КОМИТЕТ АРХИТЕКТУРЫ И ГРАДОСТРОИТЕЛЬСТВА КОСТРОМСКОЙ ОБЛАСТИ

ПРИКАЗ

от «29» декабря 2017 г. № 29

г. Кострома

О порядке обработки конфиденциальной информации, в том числе персональных данных, в комитете архитектуры и градостроительства Костромской области

В соответствии с Трудовым кодексом Российской Федерации, Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2004 года № 79-ФЗ «О государственной гражданской службе Российской Федерации», Указом Президента Российской Федерации от 30 мая 2005 года № 609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела», постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, . осуществляемой без использования средств автоматизации»

ПРИКАЗЫВАЮ:

1. Утвердить:

Положение об организации работы с персональными данными осуществляемой без использования средств автоматизации в комитете архитектуры и градостроительства Костромской области (приложение № 1);

Положение о порядке обработки и защите конфиденциальной информации в автоматизированных информационных системах комитете архитектуры и градостроительства Костромской области (приложение № 2).

2. Настоящий приказ вступает в силу со дня его подписания.

Председатель комитета,
главный архитектор Костромской области А.В. Горев

Приложение № 1
к приказу комитета архитектуры и
градостроительства Костромской области
от 29 декабря 2017 г. № 29

Положение
об организации работы с персональными данными в комитете архитектуры и градостроительства Костромской области

Глава 1. Общие положения

1. Настоящее Положение об организации работы с персональными данными в комитете архитектуры и градостроительства Костромской области (далее - Положение) разработано в соответствии с Трудовым кодексом Российской Федерации, Федеральным законом от 27 июля 2004 года № 79-ФЗ «О государственной гражданской службе Российской Федерации» (далее - Федеральный закон «О государственной гражданской службе Российской Федерации»), Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее - Федеральный закон «О персональных данных»), Указом Президента Российской Федерации от 30 мая 2005 года № 609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела» (далее – Указ Президента Российской Федерации) с целью обеспечения защиты персональных данных в комитете архитектуры и градостроительства Костромской области (далее – комитет) от несанкционированного доступа, неправомерного их использования или утраты.

2. В настоящем Положении используются термины и определения, установленные Федеральным законом «О персональных данных».

3. Председатель комитета, руководители структурных подразделений комитета обеспечивают защиту персональных данных субъектов от неправомерного их использования или утраты.

4. Председатель комитета определяет лиц, уполномоченных на обработку персональных данных субъектов, обеспечивающих обработку персональных данных в соответствии с требованиями федеральных законов, других нормативных правовых актов Российской Федерации, несущих ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты этих персональных данных.

Глава 2. Условия сбора и обработки персональных данных

5. Персональные данные следует получать лично у субъекта. В случае возникновения необходимости получения персональных данных у третьей стороны следует известить об этом субъекта заранее, получить его письменное согласие и сообщить ему о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа субъекта дать письменное согласие на их получение.

6. Не допускается обработка специальных категорий персональных данных субъектов, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, за исключением случаев, предусмотренных федеральными законами.

7. При принятии решений, затрагивающих интересы субъекта, запрещается основываться на персональных данных субъекта, полученных исключительно в результате их автоматизированной обработки или с использованием электронных носителей.

Глава 3. Хранение персональных данных, доступ к персональным данным

8. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта, не дольше, чем этого требуют цели их обработки. Персональные данные подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

9. Хранение персональных данных должно происходить в порядке, исключающем их утрату или их неправомерное использование.

10. Доступ к персональным данным без специального разрешения имеют следующие лица:

председатель комитета;

заместитель председателя комитета;

руководители структурных подразделений комитета – в отношении персональных данных государственных гражданских служащих соответствующего структурного подразделения комитета при переводе из одного подразделения в другое; доступ к персональным данным субъекта может иметь руководитель того структурного подразделения, в которое он переведен;

лица, уполномоченные на обработку персональных данных;

сам субъект в отношении своих персональных данных.

11. При получении персональных данных субъектов лица, указанные в пункте 10 настоящей главы, должны иметь право получать только те персональные данные субъекта, которые необходимы для выполнения конкретных задач и функций.

Глава 4. Работа с персональными данными, хранящимися в личных делах и личных карточках субъектов, делах, формируемых по результатам оказания государственных услуг и выполнения функций комитета архитектуры и градостроительства Костромской области

12. Формирование, ведение и хранение личных дел субъектов, а также хранение личных дел субъектов, уволенных с замещаемой должности, осуществляются сектором финансово-экономической и организационно-кадровой работы комитета в порядке, определенном Положением о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела, утвержденным Указом Президента Российской Федерации.

Формирование, ведение и хранение дел, формируемых по результатам оказания государственных услуг и выполнения функций комитета, осуществляются

руководителями структурных подразделений комитета в порядке, определенном действующим законодательством.

13. В соответствии со статьей 43 Федерального закона «О государственной гражданской службе Российской Федерации» сведения из личного дела гражданского служащего включаются в реестр гражданских служащих комитета и хранятся в базе данных государственных информационных систем, а также на электронных носителях с обеспечением защиты от несанкционированного доступа и копирования.

Формирование, ведение и хранение личных карточек субъектов (форма № Т-2ГС (МС)), а также хранение личных карточек субъектов, уволенных из комитета, с дальнейшей их передачей в архив осуществляются сектором финансово-экономической и организационно-кадровой работы комитета в соответствии с указаниями по применению и заполнению форм первичной учетной документации по учету труда и его оплаты, утвержденными постановлением Госкомстата России от 5 января 2004 года № 1 «Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты».

14. Персональные данные, внесенные в личные дела субъектов, иные сведения, содержащиеся в личных карточках субъектов, относятся к сведениям конфиденциального характера, а в случаях, установленных федеральными законами и иными нормативными правовыми актами Российской Федерации, - к сведениям, составляющим государственную тайну.

Глава 5. Общедоступные источники персональных данных

15. В целях информационного обеспечения в комитете могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом. Сведения о субъекте должны быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта либо по решению суда или иных уполномоченных государственных органов.

16. Формирование, ведение и иные действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных, содержащихся в общедоступных источниках, а также получение письменного согласия субъекта осуществляются структурными подразделениями комитета.

Глава 6. Передача персональных данных субъектов

17. Передача персональных данных субъекта возможна только с письменного согласия субъекта, за исключением случаев, предусмотренных федеральными законами.

18. При передаче персональных данных субъекта оператор должен соблюдать следующие требования:

1) не сообщать персональные данные субъекта третьей стороне без письменного согласия субъекта, за исключением случаев, установленных федеральными законами;

2) не сообщать персональные данные субъекта в коммерческих целях без его письменного согласия;

3) не запрашивать информацию о состоянии здоровья субъекта, за исключением тех сведений, которые относятся к вопросу о возможности выполнения им трудовых функций;

4) предупредить лиц, получающих персональные данные субъекта, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные субъекта, обязаны соблюдать режим секретности (конфиденциальности);

5) передавать персональные данные субъекта представителям субъекта в порядке, установленном Трудовым кодексом Российской Федерации, и ограничивать эту информацию только теми персональными данными субъекта, которые необходимы для выполнения указанными представителями их функций.

19. Персональные данные субъектов могут представляться в следующие государственные и негосударственные функциональные структуры:

налоговые инспекции;

правоохранительные органы;

органы статистики;

страховые агентства;

военкоматы;

органы социального страхования;

пенсионные фонды и иные организации, предусмотренные федеральным законодательством.

20. Сведения о субъекте (в том числе уволенном) могут быть представлены другой организации только с письменного запроса на бланке организации с приложением копии заявления самого субъекта.

21. Персональные данные субъекта могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого субъекта.

22. Не допускается сообщать персональные данные субъекта по телефону или факсу.

Глава 7. Права субъектов в целях защиты персональных данных

23. Субъект имеет право:

1) получать полную информацию о своих персональных данных и обработке этих данных;

2) осуществлять свободный бесплатный доступ к своим персональным данным, включая право получать копии любой записи, содержащей персональные данные должностного лица, гражданского служащего, за

исключением случаев, предусмотренных Федеральным законом «О персональных данных»;

3) требовать от оператора уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные Федеральным законом «О персональных данных» меры по защите своих прав;

4) требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением федеральных законов «О персональных данных», «О государственной гражданской службе Российской Федерации». Субъект при отказе оператора исключить или исправить его персональные данные имеет право заявить в письменной форме оператору о своем несогласии, обосновав соответствующим образом такое несогласие. Персональные данные оценочного характера субъект имеет право дополнить заявлением, выражающим его собственную точку зрения;

5) требовать от оператора уведомления всех лиц, которым ранее были сообщены неверные или неполные их персональные данные, обо всех произведенных в них изменениях или исключениях из них;

6) обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов или в судебном порядке, если субъект считает, что оператор осуществляет обработку его персональных данных с нарушением требований Федерального закона «О персональных данных» или иным образом нарушает его права и свободы.

Глава 8. Обязанности субъекта и оператора

24. Субъект обязан:

1) представить оператору полные и достоверные сведения;

2) в случае изменения сведений, содержащих персональные данные субъектов (фамилия, имя, отчество, адрес, абонентский номер, паспортные данные, сведения об образовании, семейном положении, состоянии здоровья (при выявлении противопоказаний для выполнения служебных обязанностей, обусловленных служебным контрактом), субъект обязан в течение пяти рабочих дней сообщить о таких изменениях в соответствующее структурное подразделение комитета.

25. Оператор обязан:

1) осуществлять обработку персональных данных исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия в трудоустройстве, обучения и продвижения по службе, обеспечения личной безопасности, контроля качества и количества выполняемой работы и обеспечения сохранности имущества;

2) получать согласие субъекта на обработку его персональных данных, оформленного в соответствии со статьей 9 Федерального закона «О персональных данных»;

3) обеспечить сохранность персональных данных субъекта;

4) обеспечить конфиденциальность сведений, содержащихся в персональных данных субъекта, в соответствии с Федеральным законом «О государственной гражданской службе Российской Федерации», другими федеральными законами, иными нормативными правовыми актами Российской Федерации;

5) представлять сведения о доходах, имуществе и обязательствах имущественного характера субъекта для опубликования общероссийским и региональным средствами массовой информации по их обращениям;

6) приобщать к личным делам субъекта документы, указанные в пунктах 16 и 17 Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела, утвержденного Указом Президента Российской Федерации;

7) знакомить субъекта с документами его личного дела не реже одного раза в год, а также по просьбе субъекта и во всех иных случаях, предусмотренных законодательством Российской Федерации;

8) в срок, не превышающий семи рабочих дней со дня представления субъектом или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, оператор обязан внести в них необходимые изменения.

Глава 9. Ответственность за нарушение норм, регулирующих обработку персональных данных

26. Лица, виновные в нарушении норм, регулирующих обработку персональных данных, несут дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

Приложение № 2
к приказу комитета архитектуры и
градостроительства Костромской области
от 29 декабря 2017 г. № 29

Положение о порядке обработки и защите конфиденциальной информации в автоматизированных информационных системах комитета архитектуры и градостроительства Костромской области

Глава 1. Общие положения

1. Настоящее Положение о порядке обработки и защите конфиденциальной информации в автоматизированных информационных системах комитета (далее - Положение) разработано в соответствии с Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных».

2. Настоящее Положение определяет цели обработки и защиты конфиденциальной информации, объекты защиты конфиденциальной информации, организационную систему обработки и защиты конфиденциальной информации, в том числе персональных данных в автоматизированных информационных системах комитета, основные направления и методы защиты конфиденциальной информации в автоматизированных информационных системах комитета, обязанности и ответственность пользователей и должностных лиц при обработке конфиденциальной информации в автоматизированных информационных системах комитета, а также ответственность за разглашение конфиденциальной информации.

3. В Положении используются термины и определения, установленные правовыми актами, указанными в пункте 1 настоящего Положения.

Глава 2. Цели обработки и защиты конфиденциальной информации

4. Основной целью обработки конфиденциальной информации автоматизированных информационных системах комитета является повышение эффективности исполнения комитетом установленных законодательством полномочий.

5. Основными целями защиты конфиденциальной информации в автоматизированных информационных системах комитета являются:

предотвращение неконтролируемого распространения конфиденциальной информации в результате ее разглашения сотрудниками или получения несанкционированного доступа к информации;

предотвращение несанкционированного уничтожения, искажения, копирования, блокирования информации;

предотвращение утрат, несанкционированного уничтожения или сбоев функционирования машинных носителей информации, обеспечение полноты, целостности, достоверности информации;

соблюдение правового режима использования автоматизированных информационных систем комитета;

обеспечение возможности обработки и использования конфиденциальной информации сотрудниками комитета, имеющими соответствующие полномочия.

Глава 3. Объекты защиты конфиденциальной информации

6. Объектами защиты конфиденциальной информации в автоматизированных информационных системах комитета являются: информация, ее материальные носители, программные и технические средства обработки, передачи и защиты информации (далее - Активы).

7. Защите подлежат следующие Активы:

информационные ресурсы, содержащие сведения, отнесенные к категории информации конфиденциального характера, представленные в виде отдельных документов, информационных массивов и баз данных, зафиксированных на машинных носителях;

основные технические средства и системы информатизации (средства вычислительной техники, информационно-вычислительные комплексы, сети и системы), программные средства (операционные системы, системы управления базами данных, другое общесистемное и программное обеспечение), телекоммуникационные системы, используемые для обработки и передачи информации, содержащей сведения, отнесенные к конфиденциальной информации;

вспомогательные технические средства и системы, не обрабатывающие информацию, но размещенные в помещениях, где обрабатывается информация, содержащая сведения, отнесенные к конфиденциальной информации.

Глава 4. Организационная система обработки и защиты конфиденциальной информации

8. Организационную систему обработки и защиты конфиденциальной информации в автоматизированных информационных системах комитета архитектуры и градостроительства Костромской области образуют;

председатель комитета - осуществляет общее руководство по вопросам обработки и защиты конфиденциальной информации, осуществляет распорядительные функции по организации работ по обработке и защите конфиденциальной информации в автоматизированных информационных системах комитета, взаимодействует с надзорными органами по общим вопросам обработки и защиты конфиденциальной информации в автоматизированных информационных системах комитета;

руководители структурных подразделений комитета, в которых производится обработка конфиденциальной информации, - организуют обработку конфиденциальной информации в своем структурном подразделении;

администратор информационной безопасности организует работу по технической защите конфиденциальной информации в комитете, производит оценку эффективности применяемых мер технической защиты конфиденциальной информации в автоматизированных информационных системах комитета пользователи (потребители) информации (далее - Пользователи) - сотрудники структурных подразделений комитета, наделенные соответствующими правами по доступу к конфиденциальной информации и непосредственно использующие эту информацию для исполнения своих должностных обязанностей или выполняющие непосредственные действия по вводу, хранению, обработке и передаче конфиденциальной информации;

для проведения работ по защите конфиденциальной информации в автоматизированных информационных системах комитета могут привлекаться на договорной основе специализированные организации, имеющие соответствующие лицензии на право проведения работ в области защиты информации.

Глава 5. Основные направления и методы защиты конфиденциальной информации

9. Основными направлениями работ по защите конфиденциальной информации являются:

физическая защита помещений, в которых обрабатывается конфиденциальная информация, от проникновения посторонних лиц; физическая защита Активов от хищения, разрушения, уничтожения; защита от несанкционированного доступа к конфиденциальной информации, несанкционированного или непреднамеренного воздействия;

защита от преднамеренных или непреднамеренных действий Пользователей, ведущих к утечке или утрате конфиденциальной информации.

10. Мероприятия по защите конфиденциальной информации включают в себя: организационно-распорядительные, технические и контрольно-корректирующие.

11. Организационно-распорядительные мероприятия по защите конфиденциальной информации включают в себя:

разработку организационно-распорядительных документов по защите конфиденциальной информации;

ограничение числа лиц, допущенных к обработке конфиденциальной информации;

организацию контролируемой зоны, размещение объекта защиты внутри контролируемой зоны на максимально возможном удалении от ее границ, ограничение доступа лиц, не допущенных к обработке конфиденциальной информации, внутрь контролируемой зоны;

размещение дисплеев и других средств отображения, исключающее несанкционированный просмотр информации;

документальное оформление перечня сведений конфиденциального характера, Реестра автоматизированных информационных систем комитета, обрабатывающих конфиденциальную информацию;

инвентаризацию, учет и надежное хранение Активов, содержащих конфиденциальную информацию или посредством которых производится обработка конфиденциальной информации;

классификацию и категорирование автоматизированных информационных систем комитета, обрабатывающих конфиденциальную информацию, исходя из требований законодательства и критичности для обеспечения государственного управления, в необходимых случаях - аттестацию автоматизированных информационных систем комитета;

выявление угроз несанкционированного доступа к конфиденциальной информации, разработку мероприятий по нейтрализации угроз;

организацию и соблюдение правил парольной защиты в автоматизированных информационных системах комитета;

повышение квалификации, совершенствование знаний и навыков Пользователей в вопросах защиты конфиденциальной информации; дисциплинарную практику.

12. Мероприятия по технической защите информации включают в себя: организацию физической защиты помещений и технических средств обработки информации с использованием организационных мер и технических средств охраны, предотвращающих или существенно затрудняющих проникновение в здания, помещения посторонних лиц, хищение документов и носителей информации, самих средств информатизации;

сегментацию локальных вычислительных сетей в комитете, применение в сегментах локальных вычислительных сетей, в которых обрабатывается конфиденциальная информация, технических средств защиты информации, соответствующих требуемому классу защиты;

техническую реализацию системы парольной защиты для автоматизированных информационных систем комитета, в которой обрабатывается конфиденциальная информация;

использование сертифицированных средств защиты информации в автоматизированных информационных системах комитета при передаче информации по открытым каналам связи в соответствии с установленными законодательством требованиями;

регистрацию действий Пользователей, технических специалистов, контроль несанкционированного доступа и действий Пользователей, технических специалистов и посторонних лиц;

использование защищенных каналов связи, реализацию технологии частных виртуальных сетей в корпоративной вычислительной сети комитета;

реализацию мероприятий по антивирусной защите в автоматизированных информационных системах комитета;

реализацию системы резервного копирования информации.

13. Контрольно-корректирующие мероприятия по защите конфиденциальной информации включают в себя:

контроль исполнения законодательства в области защиты конфиденциальной информации;

контроль исполнения организационно-распорядительных документов; контроль выполнения мероприятий по технической защите информации, оценку эффективности выполнения мероприятий по технической защите информации;

выработку корректирующих воздействий, реализуемых путем издания и последующего исполнения организационно-распорядительных документов; применение дисциплинарных мер.

14. Порядок действий по реализации мероприятий по защите конфиденциальной информации определяется инструкциями и регламентами, разрабатываемыми и утверждаемыми в соответствии с принятым в комитете порядком.

Глава 6. Обязанности и ответственность Пользователей и должностных лиц при обработке и защите конфиденциальной информации в автоматизированных информационных системах комитета архитектуры и градостроительства Костромской области

15. Должностное лицо, курирующее вопросы по защите информации, утверждает организационно-распорядительные документы по защите информации.

16. Руководители структурных подразделений, в которых производится обработка конфиденциальной информации:

несут ответственность за организацию обработки конфиденциальной информации в своем структурном подразделении;

вносят предложения по включению в Реестр автоматизированных информационных систем обработки конфиденциальной информации комитете, изменению или исключению соответствующих сведений в реестре;

вносят предложения и изменения в списки сотрудников, допускаемых к работе с конфиденциальной информацией, в эксплуатируемых автоматизированных информационных системах комитета;

обеспечивают выполнение организационных мероприятий по обеспечению защиты конфиденциальной информации;

несут ответственность за соблюдение требований по защите конфиденциальной информации пользователями своих структурных подразделений и принимают меры по фактам нарушений требований по защите конфиденциальной информации, разглашения конфиденциальной информации или утери документов, содержащих такую информацию;

несут ответственность за своевременное информирование администратора информационной безопасности о необходимости уничтожения конфиденциальной информации с жестких дисков персональных компьютеров, передаваемых в ремонт или в другие структурные подразделения и исполнительные органы государственной власти;

несут ответственность за выполнение Пользователями своего структурного подразделения общих правил работы на персональных компьютерах и в локальных вычислительных сетях комитета, при передаче

информации по каналам связи, использования сертифицированных средств криптозащиты, за организацией доступа в Интернет, соблюдение Пользователями условий хранения средств технической защиты информации;

определяют порядок передачи информации конфиденциального характера другим структурным подразделениям комитета, исполнительным органам государственной власти Костромской области, муниципальным образованиям Костромской области и сторонним организациям;

несут ответственность за характер исходящей информации, направляемой пользователями по электронной почте другим адресатам, и принятие оперативных мер к соблюдению установленных требований по защите конфиденциальной информации.

17. Администратор информационной безопасности:

организует ведение реестра автоматизированных информационных систем комитета, в которых осуществляется обработка конфиденциальной информации;

организует и обеспечивает исполнение работ по технической защите конфиденциальной информации в автоматизированных информационных системах комитета;

осуществляет контроль состояния защиты конфиденциальной информации и производит оценку эффективности применяемых мер технической защиты информации в автоматизированных информационных системах комитета;

осуществляет разработку проектов планов мероприятий по организации системы защиты информации в автоматизированных информационных системах комитета, участвует в их исполнении;

представляет отчеты о состоянии системы защиты информации в автоматизированных информационных системах комитета;

разрабатывает проекты организационно-распорядительных документов по вопросам обработки и технической защиты конфиденциальной информации в автоматизированных информационных системах комитета;

разрабатывает предложения по совершенствованию системы защиты информации в комитете;

18. Пользователи:

участвуют в обработке конфиденциальной информации, осуществляют непосредственные действия по регистрации информации в автоматизированных информационных системах комитета, ее обработке, передаче по сетям передачи данных, применению сертифицированных средств защиты информации;

используют информацию, документы, полученные из автоматизированных информационных систем комитета, в своей работе с целью реализации возложенных на них функций;

применяют (в необходимых случаях) сертифицированные средства защиты информации;

несут персональную ответственность за передачу или утерю носителей конфиденциальной информации, а также средств защиты информации.

Глава 7. Ответственность за разглашение конфиденциальной информации

19. За разглашение информации конфиденциального характера, нарушение порядка обращения с документами и машинными носителями информации, содержащими такую информацию, а также за нарушение или неисполнение требований режима защиты, обработки и порядка использования этой информации сотрудник может быть привлечен к дисциплинарной, гражданско-правовой, административной или уголовной ответственности, предусмотренной действующим законодательством.