АДМИНИСТРАЦИЯ УДОМЕЛЬСКОГО ГОРОДСКОГО ОКРУГА

РАСПОРЯЖЕНИЕ

06.09.2019 г. Удомля № 731-ра

Об обеспечении информационной безопасности и защите персональных данных в Администрации Удомельского городского округа

В соответствии с Федеральными законами от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и от 27.07.2006 № 152-ФЗ «О персональных данных», в целях совершенствования системы защиты информации и персональных данных в Администрации Удомельского городского округа,

1. Создать Комиссию по информационной безопасности Администрации Удомельского городского округа (далее-Комиссия) в следующем составе:

– Корнилова Л.Н., заместитель Главы Администрации Удомельского городского округа – председатель Комиссии;

– Семенова Л.В., руководитель отдела организационной работы и муниципальной службы, Администрации Удомельского городского округа – заместитель председателя Комиссии;

– Маракулина М.А., ведущий программист отдела организационной работы и муниципальной службы Администрации Удомельского городского округа – секретарь Комиссии.

Члены Комиссии:

– Гусева С.Н., заместитель руководителя отдела организационной работы и муниципальной службы Администрации Удомельского городского округа;

– Петрова С.В., главный специалист по мобилизационной подготовке Администрации Удомельского городского округа;

– Сивцова Е.Г., главный специалист отдела правового обеспечения и муниципального заказа Администрации Удомельского городского округа.

2. Утвердить Положение о Комиссии по информационной безопасности Администрации Удомельского городского округа (Приложение 1).

3. Утвердить инструкцию по обеспечению защиты служебной информации и персональных данных в Администрации Удомельского городского округа (Приложение 2).

4. Утвердить инструкцию оператору автоматизированной системы (АС) (пользователю ПЭВМ) по обеспечению безопасности информации при работе на

ПЭВМ (Приложение 3).

5. Разместить настоящее распоряжение на официальном сайте муниципального образования Удомельский городской округ в информационно-телекоммуникационной сети «Интернет».

6. Настоящее распоряжение вступает в силу со дня его подписания.

Глава Удомельского городского округа Р.А. Рихтер

Приложение 1
к распоряжению Администрации
Удомельского городского округа
от 06.09.2019 № 731-ра

Положение
о Комиссии по информационной безопасности Администрации Удомельского городского округа

1. Общие положения

1.1. Комиссия по информационной безопасности Администрации Удомельского городского округа (далее - Комиссия) является постоянно действующим коллегиальным органом по проведению политики информационной безопасности и защиты персональных данных, проведению мероприятий по обеспечению информационной безопасности и защите персональных данных.

1.2. Положение о Комиссии по информационной безопасности Администрации Удомельского городского округа (далее - Положение) определяет задачи, функции, права и порядок работы Комиссии.

1.3. Свою деятельность Комиссия осуществляет в соответствии с действующим законодательством Российской Федерации в сфере информационной безопасности, персональных данных, нормативно-методическими документами в области защиты информации и персональных данных и данным Положением.

1.4. Обязанности между членами Комиссии распределяет председатель Комиссии.

2. Задачи и функции Комиссии

2.1. Основными задачами Комиссии являются:

- Рассмотрение проектов муниципальных правовых актов по информационной безопасности и подготовка предложений по ним Главе Удомельского городского округа. Принятие решения об утверждении документов по информационной безопасности.
- Своевременное выявление и устранение угроз безопасности информации.
- Создание условий и механизма оперативного реагирования на угрозы безопасности информации.
- Эффективное пресечение посягательств на информационные ресурсы на основе правовых, организационных, инженерно-технических, программных средств обеспечения безопасности информации.

2.2. С целью достижения наиболее эффективного результата в решении поставленных задач Комиссия осуществляет следующие функции:

- разрабатывает перечень информационных систем и персональных данных Администрации Удомельского городского округа;
- организует разработку, внедрение и эксплуатацию системы защиты информации содержащей конфиденциальные сведения, обрабатываемых с использованием технических средств;
- проводит анализ прохождения платежных документов и другой информации, требующей защиты, в ходе всего технологического цикла с целью выявления закрытию возможных каналов утечки информации и принятия мер по их закрытию;
- проводит категорирование объектов информатизации и классификацию защищенности автоматизированных систем;
- разрабатывает разрешительную систему доступа пользователей и эксплуатационного персонала к обрабатываемой информации, подлежащей защите;
- рассматривает возможность передачи конфиденциальной информации Администрации Удомельского городского округа по запросам сторонних организаций;
- принимает решения о возможности использования в органах и структурных

подразделениях Администрации Удомельского городского округа технических, программных, программно-аппаратных и криптографических средств защиты информации;

- осуществляет контроль полноты и своевременности выполнения мероприятий по защите информации и принятых решений Комиссии в органах и структурных подразделениях Администрации Удомельского городского округа;

- ведет постоянную работу по совершенствованию системы защиты информации;

- осуществляет планирование своей деятельности.

2.3. По заданию Главы Удомельского городского округа Комиссия может осуществлять иные функции, не отраженные в настоящем Положении.

3. Права Комиссии

3.1. Комиссия имеет право:

- проводить проверки соблюдения режима защиты информации в органах и структурных подразделениях Администрации Удомельского городского округа;

- вносить предложения Главе Удомельского городского округа по совершенствованию существующей системы защиты информации;

- привлекать по согласованию с руководителями органов и структурных подразделений Администрации Удомельского городского округа к работе по созданию и совершенствованию системы защиты информации других работников Администрации Удомельского городского округа;

- проводить служебные расследования по фактам утечки информации или грубых нарушений режима защиты информации;

- требовать от работников Администрации Удомельского городского округа письменных объяснений при проведении служебных расследований;

- давать работникам Администрации Удомельского городского округа обязательные для выполнения указания по защите конфиденциальной информации, определяемые существующим в Российской Федерации законодательством и требованиями Администрации Удомельского городского округа.

3.2. Членам Комиссии запрещается:

- доводить до работников Администрации Удомельского городского округа систему защиты информации в полном объеме;

- при выходе из состава Комиссии запрещается раскрывать объем работы и конкретные направления деятельности Комиссии, разглашать информацию, ставшую известной в ходе работы в составе Комиссии.

4. Порядок работы Комиссии

4.1. Комиссия осуществляет свою деятельность в соответствии с разрабатываемым ею планом работы.

4.2. План работы Комиссии составляется с учетом плана работы на год Администрации Удомельского городского округа.

4.3. В течение года деятельность Комиссии осуществляется в соответствии с представленным планом.

4.4. Периодичность заседаний членов Комиссии устанавливается решением Комиссии, но не реже одного раза в год.

4.5. По решению Комиссии рабочим группам, членам Комиссии или его экспертам может поручаться подготовка проектов документов для рассмотрения на Комиссии.

Приложение 2
к распоряжению Администрации
Удомельского городского округа
от 06.09.2019 № 731-ра

Инструкция
по обеспечению защиты служебной информации и персональных данных в Администрации Удомельского городского округа

1.Общие положения

1.1. Настоящая Инструкция распространяется на все виды работ, связанных с обработкой служебной информации и персональными данными, требующих защиты, с применением технических средств (персональные электронно-вычислительные машины, копировально-множительные аппараты, электронные пишущие машинки) в Администрации Удомельского городского округа (далее – Администрация).

1.2. Выполнение требований настоящей Инструкции обязательно для всех должностных лиц и работников Администрации.

1.3. Инструкция разработана на основании:

1.3.1. Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации»;

1.3.2. Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

1.3.3. Указа Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера»;

1.3.4. Положения о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам, утвержденного постановлением Совета Министров-Правительства Российской Федерации от 15.09.1993 № 912-51;

1.3.5. Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, утвержденного постановлением Правительства Российской Федерации от 03.11.1994 № 1233;

1.3.6. Концепции защиты информации в Тверской области;

1.3.6. Политики информационной безопасности Администрации Удомельского городского округа.

1.4. К служебным сведениям (служебной информации) ограниченного доступа, персональным данным относится несекретная информация, связанная с деятельностью Администрации, имеющая ценность в силу своей неизвестности посторонним лицам, ограничения на распространение которой предусмотрены законодательством и диктуются служебной необходимостью, к которой отсутствует свободный доступ посторонних лиц на законном основании и к охране конфиденциальности которой в Администрации принимаются соответствующие меры, за исключением информации, доступ к которой не может быть ограничен в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации».

1.5. Требования настоящей Инструкции не распространяются на порядок обращения с информацией, содержащей сведения, составляющие государственную тайну.

1.6. Работа со служебной информацией ограниченного доступа, имеющей гриф «Для служебного пользования» производится в соответствии с Положением о порядке обращения со служебными сведениями ограниченного доступа в Администрации.

1.7. Лица, принимаемые на работу в Администрацию, заключают трудовой договор, в котором определяются обязанности муниципального служащего по сохранности служебной тайны, а также по неразглашению ставших ему известными в связи с исполнением должностных обязанностей сведений ограниченного доступа, персональных данных. На работника налагаются ограничения по использованию в неслужебных целях полученной информации.

Инструктаж работников структурных подразделений Администрации проводится их руководителями.

Инструктаж заместителей Главы Администрации Удомельского городского округа осуществляется одним из заместителей Главы Администрации Удомельского городского округа - председателем Комиссии по информационной безопасности и защите персональных данных Администрации Удомельского городского округа.

1.8. Лица, нарушившие эти требования трудового договора и создавшие тем самым условия для утечки информации, привлекаются к ответственности, в зависимости от степени нанесенного ущерба, в соответствии с действующим законодательством.

1.9. Мероприятия по защите конфиденциальной и другой информации требующей защиты, в Администрации организует и проводит:

- комиссия по информационной безопасности и защите персональных данных Администрации Удомельского городского округа;
- руководители структурных подразделений
- лица, отвечающие за информационные технологии, уполномоченный за защиту информации и персональных данных в Администрации;
- режимно-секретное подразделение;
- ответственные за защиту информации и персональных данных в структурных подразделениях Администрации – по всем вопросам информационной безопасности и защите персональных данных.

2. Требования по защите информации и персональных данных при эксплуатации технических средств

2.1. Требования распространяются на все технические средства обработки документальной информации: персональные ЭВМ, копировально-множительные аппараты, электронные пишущие машинки (далее - технические средства).

2.2. К самостоятельной работе на технических средствах допускаются лица, изучившие техническую документацию на них, освоившие правила работы и прошедшие инструктаж у непосредственного руководителя, ответственного за защиту информации в структурном подразделении.

2.3. Запрещается на установленных технических средствах, не прошедших специальные исследования, проверку и не имеющих предписания на эксплуатацию, обрабатывать информацию и документы конфиденциального характера.

2.4. Требования по защите информации в локальных вычислительных сетях (при наличии ЛВС):

2.4.1. Основной целью обеспечения информационной безопасности в локальных вычислительных сетях (далее - ЛВС) является защита информации и поддерживающей ее инфраструктуры от случайных и преднамеренных воздействий естественного или искусственного характера, которые могут привести к ущербу системы и информации пользователей.

2.4.2. Использование информации, находящейся в локальных вычислительных сетях, работниками Администрации производится в соответствии с Политикой информационной безопасности Администрации Удомельского городского округа.

2.4.3. Эксплуатация персональных компьютеров и программных средств производится в соответствии с Политикой информационной безопасности Администрации Удомельского городского округа.

2.4.4. Обеспечение информационной безопасности и защиту персональных данных в телекоммуникационных и локальных вычислительных сетях Администрации осуществляет назначенный для этого работник.

2.4.5. Ответственность за защиту электронной информации в Администрации, несут работники, ответственные за эксплуатацию электронных средств обработки информации.

2.4.6. На персональных электронно-вычислительных машинах (далее - ПЭВМ) должна обрабатываться информация, строго связанная с тематикой работ пользователя, ответственного за применение ПЭВМ.

Работникам Администрации запрещается распространение баз данных, ее частей или

тематических разделов за пределы аппарата ПЭВМ, на которых обрабатывается информация ограниченного доступа и которые в соответствии с Указом Президента Российской Федерации от 12.05.2004 № 611 не должны быть включены в сеть «Интернет» или обязаны использовать сертифицированные средства защиты информации.

2.4.7. Пользователи (потребители) информационных ресурсов несут персональную ответственность за использование полученной информации по назначению, постоянно ведут учет (журнальный) и надежное хранение съемных носителей (диски, дискеты и т.п.) конфиденциальной информации и их использование, исключающее копирование, хищение, подмену или уничтожение.

2.4.8. Информация, содержащая сведения ограниченного доступа, должна быть защищена от несанкционированного на неё воздействия.

2.4.9. Коммуникационные шкафы линий ЛВС, сервера, межсетевые экраны, находящиеся под контролем ответственных лиц Администрации, должны опечатываться и сдаваться под охрану назначенным ответственным лицом.

2.5. Принципы защиты информации и персональных данных в ЛВС:

2.5.1. Защита от несанкционированного доступа к информационным ресурсам в Администрации осуществляется за счет сервисных возможностей операционных систем и сетевых программных продуктов, что выражается в присвоении каждому пользователю уникального идентификатора для доступа к сетевым ресурсам и уникального пароля (не менее 6 символов) для подтверждения идентификации.

2.5.2. Защита информационных и технических ресурсов ЛВС Администрации от вирусов осуществляется специализированной сетевой антивирусной программой, которая устанавливается как на сервере Администрации, так и на ПЭВМ пользователей.

2.5.3. В ЛВС Администрации должны быть информационные страницы, на которых размещена специальная открытая информация для общего пользования.

2.5.4. Для хранения информации ограниченного доступа необходимо использовать учтенные электронные носители информации ПЭВМ, обеспечить организационную и техническую защиту от доступа к ПЭВМ посторонних лиц или дисковому пространству на сервере.

2.5.5. В случае использования одной ПЭВМ несколькими работниками, для каждого работника выделяется дисковое пространство на ПЭВМ, создается папка с уникальным именем, которая «закрывается» паролем.

2.5.6. Информационные ресурсы выделяются собственником в коллективное пользование лишь по согласованию с администратором сети.

2.5.7. Установка программного обеспечения для пользователей ПЭВМ осуществляется только администратором сети.

2.6. Выдача и использование пользовательских идентификаторов и паролей:

2.6.1. На каждого нового работника непосредственный руководитель подает информацию на получение идентификатора, пароля, а также на подключение к ЛВС и необходимый объем ресурсов для его работы.

Каждый пользователь ЛВС получает у ответственного лица идентификатор (имя пользователя) для подключения к сетевым ресурсам, защитный пароль и право на подключение к ЛВС. Идентификатор и пароль являются конфиденциальными сведениями. Инструктаж по порядку пользования паролем и идентификатором, их замене, ответственности за разглашение пароля и идентификатора, проводится администратором сети и работником ответственного за защиту информации Администрации под роспись.

2.6.2. Журнал учета выдачи идентификатора и пароля, имеет гриф «Для служебного пользования» и хранится в сейфе у работника ответственного за защиту информации. Доступ к нему других лиц исключен.

2.6.3. Включение ПЭВМ при отсутствии работника, отвечающего за его эксплуатацию, осуществляется администратором сети по письменному заявлению руководителя структурного подразделения Администрации.

При увольнении или перемещении работника (оператора автоматизированной системы) руководитель структурного подразделения принимает меры по оперативному изменению паролей и

идентификаторов пользователей.

2.6.4. Пользователь ПЭВМ обязан соблюдать требования настоящей Инструкции и, кроме того:

- менять защитный пароль и идентификатор для подключения к локальной вычислительной сети и ее ресурсам при участи администратора сети не реже 1 раза в квартал;
- сообщать непосредственному руководителю и администратору сети о неисправностях ПЭВМ или сбоях в программных продуктах сразу по их возникновению;
- производить сохранение обрабатываемой информации с интервалом 5-10 минут во время работы на ПЭВМ;
- делать резервные копии представляющих ценность файлов -документов на ПЭВМ с целью их быстрого восстановления;
- хранить рабочие машинные носители информации в закрывающихся на ключ ящиках столов, шкафах;
- отдавать в установленном порядке на уничтожение дискеты, имеющие физические дефекты;
- уничтожать потерявшие надобность черновики, распечатки материалов обрабатываемой информации сразу по окончании работы с ними;
- сохранять всю обрабатываемую информацию после окончания работы на ПЭВМ, завершать сеанс работы в порядке, установленном правилами эксплуатации ПЭВМ;
- сообщать непосредственному руководителю и администратору сети об обнаружении попыток или признаков несанкционированного доступа к информации.

2.6.7. Пользователю ПЭВМ строго запрещается:

- производить самостоятельно демонтаж оборудования;
- подключать к ПЭВМ нештатные устройства;
- использовать ЛВС с целью получения доступа к сетевым ресурсам без разрешения администратора сети;
- обновлять и устанавливать дополнительное программное обеспечение;
- вносить сведения в ПЭВМ с магнитных или других носителей информации, не прошедших проверку на вирусы у администратора сети;
- проводить работы, связанные с решением задач секретного характера;
- допускать к работе с информацией лиц, не имеющих к ней отношения;
- передавать пароли любому другому лицу для доступа к ЛВС;
- передавать рабочие дискеты (диски) с общим и специальным программным обеспечением другим лицам.

2.7. Требования по защите информации при эксплуатации копировально-множительной техники

2.7.1. Копирование документов, имеющую секретную или конфиденциальную информацию осуществляется работниками отдела по мобподготовке, делам ГО и ЧС Администрации на закрепленной за ними копировально-множительной технике.

2.7.2. Запрещается размножение, материалов ограниченного доступа, на установленных копировальных аппаратах, не имеющих спецпредписания на эксплуатацию.

2.7.3. Документы с грифом «ДСП» размножаются в соответствии с Положением о порядке обращения со служебными сведениями ограниченного доступа в Администрации.

2.7.4. Испорченные копии документов уничтожаются лицом, производившим копирование документа в установленном порядке.

Приложение 3
к распоряжению Администрации
Удомельского городского округа
от 06.09.2019 № _731_-ра

Инструкция
оператору автоматизированной системы (АС) (пользователю ПЭВМ)
по обеспечению безопасности информации при работе на ПЭВМ

1. Произвести внешний осмотр аппаратуры, убедится в соответствии инвентарных номеров на ПЭВМ и книги закрепления аппаратуры за работниками подразделения у непосредственного руководителя или другого должностного лица.
2. В процессе работы на ПЭВМ ответственность за соблюдение требований по обеспечению безопасности информации, её конфиденциальности, мер безопасности, исправности ПЭВМ и оборудования возлагается на пользователя.
3. Ввод идентификатора и пароля осуществлять, убедившись, что никто не наблюдает за их набором.
4. При обработке информации ограниченного доступа (конфиденциальной информации), быть уверенным, что к ПЭВМ нет доступа с локально вычислительной сети (ЛВС) или «интернет».
5. Разрешается работа со служебной информацией только с дискетами, флэш-носителями и оптическими дисками, прошедшими предварительную проверку на отсутствие программных вирусов.
6. Диски и дискеты со служебной информацией хранить отдельно, в закрываемом на ключ ящике или сейфе.
7. Выходя из помещения, в т.ч. и на короткое время, исключить доступ к информации, имеющейся на вашем компьютере или вашем дисковом пространстве, если вы работаете на ПЭВМ не один.
8. Не разрешать работать на ПЭВМ, входить в ЛВС другим лицам без разрешения непосредственного руководителя.
9. Размножение документов со служебной информацией осуществлять с разрешения непосредственного руководителя и с записью в журнале учета размноженных служебных документов.
10. Пользователь имеет право обрабатывать, размножать и отображать на ПЭВМ только не секретную информацию.
11. Систематически (1 раз в 3 месяца) осуществлять смену идентификатора и пароля.
12. При обнаружении факта или подозрения о несанкционированном доступе к информации, обнаружении нарушений и сбоев в работе АС немедленно докладывать непосредственному руководителю, сообщать в отдел организационной работы и муниципальной службы.