнения сотрудниками (работниками) соответствующих структурных подразделений своих служебных (трудовых) обязанностей.

При передаче персональных данных сотрудники Сектора по вопросам государственной службы и кадров Комитета предупреждают лиц, получающих данную информацию, о том, что эти данные могут быть использованы лишь в целях исполнения служебных (трудовых) обязанностей, для которых они получены.

5.14. Передача (обмен) персональных данных между структурными подразделениями Комитета осуществляется только между сотрудниками (работниками), имеющими доступ к персональным данным сотрудников (работников).

5.15. Передача персональных данных сотрудников (работника) третьим лицам осуществляется только с их письменного согласия (приложение № 3), которое должно включать в себя:

фамилию, имя, отчество, адрес сотрудника (работника), номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

наименование и адрес работодателя, получающего согласие сотрудника (работника);

цель обработки персональных данных;

перечень персональных данных, на обработку которых дается согласие сотрудника (работника);

наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Комитета, если обработка будет поручена такому лицу;

перечень действий с персональными данными, на совершение которых дается согласие;

срок, в течение которого действует согласие сотрудника (работника), а также способ его отзыва, если иное не установлено Законом;

подпись сотрудника (работника).

5.16. Не допускается передача персональных данных сотрудника (работника) в коммерческих целях без его письменного согласия (приложение № 4).

5.17. Уполномоченные специалисты, передающие персональные данные сотрудников (работников) третьим лицам, должны передавать их с обязательным составлением Акта приема-передачи документов (иных материальных носителей) (далее – Акт) (приложение № 5), содержащих персональные данные сотрудников (работников). Акт должен содержать следующие условия:

уведомление лица, получающего данные документы об обязанности использования полученной информации, доступ к которой ограничен в соответствии с федеральными законами лишь в целях, для которых она передана;

предупреждение об ответственности за незаконное использование переданной информации, доступ к которой ограничен в соответствии с федеральными законами, в соответствии с законодательством Российской Федерации.

5.18. Предоставление персональных данных сотрудников (работников) государственным органам производится в соответствии с нормами действующего законодательства Российской Федерации и настоящими Правилами.

5.19. Персональные данные сотрудника (работника) могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого сотрудника (работника), за исключением случаев, когда передача персональных данных сотрудника (работника) без его согласия допускается действующим законодательством Российской Федерации.

5.20. Документы, содержащие персональные данные сотрудника (работника), могут быть направлены через сеть почтовой связи Российской Федерации. При этом должна быть обеспечена их конфиденциальность. Документы, содержащие персональные данные сотрудника (работника), вкладываются в конверт, к нему прилагается сопроводительное письмо. На конверте делается надпись о том, что содержимое конверта является информацией, доступ к которой ограничен в соответствии с федеральными законами и за незаконное ее разглашение законодательством предусмотрена ответственность. Далее, конверт с сопроводительным письмом вкладывается в другой конверт, на который наносятся только реквизиты, предусмотренные почтовыми правилами для заказных почтовых отправлений.

6. Организация защиты персональных данных сотрудников (работников)

6.1. Защита персональных данных сотрудников (работников) от неправомерного их использования или утраты обеспечивается Комитетом.

6.2. Общую организацию обработки персональных данных сотрудников (работников) осуществляет главный специалист отдела информационно-компьютерной безопасности Управления информационной безопасности и технической защиты информации Комитета.

6.3. Начальник Сектора по вопросам государственной службы и кадров Комитета обеспечивает:

- ознакомление сотрудников (работников) под роспись с настоящими Правилами;

- получение от сотрудника (работника), замещающего должность, входящую в Перечень государственных гражданских служащих и работников, замещающих должности, не являющиеся должностями государственной гражданской службы, Комитета по информатизации и связи, допущенных к работе с персональными данными, обрабатываемыми в Комитете, письменного обязательства о соблюдении конфиденциальности персональных данных Комитета и соблюдении правил их обработки;

- получение от сотрудника (работника) письменного согласия на обработку его персональных данных;

- получение от сотрудника (работника) письменного согласия на получение его персональных данных у третьей стороны;

- получение письменного согласия сотрудника (работника) на передачу его персональных данных третьей стороне;

- получение письменного согласия сотрудника (работника) на передачу его персональных данных в коммерческих целях.

6.4. Организацию и контроль за защитой персональных данных в структурных подразделениях Комитета, сотрудники (работники) которых имеют доступ к персональным данным, осуществляют их непосредственные руководители.

6.5. Защите подлежат:

- информация о персональных данных сотрудников (работников);

- документы, содержащие персональные данные сотрудников (работников);

- персональные данные сотрудников (работников), содержащиеся на электронных носителях;

- персональные данные лиц, не являющихся сотрудниками (работниками), обрабатываемые Комитетом.

6.6. Ответственность за защиту персональных данных, хранящихся в электронных базах данных, от несанкционированного доступа, искажения и уничтожения информации, а также от иных неправомерных действий несут:

- начальник Сектора по вопросам государственной службы и кадров Комитета в части защиты информации, содержащей персональные данные сотрудников (работников), находящейся в Секторе по вопросам государственной службы и кадров Комитета;

- начальник Финансово-бухгалтерского отдела Комитета в части защиты информации, содержащей персональные данные сотрудников (работников), находящейся в Финансово-бухгалтерском отделе Комитета;

главный специалист Отдела городских телекоммуникаций и развития сетей связи Комитета в части защиты информации, содержащей персональные данные лиц, не являющихся сотрудниками Комитета, находящейся в Отделе городских телекоммуникаций и развития сетей связи Комитета.

ведущий специалист отдела защиты информации и противодействия техническим разведкам Управления информационной безопасности и технической защиты информации Комитета в части защиты информации, содержащей персональные данные сотрудников Комитета по ведению воинского учета, бронированию граждан, пребывающих в запасе и хранению бланков строгой отчетности.

6.7. Техническое обеспечение мероприятий по защите информации, содержащей персональные данные сотрудников (работников), от утечек по техническим каналам связи осуществляет Управление информационной безопасности и технической защиты информации Комитета в соответствии с действующим законодательством Российской Федерации.

7. Заключительные положения

8.1. Лица, виновные в нарушении норм законодательства Российской Федерации, регулирующего обработку и защиту персональных данных Комитета, несут материальную, дисциплинарную, административную и иную ответственность в порядке, установленном действующим законодательством Российской Федерации.

14

Приложение № 1
к Правилам обработки
персональных данных
в Комитете по
информатизации и связи

СОГЛАСИЕ

государственного гражданского служащего (работника, замещающего
должность, не являющуюся должностью государственной гражданской
службы) Комитета по информатизации и связи
на получение его персональных данных у третьей стороны

Председателю Комитета
по информатизации и связи
от _____

(фамилия, имя, отчество, должность)

проживающего по адресу _____

(адрес указывается с почтовым индексом)

паспорт серия _____ № _____

выдан _____

(дата выдачи и наименование органа, выдавшего документ)

Я, _____, согласен на получение моих
персональных данных, а именно: _____

(Ф.И.О. физического лица или наименование организации, у которых получается информация)

О целях, предполагаемых источниках и способах получения персональных
данных, а также о характере подлежащих получению персональных данных
и последствиях отказа дать письменное согласие на их получение, предупрежден.

(дата)

(подпись)

(расшифровка подписи)

Приложение № 2
к Правилам обработки
персональных данных
в Комитете по
информатизации и связи

СОГЛАСИЕ
государственного гражданского служащего (работника, замещающего
должность, не являющуюся должностью государственной гражданской
службы) Комитета по информатизации и связи
на передачу его персональных данных в коммерческих целях

Председателю Комитета
по информатизации и связи
от _____

(фамилия, имя, отчество, должность)

проживающего по адресу _____

(адрес указывается с почтовым индексом)

паспорт серия _____ № _____

выдан _____

(дата выдачи и наименование органа, выдавшего документ)

Я, _____, согласен на передачу моих
персональных данных в коммерческих целях _____

(Ф.И.О. физического лица или наименование организации, которые получают информацию)

О способах передачи моих персональных данных, а также о характере
подлежащих передаче персональных данных и последствиях отказа дать
письменное согласие на их передачу, предупрежден.¹

(дата)

(подпись)

(расшифровка подписи)

¹Письменное согласие государственного гражданского служащего (работника) заполняется и подписывается им собственноручно, в присутствии сотрудника Сектора по вопросам государственной службы и кадров Комитета.

Приложение № 3
к Правилам обработки
персональных данных
в Комитете по
информатизации и связи

СОГЛАСИЕ

государственного гражданского служащего (работника, замещающего
должность, не являющуюся должностью государственной гражданской
службы) Комитета по информатизации и связи
на передачу его персональных данных третьей стороне

Председателю Комитета
по информатизации и связи
от _____

(фамилия, имя, отчество, должность)

проживающего по адресу _____

(адрес указывается с почтовым индексом)

паспорт серия _____ № _____

выдан _____

(дата выдачи и наименование органа, выдавшего документ)

Я, _____

(фамилия, имя, отчество полностью)

согласен на передачу моих персональных данных, а именно: _____

(ф.И.О. физического лица или наименование организации, которые получают информацию)

О целях и способах передачи моих персональных данных,
а также о характере подлежащих передаче персональных данных и последствиях
отказа дать письменное согласие на их передачу, предупрежден.

_____ (дата)

_____ (подпись)

_____ (расшифровка подписи)

17

Приложение № 4
к Правилам обработки
персональных данных
в Комитете по
информатизации и связи

ОБЯЗАТЕЛЬСТВО

государственного гражданского служащего (работника, замещающего должность, не являющуюся должностью государственной гражданской службы) Комитета по информатизации и связи, работника по договору о соблюдении конфиденциальности персональных данных и соблюдении правил их обработки

Председателю Комитета
по информатизации и связи
от _____

(фамилия, имя, отчество, должность)

(наименование структурного подразделения Комитета)

(должность)

Я, _____, в соответствии требованиями Федерального закона «О персональных данных» и в рамках исполнения должностных обязанностей при работе с персональными данными Комитета по информатизации и связи (далее – Комитет) обязуюсь:

не разглашать третьим лицам сведения, содержащие персональные данные Комитета без согласия субъекта персональных данных, которые мне доверены (будут доверены) или станут известными в связи с выполнением должностных обязанностей;

не передавать и не раскрывать третьим лицам сведения, содержащие персональные данные Комитета без согласия субъекта персональных данных, которые мне доверены (будут доверены) или станут известными в связи с выполнением должностных обязанностей;

в случае попытки получить от меня сведения, содержащие персональные данные Комитета, сообщить непосредственному руководителю;

не использовать сведения, содержащие персональные данные Комитета с целью получения выгоды;

выполнять требования нормативных правовых актов, регламентирующих вопросы защиты сведений, содержащих персональные данные Комитета;

после прекращения права на допуск к персональным данным Комитета, в том числе, в случае расторжения служебного контракта или трудового договора, прекратить обработку персональных данных Комитета, не разглашать и не передавать третьим лицам известные мне сведения, содержащие персональные данные Комитета. С Правилами обработки персональных данных Комитета ознакомлен(а).

_____	_____	_____
(дата)	(подпись)	(расшифровка подписи)

Приложение № 5
к Правилам обработки
персональных данных
в Комитете по
информатизации и связи

АКТ

приема-передачи документов (иных материальных носителей), содержащих персональные данные государственного гражданского служащего (работника, замещающего должность, не являющуюся должностью государственной гражданской службы) Комитета по информатизации и связи

Комитет по информатизации и связи (далее — Комитет) в лице _____, действующего на основании _____, с одной стороны, и _____ (далее — _____) в лице _____, действующего на основании _____, с другой стороны, подписали настоящий акт о нижеследующем.

Во исполнение договора № _____ от «___» _____ 20__ г., Комитет передает, а _____ принимает документы (иные материальные носители), содержащие персональные данные государственного гражданского служащего (работника, замещающего должность, не являющиеся должностью гражданской службы) _____ (ФИО) на срок _____ и в целях (указать цель использования): _____.

Перечень документов (иных материальных носителей), содержащих персональные данные государственного гражданского служащего (работника, замещающего должность, не являющиеся должностью гражданской службы)

№ п/п	Наименование	Кол-во
	Всего:	

Полученные персональные данные государственного гражданского служащего (работника, замещающего должность, не являющиеся должностью гражданской службы) могут быть использованы лишь в целях, для которых они заявлены. Незаконное использование предоставленных персональных данных путем их разглашения, уничтожения и другими способами, установленными действующим законодательством, может повлечь соответствующую гражданско-правовую, материальную, дисциплинарную и иную ответственность.

Передал _____
(Ф.И.О., должность должностного лица Комитета, осуществляющего передачу персональных данных государственного гражданского служащего (работника))

Принял _____
(Ф.И.О., должность, представителя лица, принимающего документы (иные материальные носители), содержащих персональные данные государственного гражданского служащего (работника) Комитета)

Приложение № 2
к приказу Комитета
по информатизации и связи
от 11.03.2015 № 34-П

ПОРЯДОК
доступа государственных гражданских служащих
и работников, замещающих должности, не являющиеся должностями
государственной гражданской службы, Комитета по информатизации и связи
в помещения, в которых ведется обработка персональных данных

1.1. Для организации режима обеспечения безопасности помещений, в которых ведется обработка персональных данных в Комитете по информатизации и связи (далее — Комитет), должны быть проведены организационно-технические мероприятия, препятствующие возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения.

1.2. Помещения, в которых размещены Сектор по вопросам государственной службы и кадров Комитета, Финансово-бухгалтерский отдел Комитета, Отдел городских телекоммуникаций и развития сетей связи Комитета и отдел защиты информации и противодействия техническим разведкам Управления информационной безопасности и технической защиты информации Комитета являются помещениями, где обрабатываются и хранятся персональные данные Комитета.

1.3. Начальник Сектора по вопросам государственной службы и кадров Комитета, начальник Финансово-бухгалтерского отдела Комитета, главный специалист Отдела городских телекоммуникаций и развития сетей связи Комитета, ведущий специалист отдела защиты информации и противодействия техническим разведкам Управления информационной безопасности и технической защиты информации Комитета обеспечивают невозможность проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения без присутствия сотрудника (работника), ответственного за обработку персональных данных в данном помещении.

1.4. Ответственность за организацию режима обеспечения безопасности помещений, в которых обрабатываются и хранятся персональные данные Комитета, и правильность использования установленных в нем технических средств несет лицо, которое постоянно в нем работает, и руководитель структурного подразделения Комитета.

1.5. В нерабочее время указанные помещения закрываются на ключ и сдаются под охрану.

1.6. Установка нового оборудования, мебели или их замена, а также ремонт в помещениях должны проводиться в порядке, исключающем нарушения правил обработки персональных данных Комитета.

ПРАВИЛА
осуществления внутреннего контроля соответствия обработки персональных
данных требованиям к защите персональных данных, установленных
Федеральным законом «О персональных данных», принятыми в соответствии
с ним нормативными правовыми актами Российской Федерации и
организационно-распорядительными актами
Комитета по информатизации и связи

1.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в Комитете по информатизации и связи (далее — Комитет) организуют проведение периодических проверок условий обработки персональных данных Комитета.

1.2. Проверки осуществляются ответственным за организацию обработки персональных данных в Комитете (далее — ответственный) либо комиссией, образуемой председателем Комитета.

1.3. В проведении проверки не может участвовать государственный гражданский служащий (далее — сотрудник) и работник, замещающий должность, не являющуюся должностью государственной гражданской службы (далее — работник), Комитета, прямо или косвенно заинтересованный в ее результатах.

1.4. Проверки соответствия обработки персональных данных Комитета установленным требованиям к защите персональных данных проводятся на основании утвержденного ежегодного плана осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям или на основании поступившего в Комитет письменного заявления о нарушениях правил обработки персональных данных (внеплановые проверки). Проведение внеплановой проверки должно быть организовано первым заместителем председателя Комитета в течение трех рабочих дней с момента поступления соответствующего заявления.

1.5. При проведении проверки соответствия обработки персональных данных установленным требованиям должны быть полностью, объективно и всесторонне определены:

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;

порядок и условия применения средств защиты информации;

эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

состояние учета машинных носителей персональных данных;

соблюдение правил доступа к персональным данным;

наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;

мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

осуществление мероприятий по обеспечению целостности персональных данных.

1.6. Ответственный (комиссия) имеют право:

запрашивать у сотрудников Комитета информацию, необходимую для реализации полномочий;

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

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

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

вносить председателю Комитета предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации о персональных данных.

1.7. В отношении персональных данных, ставших известными главному ответственному (комиссии) в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность персональных данных.

1.8. Проверка должна быть завершена не позднее чем через десять рабочих дней со дня принятия решения о ее проведении. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, председателю Комитета докладывает ответственный либо председатель комиссии.

ПРАВИЛА работы с обезличенными данными

1.1. Условия обезличивания персональных данных Комитета по информатизации и связи (далее – Комитет).

1.1.1. Обезличивание персональных данных Комитета может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения класса информационных систем персональных данных и по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено законодательством Российской Федерации.

1.1.2. Обезличивание персональных данных Комитета должно обеспечивать не только их защиту от несанкционированного использования, но и возможность их обработки. Для этого обезличенные персональные данные должны обладать свойствами, сохраняющими основные характеристики обезличиваемых персональных данных.

К свойствам обезличенных персональных данных относятся:

полнота (сохранение всей информации о конкретных субъектах или группах субъектов, которая имелаась до обезличивания);

структурированность (сохранение структурных связей между обезличенными данными конкретного субъекта или группы субъектов, соответствующих связям, имеющимся до обезличивания);

релевантность (возможность обработки запросов по обработке персональных данных и получения ответов в одинаковой семантической форме);

семантическая целостность (сохранение семантики персональных данных при их обезличивании);

применимость (возможность решения задач обработки персональных данных, стоящих перед Комитетом, осуществляющим обезличивание персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ, без предварительного деобезличивания всего объема записей о субъектах);

анонимность (невозможность однозначной идентификации субъектов данных, полученных в результате обезличивания, без применения дополнительной информации).

1.1.3. Способы обезличивания при условии дальнейшей обработки персональных данных:

метод введения идентификаторов (замена части сведений (значений персональных данных) идентификаторами с созданием таблицы (справочника) соответствия идентификаторов исходным данным);

метод изменения состава или семантики, который реализуется путем обобщения, изменения или удаления части сведений, позволяющих идентифицировать субъекта;

метод декомпозиции (разбиение множества (массива) персональных данных на несколько подмножеств (частей) с последующим раздельным хранением подмножеств);

обобщение — понижение точности некоторых сведений (например, «Место жительства» может состоять из страны, индекса, города, улицы, дома и квартиры, а может быть указан только город);

другие способы.

1.1.4. Перечень должностей государственных гражданских служащих и работников, замещающих должности, не являющиеся должностями государственной гражданской службы, Комитета по информатизации и связи, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных в Комитете по информатизации и связи, утверждается приказом Комитета.

1.1.5. Решение о необходимости обезличивания персональных данных принимает председатель Комитета. Руководители структурных подразделений Комитета, непосредственно осуществляющие обработку персональных данных, готовят предложения по обезличиванию персональных данных, обоснование такой необходимости и способ обезличивания. Государственные гражданские служащие (работники, замещающие должности, не являющиеся должностями государственной гражданской службы) Комитета, обслуживающих базы данных с персональными данными, осуществляют непосредственное обезличивание выбранным способом, под контролем первого заместителя председателя Комитета, ответственного за организацию обработки персональных данных.

1.2. Порядок работы с обезличенными персональными данными Комитета.

1.2.1. Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.

1.2.2. Обезличенные персональные данные могут обрабатываться с использованием и без использования средств автоматизации.

1.2.3. При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение:

парольной политики;

антивирусной политики;

правил работы со съемными носителями (если они используются);

правил резервного копирования;

правил доступа в помещения, где расположены элементы информационных систем;

1.2.4. При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:

правил хранения бумажных носителей;

правил доступа к ним и в помещения, где они хранятся.

Приложение № 5
к приказу Комитета
по информатизации и связи
от 19.03.2015 № 37-17

ПРАВИЛА рассмотрения запросов субъектов персональных данных или их представителей

1.1. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

подтверждение факта обработки персональных данных Комитетом по информатизации и связи (далее - Комитет);

правовые основания и цели обработки персональных данных;

способы обработки персональных данных;

наименование и место нахождения оператора, сведения о лицах (за исключением государственных гражданских служащих и работников, замещающих должности, не являющиеся должностями государственной гражданской службы, Комитета), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Комитетом или на основании Закона;

обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен Федеральным законом «О персональных данных»;

сроки обработки персональных данных, в том числе сроки их хранения;

наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Комитета, если обработка поручена или будет поручена такому лицу.

1.2. Субъект персональных данных вправе требовать от Комитета уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные действующим законодательством меры по защите его персональных данных.

1.3. Сведения должны быть предоставлены субъекту персональных данных Комитетом в доступной форме и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

1.4. Сведения предоставляются субъекту персональных данных или его представителю Комитетом по запросу.

Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с Комитетом (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Комитетом, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

1.5. В случае если обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно в Комитет или направить ему повторный запрос в целях ознакомления с такими персональными данными не ранее чем через тридцать дней после направления первоначального запроса, если более короткий срок не установлен Федеральным законом «О персональных данных».

1.6. Субъект персональных данных вправе направить повторный запрос в Комитет в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в пункте 1.5 настоящих Правил, в случае если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального запроса. Повторный запрос наряду со сведениями, указанными в пункте 1.4, должен содержать обоснование направления повторного запроса.

1.7. Комитет вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 1.5 и 1.6. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Комитете.

1.8. От имени субъекта персональных данных может выступать его представитель при наличии нотариально удостоверенной доверенности или доверенности приравненной к нотариально удостоверенной.

ИНСТРУКЦИЯ
о действиях лиц, допущенных к информации,
содержащей персональные данные, в случае возникновения нештатных
ситуаций в Комитете по информатизации и связи

1. Общие положения

1.1. Настоящая инструкция определяет действия государственных гражданских служащих (далее – сотрудники) и работников, замещающих должности, не являющиеся должностями государственной гражданской службы (далее – работники) Комитета по информатизации и связи (далее – Комитет) в случае возникновения нештатных ситуаций в процессе обработки персональных данных в информационных системах персональных данных (далее – ИСПДн).

1.2. Положения инструкции обязательны для исполнения всеми сотрудниками (работниками) в части выполнения вмененных им обязанностей.

1.3. Общими требованиями ко всем сотрудникам (работникам) в случае возникновения нештатной ситуации являются:

сотрудник (работник), обнаруживший нештатную ситуацию, немедленно ставит в известность руководителя структурного подразделения Комитета и администратора информационной безопасности;

администратор информационной безопасности (далее – администратор безопасности) обязан проводить анализ ситуации и, в случае невозможности исправить положение, ставит в известность руководство Комитета. Кроме этого, администратор безопасности для локализации (блокирования) проявлений угроз информационной безопасности может привлекать пользователей ИСПДн, а также уполномоченного сотрудника (работника), ответственного за сопровождение технических средств ИСПДн;

по факту возникновения нештатной ситуации и выяснению причин ее проявления проводится служебная проверка.

2. Действие пользователей ИСПДн
при возникновении нештатных ситуаций

2.1. Сбой программного обеспечения.

2.1.1. Администратор безопасности совместно с сотрудником (работником) Управления информационной безопасности и технической защиты информации Комитета (далее – Управление) выясняют причину сбоя программного обеспечения. Если привести систему в работоспособное состояние своими силами (в том числе после консультаций с разработчиками программного обеспечения) не удалось, копия акта и сопроводительных материалов (а также

файлов, если это необходимо) направляются разработчику программного обеспечения для устранения причин, приведших к сбою. О произошедшем инциденте администратор безопасности сообщает начальнику Управления для принятия решения по существу.

2.2. Отключение электропитания технических средств ИСПДн.

2.2.1. Администратор безопасности совместно с сотрудником (работником) Управления проводят анализ на наличие потерь и (или) разрушения данных и программного обеспечения, а также проверяют работоспособность оборудования. В случае необходимости производится восстановление программного обеспечения и данных из последней резервной копии с составлением акта. О произошедшем инциденте администратор безопасности сообщает начальнику Управления для принятия решения по существу.

2.3. Выход из строя технических средств ИСПДн (серверов, рабочих станций).

2.3.1. Сотрудник (работник) Управления совместно с администратором безопасности выполняют мероприятия по немедленному вводу в действие резервного сервера для обеспечения непрерывной работы ИСПДн (замене рабочей станции).

2.3.2. О выходе из строя сервера (рабочей станции) сотрудник (работник) Управления, ответственный за эксплуатацию сервера (рабочей станции), сообщает начальнику Управления.

2.3.3. При необходимости производится работы по восстановлению программного обеспечения и данных из резервных копий с составлением акта.

2.4. Потеря данных.

2.4.1. При обнаружении потери данных сотрудник (работник) (работник) Управления проводит мероприятия по поиску и устранению причин потери данных (антивирусная проверка, целостность и работоспособность программного обеспечения, целостность и работоспособность оборудования).

2.4.2. При необходимости сотрудник (работник) Управления производится восстановление программного обеспечения и данных из резервных копий с составлением акта. О произошедшем инциденте сотрудник (работник) Управления сообщает администратору безопасности. Администратор безопасности сообщает начальнику Управления для принятия решения по существу.

2.5. Обнаружение вредоносной программы в программной среде средств автоматизации ИСПДн.

2.5.1. При обнаружении вредоносной программы (далее – ВП) производится ее локализация с целью предотвращения ее дальнейшего распространения. При этом зараженная рабочая станция (сервер) физически отсоединяется от локальной вычислительной сети, и сотрудник (работник) Управления и администратором безопасности проводится анализ состояния рабочей станции (сервера).

2.5.2. В результате анализа может быть предпринята попытка сохранения данных, так как после перезагрузки рабочей станции (сервера) данные могут быть потеряны. После успешной ликвидации ВП сохраненные данные подвергаются повторной проверке на наличие ВП. Кроме того, при обнаружении ВП следует руководствоваться инструкцией по эксплуатации применяемого антивирусного программного обеспечения.

2.5.3. После ликвидации ВП проводится внеочередная проверка на всех средствах локальной вычислительной системы с применением обновленных антивирусных баз. При необходимости производится восстановление программного обеспечения и данных из резервных копий с составлением акта.

2.6. Утечка информации.

2.6.1. При обнаружении утечки информации ставится в известность администратор безопасности и начальник Управления. По факту инициируется процедура служебной проверки. Если утечка информации произошла по техническим причинам, проводится анализ защищенности процессов ИСПДн и, если необходимо, принимаются меры по устранению каналов утечки и предотвращению их возникновения.

2.7. Взлом операционной системы средств автоматизации ИСПДн (несанкционированное получение доступа к ресурсам операционной системы).

2.7.1. При обнаружении взлома сервера ставится в известность начальник Управления.

2.7.2. По возможности производится временное отключение сервера от локальной вычислительной сети Комитета для проверки на наличие ВП. Возможен временный переход на резервный сервер.

2.7.3. Сотрудником (работником) Управления проверяется целостность исполняемых файлов в соответствии с хэш-функциями эталонного программного обеспечения. Сотрудником (работником) Управления проводится анализ состояния файлов-скриптов и журналов сервера, производится смена всех паролей, которые имели отношение к данному серверу.

2.7.4. В случае необходимости сотрудником (работником) Управления производится восстановление программного обеспечения и восстановление данных из эталонного архива и резервных копий с составлением акта.

2.7.5. По результатам анализа ситуации проверяется вероятность проникновения несанкционированных программ в локальную вычислительную сеть, после чего проводятся аналогичные работы по проверке и восстановлению программного обеспечения и данных на других информационных узлах ИСПДн.

2.8. Попытка несанкционированного доступа (далее – НСД).

2.8.1. При попытке НСД сотрудником (работником)(работником) Управления и администратором безопасности проводится анализ ситуации на основе информации журналов регистрации попыток НСД и предыдущих попыток НСД. По результатам анализа, в случае необходимости (есть реальная угроза НСД), принимаются меры по предотвращению НСД.

2.8.2. Проводится внеплановая смена паролей. В случае появления обновлений программного обеспечения, устраняющих уязвимости системы безопасности, сотрудником (работником) Управления устанавливаются такие обновления.

2.8.3. В случае установления в ходе служебной проверки факта осуществления попытки НСД со стороны внешних по отношению к ИСПДн субъектов, лицами, уполномоченными на проведение такого расследования, принимаются меры по фиксации и документированию факта инцидента и готовятся материалы для передачи в компетентные органы дознания для проведения предварительного расследования, установления субъекта-нарушителя, определения наличия состава преступления и принятия решения о возбуждении уголовного дела.

2.9. Компрометация ключевой информации (паролей доступа).

2.9.1. При компрометации ключевой информации (пароля доступа) администратором безопасности проводится смена пароля, анализируется ситуация на наличие последствий компрометации и принимаются необходимые меры по минимизации возможного (или нанесенного) ущерба.

2.9.2. О произошедшем инциденте администратор безопасности сообщает начальнику Управления для принятия решения по существу.

2.10. Физическое повреждение или хищение оборудования технических средств ИСПДн.

2.10.1. Сотрудником (работником), обнаружившим физическое повреждение элементов ИСПДн, ставятся в известность: руководитель структурного подразделения Комитета, начальник Управления, руководство Комитета.

2.10.2. Сотрудником (работником) Управления совместно с администратором безопасности проводится анализ с целью оценки возможности утечки или повреждения информации. Определяется причина повреждения элементов ИСПДн и возможные угрозы информационной безопасности.

2.10.3. О факте повреждения элементов ИСПДн сотрудник (работник) Управления докладывает начальнику Управления.

2.10.4. Сотрудником (работником) Управления проводится проверка программного обеспечения на целостность и на наличие ВП, а также проверка целостности данных и анализ электронных журналов.

2.10.5. При необходимости сотрудником (работником) Управления проводятся мероприятия по восстановлению программного обеспечения и данных из резервных копий с составлением акта.

2.11. Невыполнение установленных правил информационной безопасности (правил работы в ИСПДн), использование ИСПДн с нарушением требований, установленных в нормативно-технической и (или) конструкторской документации.

2.11.1. Сотрудником (работником), обнаружившим невыполнение установленных правил ИБ, использование ИСПДн с нарушением требований, установленных в нормативно-технической и (или) конструкторской документации, ставятся в известность: руководитель структурного подразделения Комитета и начальник Управления.

2.11.2. Администратором безопасности проводится анализ с целью оценки возможности утечки или повреждения информации. Определяются возможные угрозы информационной безопасности (далее – ИБ) в результате инцидента.

2.11.3. Об обнаруженном факте администратор безопасности докладывает начальнику Управления.

2.12. Ошибки сотрудников (работников).

2.12.1. В случае возникновения сбоя, связанного с ошибками сотрудников (работников), руководитель подразделения Комитета, в котором произошел инцидент, ставит в известность уполномоченного сотрудника Управления.

2.12.2. Администратором безопасности и сотрудником (работником) Управления проводится анализ с целью оценки возможности утечки или повреждения информации. Определяются возможные угрозы информационной безопасности в результате инцидента и необходимость восстановления программного обеспечения и данных.

2.12.3. При необходимости сотрудником (работником) Управления проводятся мероприятия по восстановлению программного обеспечения и данных из резервных копий с составлением акта.

2.13. Отказ в обслуживании.

2.13.1. Сотрудником (работником), обнаружившим отказ в обслуживании, ставятся в известность: руководитель структурного подразделения Комитета и начальник Управления.

2.13.2. Сотрудником (работником) Управления и администратором безопасности проводится анализ с целью определения причин, вызвавших отказ в обслуживании.

2.13.3. Сотрудником (работником) Управления проводится проверка программного обеспечения на целостность и на наличие ВП, а также проверка целостности данных и анализ электронных журналов.

2.13.4. При необходимости, сотрудником (работником) Управления проводятся мероприятия по восстановлению программного обеспечения и данных из резервных копий с составлением акта.

2.13.5. О причинах инцидента и принятых мерах сотрудник (работник) Управления информирует начальника Управления.

2.14. Несанкционированные изменения состава программных и аппаратных средств (конфигурации) ИСПДн.

2.14.1. В случае обнаружения несанкционированного изменения состава программных и аппаратных средств (конфигурации) ИСПДн администратором безопасности проводится анализ с целью оценки возможности утечки или повреждения информации. Определяются возможные угрозы ИБ в результате инцидента.

2.14.2. Сотрудником (работником) Управления проводятся мероприятия по восстановлению программного обеспечения и данных из резервных копий с составлением акта, а также (при необходимости) проверка на наличие компьютерных ВП.

2.14.3. Об инциденте администратор безопасности докладывает начальнику Управления.

2.15. Техногенные и природные проявления негативных ситуаций.

2.15.1. При стихийном бедствии, пожаре или наводнении, грозящем уничтожению или повреждению информации (данных), сотруднику (работнику), обнаружившему факт возникновения негативной ситуации надлежит:

немедленно оповестить других сотрудников (работников) и принять все меры для самостоятельной оперативной защиты помещения;

немедленно позвонить в соответствующие службы помощи (пожарная охрана, служба спасения и т.д.);

немедленно сообщить своему руководителю структурного подразделения Комитета и администратору безопасности.

2.15.2. После оперативной ликвидации причин, вызвавших пожар или наводнение, назначается внутренняя комиссия по устранению последствий инцидента.

2.15.3. Комиссия определяет ущерб (состав и объем уничтоженных оборудования и информации) и причины, по которым произошло происшествие, а также выявляет виновных.

ИНСТРУКЦИЯ
по порядку учета и хранению съемных машинных носителей информации,
доступ к которой ограничен в соответствии
с федеральными законами, в Комитете по информатизации и связи

1. Общие положения

1.1. Настоящая Инструкция разработана в соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации», ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности» и другими нормативными правовыми актами, и устанавливает порядок использования съемных машинных носителей информации доступ, к которой ограничен в соответствии с федеральными законами, предоставляемых Комитетом по информатизации и связи (далее – Комитет) для использования в информационных системах Комитета.

2. Основные термины, определения и сокращения

2.1. Администратор безопасности ЛВС Смольного – технический специалист, обеспечивает ввод в эксплуатацию, поддержку и последующий вывод из эксплуатации ПО и оборудования вычислительной техники (далее – администратор).

2.2. АРМ – автоматизированное рабочее место пользователя (ПК с прикладным ПО) для выполнения определенной производственной задачи.

2.3. ИБ – информационная безопасность – комплекс организационно-технических мероприятий, обеспечивающих конфиденциальность, целостность и доступность информации.

2.4. ИС – информационная система, обеспечивающая хранение, обработку, преобразование и передачу информации с использованием компьютерной и другой техники.

2.5. Съемный машинный носитель информации – материальный носитель, используемый для записи, хранения и воспроизведения информации, обрабатываемых с помощью средств вычислительной техники.

2.6. ПК – персональный компьютер.

2.7. Паспорт ПК – документ, содержащий полный перечень оборудования и программного обеспечения АРМ.

2.8. ПО – программное обеспечение вычислительной техники.

2.9. ПО вредоносное — ПО или изменения в ПО, приводящие к нарушению конфиденциальности, целостности и доступности критичной информации.

2.10. ПО коммерческое — ПО сторонних производителей (правообладателей). Предоставляется в пользование на возмездной (платной) основе.

2.11. Пользователь — государственный гражданский служащий и работник, замещающий должность, не являющуюся должностью государственной гражданской службы, Комитета, использующий мобильные устройства и машинные носители информации для выполнения своих служебных обязанностей.

3. Порядок использования съемных машинных носителей информации, доступ к которой ограничен в соответствии с федеральными законами (далее — машинные носители информации)

3.1. Под использованием машинных носителей информации в ИС Комитета понимается их подключение к инфраструктуре ИС с целью обработки, приема/передачи информации между ИС и машинными носителями информации.

3.2. В ИС допускается использование только учтенных машинных носителей информации, которые являются собственностью Комитета и подвергаются регулярной ревизии и контролю.

3.3. К предоставленным Комитетом машинным носителям информации предъявляются те же требования ИБ, что и для стационарных АРМ (целесообразность дополнительных мер обеспечения ИБ определяется администратором безопасности).

3.4. Машинные носители информации предоставляются пользователям Комитета по инициативе руководителей структурных подразделений в случаях:
необходимости выполнения вновь принятым пользователем своих должностных обязанностей;
возникновения у пользователей Комитета производственной необходимости.

4. Порядок учета, хранения и обращения с машинными носителями информации, твердыми копиями и их утилизации

4.1. Все находящиеся на хранении и в обращении машинные носители информации в Комитете подлежат учету.

4.2. Каждый машинный носитель информации с записанной на нем информацией должен иметь этикетку, на которой указывается его уникальный учетный номер.

4.3. Учет и выдачу машинных носителей информации осуществляет администратор. Факт выдачи машинного носителя информации фиксируется в журнале учета машинных носителей информации. При увольнении пользователь сдает машинный носитель информации для хранения уполномоченному должностному лицу Комитета, о чем делается соответствующая запись в журнале учета.

4.4. Пользователи Комитета могут получать машинный носитель от уполномоченного должностного лица Комитета для выполнения работ на конкретный срок. При получении и сдаче машинного носителя делаются соответствующие записи в журнале учета.

4.5. При использовании пользователями машинных носителей информации необходимо:

4.5.1. Соблюдать требования настоящей Инструкции.

4.5.2. Использовать машинные носители информации исключительно для выполнения своих служебных обязанностей.

4.5.3. Ставить в известность администраторов о любых фактах нарушения требований настоящей Инструкции.

4.5.4. Бережно относиться к машинным носителям информации.

4.5.5. Обеспечивать физическую безопасность машинных носителей информации всеми разумными способами, в том числе хранением носителя в сейфе.

4.5.6. Извещать администраторов о фактах утраты (кражи) машинных носителей информации.

4.6. При использовании машинных носителей информации запрещено:

4.6.1. Использовать машинные носители информации в личных целях.

4.6.2. Передавать машинные носители информации другим лицам (за исключением администраторов).

4.6.3. Хранить машинные носители информации вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам.

4.6.4. Выносить машинные носители информации из служебных помещений для работы с ними на дому либо в других помещениях (местах).

4.7. Любое взаимодействие (обработка, прием, передача информации), инициированное пользователем Комитета между ИС и неучтенными (личными) носителями информации, рассматривается как несанкционированное (за исключением случаев, оговоренных с администраторами заранее). Администратор оставляет за собой право блокировать или ограничивать использование машинных носителей информации.

4.8. Информация об использовании пользователем Комитета машинных носителей информации в ИС протоколируется и, при необходимости, может быть предоставлена ответственному лицу за организацию обработки персональных данных в Комитете.

4.9. В случае выявления фактов несанкционированного и/или нецелевого использования машинных носителей информации инициируется служебная проверка, проводимая комиссией, состав которой утвержден председателем Комитета.

4.10. По факту выявленных обстоятельств составляется акт расследования инцидента и передается председателю Комитета для принятия мер согласно действующему законодательству.

4.11. Информация, хранящаяся на машинных носителях информации, подлежит обязательной проверке на отсутствие вредоносного ПО.

4.12. При отправке или передаче информации адресатам на машинные носители информации записываются только предназначенные адресатам данные. Отправка информации адресатам на машинных носителях информации

осуществляется в порядке, установленном для документов для служебного пользования.

4.13. Вынос машинных носителей информации для непосредственной передачи адресату осуществляется только с письменного разрешения руководителя структурного подразделения.

4.14. В случае утраты или уничтожения машинных носителей информации либо разглашения содержащихся в них сведений, об этом немедленно ставится в известность руководитель соответствующего структурного подразделения. По факту утраты носителя составляется акт. Соответствующие отметки вносятся в журналы учета машинных носителей информации.

4.15. Машинные носители информации, пришедшие в негодность или отслужившие установленный срок, подлежат уничтожению. Уничтожение машинных носителей информации осуществляется уполномоченной комиссией. По результатам уничтожения машинных носителей информации составляется акт согласно приложению к инструкции.

4.16. В случае увольнения или перевода пользователя в другое структурное подразделение, предоставленные ему машинные носители информации изымаются.

5. Ответственность

5.1. Пользователи, нарушившие требования настоящей Инструкции, несут ответственность в соответствии с действующим законодательством.

Приложение
к Инструкции по порядку учета
и хранению машинных носителей
информации, доступ к которой ограничен
в соответствии с федеральными законами
в Комитете по информатизации и связи

АКТ²
об уничтожении (машинных, бумажных) носителей информации,
доступ к которой ограничен в соответствии с федеральными законами

Комиссия в составе:

Председатель — _____

Члены комиссии — _____

провела отбор (машинных, бумажных) носителей информации, доступ
к которой ограничен в соответствии с федеральными законами и установила,
что в соответствии с требованиями руководящих документов по защите
информации

_____ информация, записанная
на них в процессе эксплуатации, подлежит гарантированному уничтожению:

№ п/п	Дата	Тип носителя	Регистрационный номер носителя ПДн	Кол-во	Примечание

Всего (машинных, бумажных) носителей

_____ (цифрами и прописью)

На указанных носителях информация, доступ к которой ограничен
в соответствии с федеральными законами уничтожена путем

_____ (стирания на устройстве гарантированного уничтожения информации и т.п.)

Перечисленные материальные носители информации, доступ к которой
ограничен в соответствии с федеральными законами уничтожены путем

_____ (разрезания, сжигания, механического уничтожения и т.п.)

Председатель комиссии: _____ / _____ /

Члены комиссии: _____ / _____ /

²Примечание:

1. Акт составляется отдельно на каждый способ уничтожения машинных носителей.
2. Все листы акта, а также все произведенные исправления и дополнения в акте заверяются подписями всех членов комиссии.

ИНСТРУКЦИЯ

**о порядке резервного копирования и восстановления работоспособности
технических средств и программного обеспечения, баз данных и средств
защиты информации информационных систем персональных данных
в Комитете по информатизации и связи**

1. Назначение и область действия

Порядок резервного копирования и восстановления работоспособности технических средств (далее — ТС) и программного обеспечения (далее — ПО), баз данных и средств защиты информации (далее — СЗИ) определяет действия (далее — Инструкция), связанные с функционированием информационных систем персональных данных (далее — ИСПДн) в Комитете по информатизации и связи (далее — Комитет), меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн.

Целью настоящего документа является превентивная защита элементов ИСПДн от предотвращения потери защищаемой информации.

Задачей данной Инструкции является:

определение мер защиты от потери информации;

определение действий восстановления в случае потери информации.

Действие настоящей Инструкции распространяется на всех государственных гражданских служащих и работников, замещающих должности, не являющиеся должностями государственной гражданской службы Комитета (далее — пользователи), имеющих доступ к ресурсам ИСПДн, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

системы жизнеобеспечения;

системы обеспечения отказоустойчивости;

системы резервного копирования и хранения данных;

системы контроля физического доступа.

Пересмотр настоящего документа осуществляется по мере необходимости, но не реже одного раза в два года.

Ответственным за реагирование на инциденты безопасности, приводящие к потере защищаемой информации, назначается администратор безопасности ИСПДн Комитета.

Ответственным за контроль обеспечения мероприятий по предотвращению инцидентов безопасности, приводящих к потере защищаемой информации, назначается ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных Комитета.

2. Порядок реагирования на инцидент

В настоящем документе под инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн, а также потерей защищаемой информации.

Происшествие, вызывающее инцидент, может произойти:
в результате непреднамеренных действий пользователей;
в результате преднамеренных действий пользователей и третьих лиц;
в результате нарушения правил эксплуатации технических средств ИСПДн;
в результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

В кратчайшие сроки, не превышающие одного рабочего дня, администратор безопасности ИСПДн и оператор ИСПДн предпринимают меры по восстановлению работоспособности информационной системы. Предпринимаемые меры по возможности согласуются с вышестоящим руководством.

3. Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов

3.1. Технические меры

К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения Инцидентов, такие как:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

Системы жизнеобеспечения ИСПДн включают:

- пожарные сигнализации и системы пожаротушения;
- системы вентиляции и кондиционирования;
- системы резервного питания.

Все критичные помещения Комитета (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ИСПДн в помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха.

Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

- локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;

источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;

дублированные системы электропитания в устройствах (серверы, концентраторы, мосты и т. д.);

резервные линии электропитания в пределах комплекса зданий;

аварийные электрогенераторы;

системы обеспечения отказоустойчивости;

кластеризация;

технология RAID.

Для обеспечения отказоустойчивости критичных компонентов ИСПДн при сбое в работе оборудования и их автоматической замены без простоев должны использоваться методы кластеризации. Могут использоваться следующие методы кластеризации: для наиболее критичных компонентов ИСПДн должны использоваться территориально удаленные системы кластеров. Для защиты от отказов отдельных дисков серверов, осуществляющих обработку и хранение защищаемой информации, должны использоваться технологии RAID, которые (кроме RAID-0) применяют дублирование данных, хранимых на дисках.

Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на твердый носитель (ленту, жесткий диск и т.п.).

3.2 Организационные меры

Резервное копирование и хранение данных должно осуществляться на периодической основе:

для обрабатываемых персональных данных – не реже раза в неделю;

для технологической информации – не реже раза в месяц;

эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИСПДн – не реже раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

Данные о проведении процедуры резервного копирования, должны отражаться в специально созданном журнале учета согласно приложению.

Носители, на которые произведено резервное копирование, должны быть пронумерованы: номером носителя, датой проведения резервного копирования.

Носители должны храниться в негорючем шкафу или помещении оборудованном системой пожаротушения.

Носители должны храниться не менее года, для возможности восстановления данных.

4. Ответственность

Ответственность за поддержание установленного в настоящей Инструкции порядка проведения резервного копирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных возлагается на администратора безопасности ИСПДн Комитета.

Приложение
к Инструкции о порядке резервного
копирования и восстановления
работоспособности технических средств
и программного обеспечения, баз данных
и средств защиты информации
информационных систем персональных
данных в Комитете по информатизации
и связи

ЖУРНАЛ
учета записей резервных копий

№ записи	ИСПДн	Дата создания резервной копии	Наименование носителя	ФИО, должность лица, осуществившего резервное копирование	Подпись должностного лица, осуществившего резервное копирование

ИНСТРУКЦИЯ
ответственного за организацию обработки персональных данных
в Комитете по информатизации и связи

1. Инструкция ответственного за организацию обработки персональных данных (далее – Инструкция) разработана в соответствии с Федеральным законом «О персональных данных», Федеральным законом «О порядке рассмотрения обращений граждан Российской Федерации», Постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», другими нормативными правовыми актами.

2. Инструкция определяет ответственность, обязанности и права лица, назначенного ответственным за организацию обработки персональных данных.

3. Ответственный за организацию обработки персональных данных отвечает за осуществление внутреннего контроля за соблюдением законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных, доведение до сведений государственных гражданских служащих (сотрудников) и работников, замещающих должности, не являющиеся должностями государственной гражданской службы (работников), Комитета по информатизации и связи (далее – Комитет) положений законодательства Российской Федерации о персональных данных, правовых актов Комитета по вопросам обработки персональных данных, требований к защите персональных данных, организации приема и обработки обращений и осуществлению контроля за приемом и обработкой таких обращений.

4. Ответственный за организацию обработки персональных данных обязан:

определить 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;

определять порядок и условия применения средств защиты информации;

анализировать эффективность применения мер по обеспечению безопасности персональных данных;

контролировать состояние учета машинных носителей персональных данных;

проверять соблюдение правил доступа к персональным данным;
контролировать проведение мероприятий по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

обеспечивать конфиденциальность персональных данных, ставших известными в ходе проведения мероприятий внутреннего контроля.

5. Ответственный за организацию обработки персональных данных имеет право:

осуществлять проверки по контролю соответствия обработки персональных данных требованиям к защите персональных данных;

запрашивать у сотрудников (работников) информацию, необходимую для реализации полномочий;

требовать от ответственных за обработку персональных данных уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

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

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

вносить председателю Комитета предложения о привлечении к дисциплинарной ответственности сотрудников (работников) Комитета, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

Приложение № 10
к приказу Комитета
по информатизации и связи
от 11.03.2015 № 24-17

ИНСТРУКЦИЯ

**пользователя персонального компьютера при работе в локальной
вычислительной сети Смольного в Комитете по информатизации и связи**

1. Общие положения

Целью настоящей Инструкции является регулирование работы пользователей персональных компьютеров при работе в локальной вычислительной сети Смольного (далее – сеть), а также распределении сетевых ресурсов коллективного пользования и поддержания необходимого уровня защиты информации, ее сохранности и соблюдения прав доступа. Инструкция содержит необходимые требования по обеспечению совместной работы, более эффективному использованию сетевых ресурсов и уменьшению риска неправомерного их использования.

1.1. Государственному гражданскому служащему и работнику, замещающему должность, не являющуюся должностью государственной гражданской службы в Комитете по информатизации и связи (далее – Комитет) (далее – пользователь) разрешена работа только на определенных компьютерах, в определенное регламентом время и только с разрешенными программами и сетевыми ресурсами.

1.2. Пользователь подключенного к сети компьютера – лицо, за которым закреплена ответственность за данный компьютер. Пользователь должен принимать все необходимые меры по защите информации и контролю прав доступа к компьютеру;

1.3. Каждый пользователь использует индивидуальное «имя пользователя» для своей идентификации в сети, выдаваемое службой технической поддержки в соответствии с заявкой.

1.4. Каждый пользователь самостоятельно задает пароль для входа в компьютерную сеть. При этом пароль должен содержать не менее 6 символов и состоять из букв и цифр. Рекомендации по использованию пароля приведены в Приложении к настоящей Инструкции. Консультацию по использованию пароля можно получить в Управлении информационной безопасности и технической защиты информации Комитета по информатизации и связи (далее – Управление).

1.5. Каждый пользователь должен использовать только свое имя пользователя и пароль для входа в компьютер, локальную сеть и сеть Интернет (если данный ресурс подключен). Передача имени пользователя и пароля третьим лицам, за исключением специалистов Управления для решения служебных задач, категорически запрещена.

1.6. В случае появления у пользователя сведений или подозрений о фактах нарушения настоящих правил, а в особенности о фактах

несанкционированного удаленного доступа к информации, размещенной на контролируемом им компьютере, или на каком-либо другом, пользователь должен немедленно сообщить об этом в Управление, сотруднику (работнику), назначенному ответственным за защиту информации (далее — специалист, ответственный за защиту информации).

1.7. Специалист, ответственный за защиту информации, — лицо, следящее за правильным функционированием сети и комплексной защитой обрабатываемой информации. Специалист, ответственный за защиту информации, вправе ограничивать доступ к некоторым сетевым ресурсам вплоть до их полной блокировки, изменять распределение трафика и проводить другие меры, направленные на обеспечение безопасности информации и повышение эффективности использования сетевых ресурсов.

1.8. Специалист, ответственный за защиту информации, имеет право отключить компьютер пользователя от сети в случае, если с данного компьютера производились попытки несанкционированного доступа к информации на других компьютерах, и в случаях других серьезных нарушений настоящей инструкции.

1.9. Управление информирует пользователей, посредством уведомления через электронную почту, обо всех плановых профилактических работах, которые могут привести к частичной или полной неработоспособности сети на ограниченное время, а также об изменениях предоставляемых сервисов и ограничениях, накладываемых на доступ к ресурсам сети;

1.10. Пользователь должен ознакомиться с настоящей Инструкцией. Обязанность ознакомления пользователя с Инструкцией лежит на специалисте, ответственном за защиту информации, и на руководителе структурного подразделения.

2. Работа за компьютером

2.1. Запрещено самостоятельно вскрывать компьютер и вынимать его комплектующие. При возникновении неисправностей необходимо обратиться в службу технической поддержки.

2.2. Все кабели, соединяющие системный блок с другими устройствами, следует вставлять (вынимать) только при выключенном компьютере. Исключение составляют USB-устройства, они могут быть подключены к включенному компьютеру.

2.3. Запрещено самостоятельно устанавливать, удалять, деактивировать и изменять программное обеспечение на компьютере.

2.4. Запрещено аварийно завершать работу компьютера кнопкой «Reset» или отключением от электросети. Необходимо корректно завершать работу компьютера, через кнопку «Пуск» в панели задач. В случае невозможности корректного завершения работы компьютера обращаться в Управление.

2.5. Запрещено подвергать компьютер и периферийные устройства физическим, термическим и химическим воздействиям.

2.6. Перед началом работы пользователь должен:

включить выключатель сетевого фильтра. При включении кнопка должна начать светиться;

включить источник бесперебойного питания (ИБП) и выждать 5 секунд (если установлен ИБП);

включить монитор (если выключен);
включить компьютер кнопкой «Power». Дождаться загрузки операционной системы (ОС);

войти в систему, используя свои личные имя пользователя и пароль.

2.7. По завершении рабочего дня компьютер необходимо выключить и обесточить, для этого пользователь должен:

закрыть все открытые программы и документы, сохранив нужные изменения;

с помощью меню «Пуск – Завершение работы» выключить компьютер и дождаться завершения работы;

выключить монитор;

выключить ИБП, нажав кнопку на передней панели (если установлен ИБП);

выключить сетевой фильтр.

2.8. При отключении электроэнергии ИБП позволяет компьютеру оставаться в рабочем состоянии до 5-10 минут. При отключении электроэнергии в помещении пользователь должен в немедленном порядке провести выключение компьютера в соответствии с пунктом 2.7. Инструкции.

3. Общие правила работы в локальной вычислительной сети Смольного

3.1. Пользователи сети обязаны:

3.1.1. Соблюдать правила работы в сети, оговоренные настоящей Инструкцией.

3.1.2. При доступе к внешним ресурсам сети, соблюдать правила, установленные Управлением, для используемых ресурсов.

3.1.3. При уходе с рабочего места, необходимо активизировать средства защиты от несанкционированного доступа к информации при помощи сочетания клавиш «Ctrl+Alt+Del» и выбрав пункт «Блокировка».

3.1.3. Немедленно сообщать в Управление об обнаруженных проблемах в использовании предоставленных ресурсов, а также о фактах нарушения настоящей инструкции. Управлением проводится расследование указанных фактов и принимаются соответствующие меры.

3.1.4. Не разглашать известную конфиденциальную информацию (имя пользователя и пароль), необходимую для безопасной работы в сети.

3.1.5. Выполнять предписания специалиста, ответственного за защиту информации, направленные на обеспечение безопасности сети.

3.1.6. В случае обнаружения неисправности компьютерного оборудования или программного обеспечения, пользователь должен обратиться в службу технической поддержки.

3.2. Пользователи сети имеют право:

3.2.1. Использовать в работе предоставленные им сетевые ресурсы в оговоренных в настоящей инструкции рамках, если иное не предусмотрено по согласованию с Управлением.

3.2.2. Обращаться за помощью в Управление при решении задач с использованием ресурсов сети.

3.2.3. Вносить предложения по улучшению работы с тем или иным ресурсом.

3.3. Пользователям сети запрещено:

3.3.1. Использовать любые программы, не предназначенные для выполнения прямых служебных обязанностей.

3.3.2. Разрешать посторонним лицам пользоваться вверенным пользователю компьютером (кроме случаев подключения/отключения ресурсов, выполняемого специалистами службы технической поддержки по заявке, согласованной с Управлением).

3.3.3. Самостоятельно устанавливать или удалять установленные программы на компьютерах, подключенных к сети, изменять настройки операционной системы и приложений, влияющие на работу сетевого оборудования и сетевых ресурсов.

3.3.4. Повреждать, уничтожать или фальсифицировать информацию, не принадлежащую пользователю.

3.3.5. Вскрывать сетевое и периферийное оборудование; подключать к компьютеру дополнительное оборудование без согласования с Управлением, изменять настройки BIOS, а также производить загрузку рабочих станций с дискет и других носителей.

3.3.6. Самовольно подключать компьютер к сети, а также изменять настройки сети компьютера. Подключение к сети оборудования, не принадлежащего Комитету, категорически запрещено, так как создает угрозу безопасности информации.

3.3.7. Получать и передавать в сеть информацию, противоречащую действующему законодательству Российской Федерации, представляющую служебную или государственную тайну, а также конфиденциальную информацию, в том числе персональные данные.

3.3.8. Использовать иные формы доступа к информационно-телекоммуникационной сети «Интернет», за исключением способов, разрешенных Управлением.

3.3.9. Осуществлять попытки несанкционированного доступа к ресурсам сети, проводить или участвовать в сетевых атаках и сетевом взломе.

4. Работа с электронной почтой

4.1. Электронная почта предоставляется пользователю только для выполнения своих прямых служебных обязанностей по служебной записке руководителя соответствующего структурного подразделения Комитета. Использование ее в личных целях запрещено. Создание почтового ящика проводится службой технической поддержки по заявке, согласованной с Управлением.

4.2. Комитет оставляет за собой право получить доступ к электронной почте пользователей. Содержимое электронного письма не может быть раскрыто, кроме как с целью обеспечения безопасности или по требованию правоохранительных органов.

4.3. Исходящие сообщения могут быть выборочно проверены, чтобы гарантировать соблюдение политики безопасности.

4.4. Использование электронной почты третьими лицами запрещено.

4.5. В качестве клиентов электронной почты могут использоваться только согласованные Управлением почтовые программы.

5. Работа в информационно-телекоммуникационной сети «Интернет»

5.1. Доступ к информационно-телекоммуникационной сети «Интернет» для пользователей предоставляется по служебной записке руководителя соответствующего структурного подразделения Комитета и только на выделенных для работы с Интернет ресурсом персональных компьютерах.

5.2. Пользователи используют поиск информации в информационно-телекоммуникационной сети «Интернет» только в случае, если это необходимо для выполнения своих должностных обязанностей.

5.3. По использованию Интернет ведется статистика, которая хранится на электронных носителях на Узле телематических служб Смольного.

5.4. Действия любого пользователя, подозреваемого в нарушении правил пользования Интернетом, могут быть заархивированы и использоваться для принятия решения о применении к нему санкций.

5.5. Пользователям, пользующимся Интернетом, запрещено передавать или загружать на компьютер материал, который является непристойным, порнографическим или нарушает действующее законодательство Российской Федерации.

5.6. Программное обеспечение, используемое для работы в информационно-телекоммуникационной сети «Интернет», должно быть согласовано с Управлением.

5.7. При необходимости переноса рабочих материалов, полученных из информационно-телекоммуникационной сети «Интернет», на персональный компьютер пользователя, требуется их проверка при помощи антивирусных программ, согласно Инструкции по организации антивирусной защиты в Комитете по информатизации и связи.

5.8. Пользователи, должны соблюдать эту политику после предоставления им доступа к информационно-телекоммуникационной сети «Интернет».

6. Ответственность

6.1. Пользователь отвечает за информацию, хранящуюся на его компьютере, технически исправное состояние компьютера и вверенной техники.

6.2. Пользователь несет личную ответственность за весь информационный обмен между его компьютером и другими компьютерами в сети и за ее пределами.

6.3. Узел телематических служб Смольного отвечает за бесперебойное функционирование вверенной ему сети, качество предоставляемых пользователям сервисов.

6.4. За нарушение настоящей инструкции пользователь может быть отстранен от работы в сети.

Приложение
к Инструкции пользователя
персонального компьютера при работе
в локальной вычислительной сети
Смольного в Комитете
по информатизации и связи

РЕКОМЕНДАЦИИ по использованию пароля

1. Пароль должен включать в себя алфавитно-цифровые символы. Рекомендуется использовать буквы латинского алфавита. Кроме алфавитно-цифровых символов разрешается использовать, например, символы знаков препинания.
2. Минимальная длина пароля не должна быть менее 6 (шести) символов.
3. Пароль меняется не реже 1 раза в 30 дней.
4. Разрешается не более 6 попыток неверного ввода пароля.
5. Последние 6 паролей не должны повторяться.
6. Пароль для подключения к локальной сети должен регулярно обновляться самим пользователем.
7. Смена пароля пользователя осуществляется после входа в систему под своей учетной записью при помощи комбинации клавиш - Ctrl+Alt+Delete, а затем нажатием кнопки «Смена пароля» и действий в соответствии с предлагаемым алгоритмом (Ввод старого пароля, ввод нового пароля и его подтверждение).

ИНСТРУКЦИЯ
пользователя автоматизированной системы обработки
конфиденциальной информации и персональных данных
в Комитете по информатизации и связи

1. Общие положения

1.1. Настоящая Инструкция разработана для обеспечения защиты конфиденциальной информации, в том числе персональных данных, в автоматизированных системах, используемых в Комитете по информатизации и связи (далее – Комитет).

Конфиденциальная информация – информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

1.2. Наиболее вероятными каналами утечки информации для автоматизированных систем (далее – АС) являются:

несанкционированный доступ к информации, обрабатываемой в автоматизированной системе;

хищение технических средств, с хранящейся в них информацией, или отдельных носителей информации;

просмотр информации с экранов дисплеев мониторов и других средств ее отображения с помощью оптических устройств;

воздействие на технические или программные средства в целях нарушения целостности (уничтожения, искажения) информации, работоспособности технических средств, средств защиты информации, адресности и своевременности обмена, в том числе электромагнитного, через специально внедренные электронные и программные средства («закладки»).

1.3. Работа с конфиденциальной информацией, персональными данными, а также со служебными документами ограниченного распространения (далее – информация ограниченного распространения), строится на следующих принципах:

принцип персональной ответственности – в любой момент времени за каждый документ (не зависимо от типа носителя: бумажный, электронный) должен отвечать и распоряжаться конкретный сотрудник, выдача документов осуществляется под роспись;

принцип контроля и учета – все операции с документами должны отражаться в соответствующих журналах и карточках (передача из рук в руки, снятие копии и т.п.).

2. Обязанности государственных гражданских служащих и работников, замещающих должности, не являющиеся должностями государственной гражданской службы, имеющих доступ к конфиденциальной информации

2.1. Государственные гражданские служащие (далее – сотрудники) и работники, замещающие должности, не являющиеся должностями государственной гражданской службы (далее – работники), получившие доступ к конфиденциальной информации, обязаны хранить в тайне данные сведения, ставшие им известными во время работы или иным путем и пресекать действия других лиц, которые могут привести к разглашению такой информации. О таких фактах, а также о других причинах или условиях возможной утечки информации немедленно информировать руководителя структурного подразделения Комитета, специалиста по защите информации.

Конфиденциальная информация не подлежит разглашению. Прекращение доступа к такой информации не освобождает сотрудника (работника) от взятых им обязательств по неразглашению сведений ограниченного распространения.

В случае оставления занимаемой должности сотрудник (работник) обязан вернуть все документы и материалы, относящиеся к деятельности подразделения, организации. В том числе отчеты, инструкции, переписку, списки сотрудников (работников), компьютерные программы, а также все прочие материалы и копии названных материалов, имеющих какое-либо отношение к деятельности администрации, полученные в течение срока работы.

2.2. Сотрудники (работники) при работе с конфиденциальной информацией обязаны:

- строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами АС;

- выполнять требования специалиста по защите информации, касающиеся обеспечения информационной безопасности;

- знать и строго выполнять правила работы со средствами защиты информации (средствами разграничения доступа), используемыми на персональных компьютерах;

- хранить в тайне свой аутентификатор (пароль доступа в автоматизированную систему), а также информацию о системе защиты, установленной на АС;

- использовать для работы, только учтенные съемные накопители информации (гибкие магнитные диски, карты памяти, компакт диски и т.д.);

- контролировать обновление антивирусных баз и в случае необходимости сообщать о необходимости обновления в службу технической поддержки и специалисту по защите информации, ответственному за антивирусную защиту автоматизированной системы;

- немедленно ставить в известность руководителя структурного подразделения Комитета, сотрудников (работников) Управления информационной безопасности и технической защиты информации Комитета (далее – Управление):

в случае утери посетителя с конфиденциальной информацией или при подозрении компрометации личных ключей и паролей;

нарушений целостности пломб (наклеек с защитной и идентификационной информацией, нарушении или несоответствии номеров печатей) на аппаратных средствах ПЭВМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа (далее - НСД) к защищенной АС;

несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств АС.

В случае отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию рабочей станции, выхода из строя или неустойчивого функционирования узлов ПЭВМ или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения, некорректного функционирования установленных в автоматизированной системе технических средств защиты ставить в известность ответственного за техническое обслуживание и (или) ответственного за обслуживание программного обеспечения.

2.3. Ставить в известность сотрудников (работников) Управления при:

необходимости обновления антивирусных баз;

обновлении программного обеспечения;

проведении регламентных работ, модернизации аппаратных средств или изменении конфигурации АС;

необходимости вскрытия системных блоков персональных компьютеров входящих в состав АС;

резервном копировании информации.

2.4. Уборка помещений должна производиться под контролем сотрудника, имеющего доступ в помещение и постоянно в нем работающего.

Вынос ПЭВМ, на которой проводилась обработка конфиденциальной информации, за пределы территории здания с целью их ремонта, замены и т. п. без согласования с Управлением запрещен. При принятии решения о выносе компьютеров, жесткие магнитные диски должны быть демонтированы и сданы на хранение ответственному за учет служебных документов ограниченного распространения структурного подразделения. В случае действия гарантийных обязательств фирмы-поставщика вскрытие корпуса и демонтаж носителей должны быть предварительно согласованы.

ПЭВМ, используемые для работы с конфиденциальной информацией, должны быть размещены таким образом, чтобы исключалась возможность визуального просмотра экрана видеомонитора, не имеющими отношения к конкретно обрабатываемой информации сотрудниками.

2.5. Запрещается:

передать, кому бы то ни было (в том числе родственникам) устно или письменно конфиденциальную информацию;

использовать конфиденциальную информацию при подготовке открытых публикаций, докладов, научных работ и т.д.;

выполнять работы с документами, содержащими конфиденциальную информацию на дому, выносить их из служебных помещений, снимать копии или производить выписки из таких документов без разрешения руководителя;

накапливать ненужную для работы конфиденциальную информацию, при работе с персональными данными, соблюдать сроки ее хранения;

передавать или принимать без расписки документы, содержащие конфиденциальную информацию и персональные данные;

оставлять на рабочих столах, в столах и незакрытых сейфах документы, содержащие конфиденциальную информацию, а также оставлять незапертыми и не опечатанными после окончания работы сейфы, помещения и хранилища с документами.

использовать компоненты программного и аппаратного обеспечения АС подразделения в неслужебных целях;

самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств рабочих станций или устанавливать дополнительно любые программные и аппаратные средства;

осуществлять обработку конфиденциальной информации в присутствии посторонних (не допущенных к данной информации) лиц;

записывать и хранить конфиденциальную информацию на неучтенных носителях информации (картах памяти и т.п.);

оставлять включенной без присмотра свою рабочую станцию (ПЭВМ), не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);

умышленно использовать недокументированные свойства и опибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок - ставить в известность специалистов службы технической поддержки и Управление.

3. Ответственность

Сотрудник (работник) несет ответственность за соблюдение требований настоящей инструкции, а также других документов в области защиты информации.

За разглашение конфиденциальной информации, персональных данных, а также служебной тайны, нарушение порядка работы с документами или машинными носителями, содержащими такую информацию, сотрудники могут быть привлечены к дисциплинарной или иной, предусмотренной действующим законодательством ответственности.

ИНСТРУКЦИЯ по организации антивирусной защиты в Комитете по информатизации и связи

1. Общие положения

Настоящая Инструкция определяет требования к организации защиты информации, обрабатываемой на компьютерах в Комитете по информатизации и связи (далее – Комитет), от разрушающего воздействия компьютерных вирусов и устанавливает ответственность государственного гражданского служащего (далее – сотрудник) и работника, замещающего должность, не являющуюся должностью гражданской службы в Комитете (далее – работник), за ее выполнением.

2. Установка и обновление антивирусных средств

2.1. К использованию на компьютерах сотрудников Комитета допускаются только лицензионные антивирусные средства.

2.2. Установка и настройка средств антивирусного контроля на компьютерах осуществляется специалистами службы технической поддержки Смольного.

2.3. Обновление средств антивирусного контроля осуществляется автоматически.

3. Применение средств антивирусного контроля

3.1. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях. Контроль информации на съемных носителях производится непосредственно перед ее использованием.

3.2. Все жесткие диски персональных компьютеров проверяются на наличие вирусов системой антивирусной защиты в автоматическом режиме не реже одного раза в неделю.

3.3. Файлы, помещаемые в электронный архив (на сервер), должны в обязательном порядке проходить антивирусный контроль.

3.4. Особое внимание следует обратить на недопустимость использования съемных носителей, принадлежащих лицам, временно допущенным к работе на компьютере в Комитете (обучающиеся, участники совещаний, студенты-практиканты и т.п.). Работа этих лиц должна проводиться

под непосредственным контролем сотрудника или ответственного за информационную безопасность, особенно если работа происходит с использованием ресурсов локальной вычислительной сети.

3.5. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) сотрудник структурного подразделения самостоятельно должен провести внеочередной антивирусный контроль компьютера и сообщить в службу технической поддержки Смольного.

4. Действия сотрудников (работников) при обнаружении компьютерного вируса

4.1. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники (работники) подразделений обязаны:

- приостановить работу;

- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов службу технической поддержки Смольного;

- совместно с владельцем зараженных вирусом файлов специалисты службы технической поддержки должны провести анализ необходимости дальнейшего их использования;

- провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь специалистов службы технической поддержки).

5. Контроль

5.1. Контроль за проведением мероприятий антивирусного контроля в локальной вычислительной сети Смольного и соблюдение требований настоящей Инструкции осуществляется Управлением.

5.2. Периодический контроль за соблюдением положений настоящей Инструкции возлагается на начальника Управления.

Приложение № 13
к приказу Комитета
по информатизации и связи
от 14.03.15 № 31-П

ПЕРЕЧЕНЬ
информационных систем персональных данных (ИСПДн) Комитета по информатизации и связи,
в которых должна быть обеспечена безопасность информации

№ п/п	Наименование ИСПДн (ее составной части)	Наименование объекта (полное и сокращенное) Отраслевая (ведомственная) принадлежность объекта	Исходные данные классификации ИСПДн по требованиям защиты информации										Примечание
			Категория персональных данных	персональные данные	сотрудников оператора	Количество персональных данных, содержащихся в информационной системе	Тип угрозы, актуальных для информационной системы	Масштаб	Степень возможного ущерба	Уровень значимости информации (УЗ)	Класс защищенности	Уровень защищенности	
1.	«Бухгалтерия»	Комитет по информатизации и связи (КИС), Смольный, Санкт-Петербург, 191060	иные	персональные данные	сотрудников оператора	менее 100000	Угрозы 3 типа	объектовый	низкая	4-й	К-3	УЗ-3	

№ п/п	Наименование ИСПДн (ее составной части)	Наименование объекта и (полное и сокращенное) Отраслевая (ведомственная) принадлежность	Исходные данные классификации ИСПДн по требованиям защиты информации									Примечание
			Категория персональных данных	Прината/уязвимость персональных данных	Количество персональных данных, содержащихся в информационной системе	Тип угрозы, актуальных для информационной системы	Масштаб	Степень возможного ущерба	Уровень значимости информации (УЗ)	Класс защищенности	Уровень защищенности	
2.	Автоматизированная информационная система «Управление персоналом государственных органов» в исполнительных органах государственной власти Санкт-Петербурга	Комитет по информатизации и связи (КИС), Смольный, Санкт-Петербург, 191060	иные	персональные данные сотрудников оператора	менее 100000	Угрозы 3 типа	объектовый	низкая	4-й	К-3	УЗ-3	

№ п/п	Наименование ИСПДн (ее составной части)	Наименование объекта (полное и сокращенное) Отраслевая (ведомственная) принадлежность объекта	Исходные данные классификации ИСПДн по требованиям защиты информации									Примечание
			Категория персональных данных	Ирина, личность персональных данных	Количество персональных данных, содержащихся в информационной системе	Тип угрозы, актуальных для информационной системы	Масштаб	Степень возможного ущерба	Уровень значимости информации (УЗ)	Класс защищенности	Уровень защищенности	
3.	Обращения граждан	Комитет по информатизации и связи (КИС), Смольный, Санкт-Петербург, 191060	иные	субъектов персональных данных, не являющихся сотрудниками								*

* Автоматическая обработка информации не производится

ПЕРЕЧЕНЬ
должностей государственных гражданских служащих
и работников, замещающих должности, не являющиеся должностями
государственной гражданской службы, Комитета по информатизации и связи,
ответственных за проведение мероприятий по обезличиванию
обрабатываемых персональных данных
в Комитете по информатизации и связи

1. Председатель Комитета по информатизации и связи.
2. Первый заместитель председателя Комитета по информатизации и связи.
3. Заместители председателя Комитета по информатизации и связи.
4. Сектор по вопросам государственной службы и кадров Комитета по информатизации и связи:
начальник Сектора по вопросам государственной службы и кадров Комитета по информатизации и связи.
главный специалист Сектора по вопросам государственной службы и кадров Комитета по информатизации и связи;
5. Финансово-бухгалтерский отдел Комитета по информатизации и связи:
начальник Финансово-бухгалтерского отдела – главный бухгалтер Комитета по информатизации и связи;
главный специалист Финансово-бухгалтерского отдела Комитета по информатизации и связи;
старший бухгалтер Финансово-бухгалтерского отдела Комитета по информатизации и связи.
6. Отдел защиты информации и противодействия техническим разведкам Управления информационной безопасности и технической защиты информации Комитета по информатизации и связи:
ведущий специалист отдела защиты информации и противодействия техническим разведкам Управления информационной безопасности и технической защиты информации.
7. Отдел городских телекоммуникаций и развития сетей связи:
главный специалист Отдела городских телекоммуникаций и развития сетей связи.

Приложение № 15
к приказу Комитета
по информатизации и связи
от 11.03.15 № 31-17

ПЕРЕЧЕНЬ
сведений конфиденциального характера, подлежащих защите
в Комитете по информатизации и связи

1. Информация персонального характера государственных гражданских служащих (далее — сотрудники) и работников, замещающих должности, не являющиеся должностями государственной гражданской службы (далее — работники) Комитета по информатизации и связи:

биографические и опознавательные данные;
отзывы о служебной деятельности и аттестационные листы;
служебное положение;
семейное положение;
социальное положение;
образование, навыки, профессии;
финансовое положение (уровень и состав доходов);
состояние здоровья;
домашний адрес и телефон;
сведения о нахождении сотрудников подразделений Комитета по информатизации и связи (далее — Комитет) под следствием и судом — до вынесения приговора (судебного решения).

иные персональные данные и сведения о фактах, событиях и обстоятельствах частной жизни сотрудников Комитета за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.

2. Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна), а также:

сведения о системе управления Комитетом и подведомственными предприятиями и учреждениями (применяемые формы, методы и способы управления, предметы и цели совещаний, заседаний руководства, факты ведения переговоров; сведения о лицах, принимающих решения, перспективные планы развития, модернизации и совершенствования структуры подразделения; проекты приказов, распоряжений и постановлений);

суммы на банковских счетах Комитета, содержание финансовых договоров со сторонними организациями, содержание переговоров и совещаний.

информация об информационно-телекоммуникационных системах, каналах связи, компьютерных сетях, средствах вычислительной техники, программных средствах (операционных системах, системах управления базами данных и другого общесистемного и программного обеспечения), системах связи, передачи данных, используемых для сбора, хранения, обработки и передачи информации ограниченного доступа Комитета по информатизации и связи;

сведения о системах защиты информации (средства, методы и способы защиты информации, а также коды и процедуры доступа к информационным сетям Комитета).

3. Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с действующим законодательством Российской Федерации.

4. Сведения, составляющие коммерческую тайну предприятий, организаций и других хозяйствующих субъектов, с которыми Комитет заключил финансовые договора, и ставшие известными сотрудникам (работникам) Комитета в силу их служебной деятельности.

5. Сведения о разработке новых технологий и алгоритмов, оригинальных программ и новых технических решений до официальной публикации информации о них.

Приложение № 16
к приказу Комитета
по информатизации и связи
от 11.03.15 № 31-17

ПЕРЕЧЕНЬ

государственных гражданских служащих и работников, замещающих должности, не являющиеся должностями государственной гражданской службы, Комитета по информатизации и связи, допущенных к работе с персональными данными, обрабатываемыми в Комитете по информатизации и связи

Акаткина Наталья Алексеевна	- начальник Финансово-бухгалтерского отдела — главный бухгалтер Комитета по информатизации и связи
Баркова Елена Егоровна	- старший бухгалтер Финансово- бухгалтерского отдела Комитета по информатизации и связи
Жукова Екатерина Вячеславовна	- старший бухгалтер Финансово- бухгалтерского отдела Комитета по информатизации и связи
Кузнецова Юлия Аркадьевна	- главный специалист Финансово- бухгалтерского отдела Комитета по информатизации и связи
Паршин Вячеслав Николаевич	- начальник Сектора по вопросам государственной службы и кадров Комитета по информатизации и связи
Смирнова Вера Владимировна	- главный специалист Финансово- бухгалтерского отдела Комитета по информатизации и связи
Смирнова Наталья Александровна	- главный специалист Сектора по вопросам государственной службы и кадров Комитета по информатизации и связи
Сковпелъ Галина Георгиевна	- главный специалист Отдела городских телекоммуникаций и развития сетей связи Комитета по информатизации и связи

Приложение № 17
к приказу Комитета
по информатизации и связи
от 11.03.15 № 34-71

СОГЛАСИЕ
на обработку персональных данных

Председателю Комитета
по информатизации и связи
от _____

(фамилия, имя, отчество, должность)

проживающего по адресу _____

(адрес указывается с почтовым индексом)

паспорт серия _____ № _____

выдан _____

(дата выдачи и наименование органа, выдавшего документ)

Я, _____, в соответствии
(фамилия, имя, отчество полностью)

со статьей 9 Федерального закона «О персональных данных»¹ даю согласие _____

_____ (наименование исполнительного органа государственной власти Санкт-Петербурга)

расположенному по адресу _____

на автоматизированную, а также без использования средств автоматизации, обработку моих персональных данных, а именно совершение действий, предусмотренных пунктом 3 части первой статьи 3 Федерального закона «О персональных данных» со сведениями о фактах, событиях и обстоятельствах моей жизни, представленных

В _____ в целях
(наименование исполнительного органа государственной власти Санкт-Петербурга)

¹ 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.

обеспечения соблюдения законодательства Российской Федерации.

Настоящее согласие действует со дня его подписания до дня его отзыва в письменной форме.

(дата)

(подпись)

(расшифровка подписи)

Приложение № 18
к приказу Комитета
по информатизации и связи
от А.В.В. № 31-П

ОБЯЗАТЕЛЬСТВО

государственного гражданского служащего и работника, замещающего
должность, не являющуюся должностью государственной гражданской
службы, Комитета по информатизации и связи, непосредственно
осуществляющего обработку персональных данных, в случае расторжения
с ним служебного контракта (трудового договора) прекратить обработку
персональных данных, ставших известными ему в связи исполнения
должностных обязанностей

Председателю Комитета
по информатизации и связи
от _____

(фамилия, имя, отчество, должность)

(наименование структурного подразделения)

(должность)

Я, _____,
(фамилия, имя, отчество полностью)

являясь сотрудником _____

(указать наименование структурного подразделения)

обязуюсь прекратить обработку персональных данных, ставших известными
мне в связи с исполнением должностных обязанностей, в случае расторжения
со мной служебного контракта (трудового договора).

В соответствии со статьей 7 Федерального закона «О персональных данных»,
я уведомлен(а) о том, что персональные данные являются конфиденциальной
информацией, и я обязан(а) не раскрывать третьим лицам и не распространять
персональные данные без согласия субъекта персональных данных, ставшие
известными мне в связи с исполнением должностных обязанностей.

Я предупрежден(а) о том, что в случае нарушения данного обязательства
буду привлечен(а) к ответственности в соответствии с законодательством
Российской Федерации.

(дата)

(подпись)

(расшифровка подписи)

65

Приложение № 19
к приказу Комитета
по информатизации и связи
от 11.03.15 № 31-11

РАЗЪЯСНЕНИЕ
субъекту персональных данных юридических последствий отказа
предоставить свои персональные данные в связи с поступлением
на государственную гражданскую службу
в Комитет по информатизации и связи, ее прохождением

Мне, _____,
разъяснены юридические последствия отказа предоставить свои персональные
данные Комитету по информатизации и связи (далее – Комитет).

В соответствии со статьями 26, 42 Федерального закона «О государственной
гражданской службе Российской Федерации», Положением о персональных
данных государственного гражданского служащего Российской Федерации
и ведении его личного дела, утвержденным Указом Президента Российской
Федерации от 30.05.2005 № 609 «Об утверждении Положения о персональных
данных государственного гражданского служащего Российской Федерации
и ведении его личного дела», определен перечень персональных данных, которые
субъект персональных данных обязан предоставить Комитету в связи
с поступлением или прохождением государственной гражданской службы.

Без представления субъектом персональных данных обязательных
для заключения служебного контракта сведений, служебный контракт
не может быть заключен.

На основании пункта 11 части 1 статьи 33 Федерального закона
«О государственной гражданской службе Российской Федерации» служебный
контракт прекращается, государственный гражданский служащий освобождается
от замещаемой должности гражданской службы и увольняется с гражданской
службы веледствие нарушения установленных обязательных правил заключения
служебного контракта, если это нарушение исключает возможность замещения
должности гражданской службы.

(дата)

(подпись)

(расшифровка подписи)