АДМИНИСТРАЦИЯ УДОМЕЛЬСКОГО ГОРОДСКОГО ОКРУГА

РАСПОРЯЖЕНИЕ

29.01.2019 г. Удомля № 60-ра

Об утверждении Политики информационной безопасности Администрации Удомельского городского округа

В соответствии с распоряжением Правительства Тверской области от 12.10.2017 № 345-рп «Об утверждении Политики информационной безопасности исполнительных органов государственной власти Тверской области, государственных учреждений Тверской области и государственных унитарных предприятий Тверской области», в целях обеспечения защиты информации, обрабатываемой в информационных системах Администрации Удомельского городского округа

1. Утвердить Политику информационной безопасности Администрации Удомельского городского округа (Приложение).
2. Руководителям органов Администрации Удомельского городского округа разработать Политику информационной безопасности и обеспечить ее размещение на официальном сайте Администрации Удомельского городского округа.
3. Разместить настоящее распоряжение на официальном сайте муниципального образования Удомельский городской округ в информационно-телекоммуникационной сети «Интернет».
4. Отделу организационной работы, муниципальной службы и хозяйственного обеспечения Администрации Удомельского городского округа (Л.В. Семенова) ознакомить с настоящим распоряжением под роспись всех работников Администрации Удомельского городского округа.
5. Настоящее распоряжение вступает в силу со дня его подписания.

Глава Удомельского городского округа Р.А. Рихтер

Приложение
к распоряжению Администрации
Удомельского городского округа
от 29.01.2019 № 60-ра

Политика
информационной безопасности
Администрации Удомельского городского округа

1. Общие положения

1.1. Политика информационной безопасности Администрации Удомельского городского округа (далее – Политика), представляет собой совокупность правил, процедур, практических приемов и общих принципов защиты информации, определяющих особенности эксплуатации информационных систем Администрации Удомельского городского округа (далее – информационные системы), которыми руководствуется Администрация Удомельского городского округа (далее – Администрации) при создании и эксплуатации информационных систем.

1.2. Целями реализации Политики являются минимизация ущерба от реализации угроз безопасности информации, повышение деловой репутации и корпоративной культуры работников Администрации при использовании ими информационных технологий.

1.3. В ходе реализации Политики Администрации руководствуются следующими принципами:

1.3.1. принцип законности, в соответствии с которым все организационные мероприятия должны соответствовать федеральному законодательству и законодательству Тверской области в сфере защиты информации;

1.3.2. принцип комплексного подхода к обеспечению информационной безопасности, при котором обеспечить ее необходимый уровень возможно только путем совокупности организационных мероприятий и технических мер, включающих в себя физическую охрану носителей информации, использование категорий информации для обозначения уровня конфиденциальности документов, подбор и подготовку кадров в сфере информационной безопасности, использование технических средств защиты информации, обучение работников, расследование инцидентов информационной безопасности;

1.3.3. принцип непрерывности, в соответствии с которым обеспечение информационной безопасности является постоянным процессом, который состоит из регулярных проверок актуальности угроз информационной безопасности, проверок адекватности мер защиты существующим угрозам информационной безопасности, регулярной модернизации средств защиты информации, своевременного повышения квалификации специалистов, иных мероприятий;

1.3.4. принцип специализации, который подразумевает возможность привлекать для проектирования и внедрения специальных программных и технических средств защиты специалистов, имеющих соответствующий опыт, или организации, имеющие лицензию на соответствующий вид деятельности;

1.3.5. принцип экономической целесообразности, в соответствии с которым при реализации мероприятий по обеспечению информационной безопасности расходы местного бюджета Удомельского городского округа на эти цели соизмеряются с вероятным ущербом от реализации угроз информационной безопасности;

1.3.6. принцип своевременности, подразумевающий упреждающий характер мероприятий по обеспечению информационной безопасности, прогнозирование появления угроз информационной безопасности на этапе проектирования информационных систем Администрации и осуществление модернизации средств защиты информации при внесении изменений в существующие информационные системы Администрации;

1.3.7. принцип взаимодействия, предполагающий взаимодействие и распределение зон ответственности при обеспечении информационной безопасности, а также организацию сотрудничества в этой сфере со сторонними экспертами и организациями – лицензиатами, а также федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации.

1.4. В целях реализации требований Политики в Администрации назначается администратор информационной безопасности из числа работников Администрации.

1.5. Для целей Политики применяются следующие термины:

1.5.1. администратор информационной безопасности – должностное лицо Администрации, ответственное за соблюдение требований законодательства в сфере защиты информации;

1.5.2. вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы информационной системы;

1.5.3. инцидент информационной безопасности – любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность Администрации (утрата услуг, оборудования или устройств, системные сбои или перегрузки, ошибки пользователей, несоблюдение политики информационной безопасности, нарушение физических мер защиты, неконтролируемые изменения информационных систем, сбои программного обеспечения и отказы технических средств, нарушение правил доступа);

1.5.4. лицензионное программное средство – программное средство, использование одной или нескольких копий которого осуществляется на основе лицензии – правового инструмента, определяющего использование и распространение программного средства, защищенного авторским правом;

1.5.5. масштаб информационной системы:

федеральный – если информационная система функционирует на территории Российской Федерации (в пределах федерального округа) и имеет сегменты (технические средства информационных систем) в субъектах Российской Федерации, муниципальных образованиях и (или) организациях;

региональный (межведомственный) – если информационная система функционирует на территории Тверской области и имеет сегменты (технические средства информационных систем) в одном или нескольких муниципальных образованиях Тверской области и (или) подведомственных и иных организациях Тверской области;

объектовый – если информационная система функционирует на объектах одного федерального органа исполнительной власти, ИОГВ Тверской области (государственного учреждения, унитарного предприятия Тверской области), муниципального образования Тверской области и (или) организации и не имеет сегментов (технических средств информационных систем) в территориальных органах, представительствах, филиалах, подведомственных и иных организациях;

1.5.6. несанкционированный доступ к информации – доступ к информации, нарушающий установленные правила ее получения;

1.5.7. пользователь информационной системы (средства вычислительной техники) – лицо, участвующее в функционировании информационной системы (средства вычислительной техники) или использующее результаты ее функционирования;

1.5.8. программное обеспечение – совокупность программных средств и программных продуктов;

1.5.9. программное средство – объект, состоящий из программ, процедур, правил, а также, если предусмотрено, сопутствующих им документов и данных, относящихся к функционированию информационной системы;

1.5.10. программный продукт – программное средство, предназначенное для поставки, передачи, продажи пользователю;

1.5.11. средство криптографической защиты информации (далее также – СКЗИ) – аппаратные, программно-аппаратные и программные средства, осуществляющее криптографическое преобразование информации для обеспечения ее безопасности;

1.5.12. средство вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем;

1.5.13. сервер – компьютер, выделенный из группы персональных компьютеров для выполнения какой-либо сервисной задачи без непосредственного участия человека;

1.5.14. спам – телематическое электронное сообщение, предназначенное неопределенному кругу лиц, доставленное абоненту и (или) пользователю без их предварительного согласия и не позволяющее определить отправителя этого сообщения, в том числе ввиду указания в нем несуществующего или фальсифицированного адреса отправителя;

1.5.15. учетная запись «Администратор» – учетная запись пользователя информационной системы, позволяющая вносить изменения в настройки информационной системы, затрагивающие всех пользователей информационной системы (изменение параметров безопасности, установка программного обеспечения, работа с любыми файлами в информационной системе, изменение параметров учетных записей других пользователей).

2. Классификация информационных систем Администрации

2.1. Информационные системы Администрации могут содержать общедоступную информацию и информацию ограниченного доступа.

2.2. В зависимости от категории информации, содержащейся в информационных системах, информационные системы подразделяются на следующие типы:

2.2.1. информационные системы, содержащие сведения, представляющие общедоступную информацию;

2.2.2. информационные системы, содержащие сведения, составляющие государственную тайну;

2.2.3. информационные системы, содержащие служебные сведения ограниченного доступа;

2.2.4. информационные системы персональных данных.

3. Инвентаризация информационных систем Администрации

3.1. Инвентаризация информационных систем (далее – инвентаризация) проводится в Администрации не реже одного раза в год.

Целью инвентаризации является получение полной и достоверной информации об объеме и составе информационных систем и их технических средств, для обеспечения безопасности информации при их эксплуатации.

В перечень информационных систем, подлежащих инвентаризации, могут быть включены любые информационные системы, указанные в пункте 2.2. Политики, независимо от их местонахождения.

Основанием для проведения инвентаризации является распоряжение Администрации.

3.2. Для проведения инвентаризации в Администрации распоряжением Администрации создается инвентаризационная комиссия. В распоряжении о создании инвентаризационной комиссии устанавливаются сроки проведения инвентаризации, утверждаются председатель, а также персональный состав инвентаризационной комиссии, в который могут быть включены:

3.2.1. заместитель Главы Администрации Удомельского городского округа, ответственный за организацию защиты информации;

3.2.2. работник, осуществляющий бухгалтерский (бюджетный) учет;

3.2.3. администратор информационной безопасности.

3.3. Инвентаризация включает следующие мероприятия:

3.3.1. описание информационной системы, в котором отражаются границы информационной системы, размещение ее технических средств и поддерживающей инфраструктуры применительно к организационной структуре Администрации, определяется масштаб информационной системы;

3.3.2. определение типа информационной системы в зависимости от категории, обрабатываемой в ней информации;

3.3.3. группировка по отдельным признакам (например, по тематикам) файлов, созданных пользователями, не отнесенных ни к одной из информационных систем, но представляющих информационную ценность для Администрации;

3.3.4. определение порядка использования информационных систем, в ходе которого уточняется эксплуатируется ли указанная информационная система только в интересах Администрации или же используется совместно с пользователями других исполнительных органов государственной власти Тверской области, государственных учреждений Тверской области и государственных унитарных предприятий Тверской области, указывается количество пользователей информационной системы, а также определяется должностное лицо, ответственное за ее эксплуатацию;

3.3.5. уточнение комплекса мероприятий по поддержанию, развитию, совершенствованию и защите информационных систем.

3.4. На основе данных, полученных по итогам инвентаризации, администратор информационной безопасности составляет перечень информационных систем Администрации в соответствии с Приложением 1 к Политике, а также составляет или уточняет перечень данных, подлежащих резервному копированию и хранению в Администрации в соответствии с Приложением 2 к Политике. Перечни информационных систем Администрации передаются в исполнительный орган власти Тверской области, уполномоченный в сфере информационных технологий, для занесения в реестр информационных систем Тверской области.

4. Управление доступом к информационным системам Администрации

4.1. Основные правила и методы защиты информационных систем от несанкционированного доступа:

4.1.1. для управления доступом к информационным системам в Администрации вводится разрешительная система допуска пользователей (обслуживающего персонала) к информационным системам и связанным с их использованием работам и документам;

4.1.2. для входа в информационную систему используется парольная аутентификация, при необходимости – другие способы аутентификации;

4.1.3. при любом оставлении работником рабочего места средство вычислительной техники информационной системы должно блокироваться и требовать аутентификации для дальнейшего продолжения работы;

4.1.4. каждому работнику Администрации, имеющему право доступа к информационной системе, присваивается отличная от других учетная запись пользователя;

4.1.5. каждый работник при получении переданного ему пароля доступа к информационной системе или иных средств аутентификации информируется, что он предупрежден о необходимости сохранять полученный пароль в тайне, не передавать вверенный ему пароль или иные средства аутентификации третьим лицам, в том числе другим работникам Администрации.

4.2. Разрешительная система допуска пользователей к информационным системам и связанным с их использованием работам и документам подразумевает:

4.2.1. вход в информационные системы с помощью учетной записи, относящейся к типу «Администратор», разрешен только лицам, уполномоченным на выполнение административных функций в информационных системах;

4.2.2. вход в информационные системы остальным пользователям разрешен только с использованием ограниченной учетной записи, позволяющей им обрабатывать информацию в

данных информационных системах исключительно в рамках их компетенции для исполнения своих должностных обязанностей;

4.2.3. работникам разрешено использовать только те учетные записи, которые присвоены им в порядке, определенном Политикой;

4.2.4. учетные записи уволенных работников, а также любого работника, который не осуществлял доступ к информационной системе в течение трех месяцев, должны быть заблокированы и/или удалены из информационной системы. Для возобновления доступа данный работник должен вновь пройти процедуру получения прав доступа к информационной системе.

4.3. Настройки средств вычислительной техники информационных систем в штатном режиме должны предусматривать загрузку операционных систем только с жестких дисков и исключать загрузку операционных систем с других носителей.

4.4. Допуск всех работников к работе с информационными системами осуществляется только после их ознакомления с Политикой.

4.5. О выявленных попытках несанкционированного доступа к информационным системам администратор информационной безопасности незамедлительно сообщает Главе Удомельского городского округа Главе Удомельского городского округа служебной запиской.

Главе Удомельского городского округа по факту попытки несанкционированного доступа к информационным системам назначается служебная проверка.

5. Основные правила и методы предотвращения неавторизованного доступа к информации Администрации с использованием парольной аутентификации

5.1. Пароли подразделяются на пароли пользователей информационной системы и пароли администраторов информационной безопасности и относятся к служебным сведениям ограниченного доступа.

5.2. При первоначальном предоставлении пользователю доступа к информационной системе или в случае утери пароля пользователем, администратор информационной безопасности выдает временный пароль, который требуется сменить при первом входе в информационную систему.

5.3. Пароли администратора информационной безопасности подлежат хранению в сейфе у администратора информационной безопасности в запечатанном конверте с указанием наименования информационной системы, должности, фамилии, инициалов должностного лица, ответственного за эксплуатацию информационной системы.

5.4. Порядок хранения и использования паролей определяет администратор информационной безопасности.

5.5. Пароль пользователя информационной системы должен отвечать следующим требованиям:

5.5.1. длина пароля должна быть не менее 8 символов;

5.5.2. пароль не должен содержать в себе имя учетной записи пользователя информационной системы;

5.5.3. в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);

5.5.4. при смене пароля новое значение должно отличаться от предыдущего не менее чем в 2 позициях;

5.5.5. пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, даты рождений и т.д.);

5.5.6. пароль должен изменяться не реже чем один раз в 6 месяцев;

5.5.7. пароль должен быть уникальным по отношению к паролям других учетных записей данного пользователя.

5.6. Пароль администратора информационной безопасности должен отвечать следующим требованиям:

5.6.1. длина пароля должна быть не менее 12 символов;

5.6.2. в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);

5.6.3. при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;

5.6.4. пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, даты рождений и т.д.);

5.6.5. пароль должен изменяться не реже чем один раз в 3 месяца;

5.6.6. пароль должен быть уникальным по отношению к паролям других учетных записей администратора информационной безопасности.

5.7. Запрещается сообщать пароль кому-либо, в том числе при помощи почтовых сообщений, через информационно-телекоммуникационную сеть «Интернет» (далее – ИТКС Интернет), каким-либо иным способом.

5.8. При компрометации пароля пользователь должен сообщить об этом администратору информационной безопасности и незамедлительно сменить пароль.

6. Основные правила и методы организации антивирусной защиты информационных систем Администрации

6.1. Организация антивирусной защиты в Администрации, а также контроль за выполнением мероприятий по антивирусной защите возлагаются на администратора информационной безопасности.

6.2. На администратора информационной безопасности возлагаются следующие функции:

6.2.1. организация выбора средств антивирусной защиты, приобретения, установки на объекты защиты, настройки и сопровождения;

6.2.2. организация и проведение технических мероприятий по антивирусной защите;

6.2.3. разработка документов, устанавливающих правила безопасной работы со средствами вычислительной техники и регламентирующих действия пользователей в ситуациях, связанных с действием вредоносных программ.

6.3. К объектам антивирусной защиты относятся информация, содержащаяся в информационной системе, технические средства информационных систем (в том числе средства вычислительной техники), и предоставляемые ими сервисы (почта и т.д.), машинные носители информации, входящие в состав информационных систем или временно подключаемые к ним, средства и системы связи и передачи данных, общесистемное, прикладное, специальное программное обеспечение, информационные технологии, а также средства защиты информации.

6.4. К средствам антивирусной защиты относятся программы, предназначенные для обнаружения и уничтожения вредоносных программ, а также ликвидации последствий от их воздействий.

6.5. Для антивирусной защиты информационных систем Администрации используются официально приобретенные средства антивирусной защиты.

6.6. Рекомендуется использовать средства антивирусной защиты с возможностью централизованного управления и автоматической установкой обновлений антивирусного программного обеспечения и баз данных признаков вредоносных программ.

6.7. Для периодических проверок объектов антивирусной защиты рекомендуется использовать средства антивирусной защиты различных производителей.

6.8. Не допускается подключение и эксплуатация средств вычислительной техники в информационных системах без установленных и надлежащим образом настроенных активных и актуальных средств антивирусной защиты.

6.9. Пользователям информационных систем запрещается предпринимать попытки отключения, изменения настроек и влияния на работу эксплуатируемых средств антивирусной защиты.

6.10. При возникновении подозрения о наличии на средстве вычислительной техники вредоносных программ (нетипичная работа программного обеспечения, появление графических и звуковых эффектов, искажений данных, исчезновение (несанкционированное уничтожение) файлов, регулярное появление сообщений о системных ошибках и т.п.) пользователи информационных систем самостоятельно или вместе с администратором информационной безопасности проводят внеочередной антивирусный контроль средства вычислительной техники.

6.11. В случае обнаружения вредоносных программ пользователи информационных систем обязаны:

6.11.1. приостановить работу;

6.11.2. немедленно поставить в известность об этом администратора информационной безопасности, владельца зараженных файлов (ресурсов), а также других работников, использующих эти файлы в работе;

6.11.3. совместно с владельцем зараженных файлов (ресурсов) провести анализ необходимости дальнейшего их использования;

6.11.4. провести лечение или уничтожение зараженных файлов.

6.12. В случае обнаружения вредоносных программ администратор информационной безопасности организует внеочередной антивирусный контроль всех средств вычислительной техники информационной системы, в которой обнаружена вредоносная программа.

6.13. Все файлы, полученные из ИТКС Интернет посредством электронной почты, а также копируемые на средства вычислительной техники с любых внешних носителей информации подлежат обязательной проверке средствами антивирусной защиты.

7. Основные правила и методы организации резервного копирования в Администрации

7.1. Ответственным за проведение резервного копирования, хранение резервных копий, а также восстановление информации является администратор информационной безопасности.

7.2. Администратор информационной безопасности в зависимости от функциональных особенностей эксплуатируемых информационных систем определяет перечень данных, подлежащих резервному копированию и хранению, в соответствии с Приложением 2 к Политике, расписание резервного копирования в соответствии с Приложением 3 к Политике.

7.3. Резервному копированию подлежит информация следующих основных категорий:

7.3.1. персональная информация пользователей (личные каталоги на файловых серверах);

7.3.2. групповая информация пользователей (общие каталоги подразделений);

7.3.3. информация, необходимая для восстановления серверов и систем управления базами данных;

7.3.4. персональные профили пользователей сети;

7.3.5. информация правовых справочных систем общего использования («Гарант», «Консультант+» и т.п.);

7.3.6. рабочие копии установочных компонент программного обеспечения вычислительных средств информационных систем Администрации;

7.3.7. регистрационная информация подсистем информационной безопасности информационных систем Администрации.

7.4. Для организации системы резервного копирования используются стандартные программные средства операционной системы либо специализированные лицензионные программные средства резервного копирования.

7.5. Средства резервного копирования должны обеспечивать производительность, достаточную для сохранения копируемой информации.

7.6. Информация с носителей, которые перестают использоваться в системе резервного копирования, стирается без возможности восстановления данных.

7.7. Хранение съемных носителей с резервными копиями осуществляется в отдельных запираемых сейфах, доступ к которым имеет только администратор информационной безопасности.

7.8. Все процедуры по загрузке, выгрузке носителей, на которые производится резервное копирование, а также любое перемещение съемных носителей осуществляются администратором информационной безопасности.

7.9. Основанием для инициирования процедуры восстановления служит полная или частичная утрата информации вследствие сбоев оборудования, программного обеспечения в критических и кризисных ситуациях. Восстановление данных производится администратором информационной безопасности.

7.10. О выявленных попытках несанкционированного доступа к резервируемой информации, а также иных нарушениях информационной безопасности, произошедших в процессе резервного копирования, администратор информационной безопасности сообщает Главе Удомельского городского округа служебной запиской в течение рабочего дня после обнаружения указанного события.

7.11. Главой Удомельского городского округа по факту попытки несанкционированного доступа к резервируемой информации назначается служебная проверка.

7.12. Контроль результатов резервного копирования осуществляется администратором информационной безопасности. В случае обнаружения ошибки резервного копирования или выхода из строя системы резервного копирования администратор информационной безопасности выполняет повторное копирование информации вручную в максимально сжатые сроки, не нарушая технологические процессы обработки информации пользователями.

8. Порядок работы с электронной почтой в Администрации

8.1. Электронная почта в Администрации должна использоваться только в служебных целях.

8.2. При работе с электронной почтой работникам Администрации запрещается:

8.2.1. использовать адрес служебной электронный почты в личных целях;

8.2.2. публиковать свой адрес служебной электронный почты либо адреса других работников на общедоступных интернет-ресурсах (форумы, конференции и т.п.) без предварительного согласования с руководителем отдела;

8.2.3. отправлять сообщения с вложенными файлами, общий размер которых превышает максимально допустимый;

8.2.4. открывать вложенные файлы во входящих сообщениях без предварительной проверки антивирусными средствами;

8.2.5. осуществлять массовую рассылку почтовых сообщений (более 10) внешним адресатам, если это не обусловлено служебной необходимостью;

8.2.6. осуществлять рассылку материалов, содержащих вредоносные программы, или файлы, предназначенные для нарушения, уничтожения либо ограничения функциональности электронного оборудования или программного обеспечения, для осуществления несанкционированного доступа, а также серийные номера к коммерческим программным продуктам и программное обеспечение для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в ИТКС Интернет, а также ссылки на вышеуказанную информацию;

8.2.7. распространять защищаемые авторскими правами материалы, затрагивающие какой-либо патент, торговую марку, коммерческую тайну, копирайт или прочие права собственности и (или) авторские и смежные с ними права третьей стороны;

8.2.8. распространять информацию, содержание и направленность которой запрещены законодательством Российской Федерации, включая материалы, носящие вредоносную, угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия, и т.д.;

8.2.9. осуществлять отправку сообщений электронной почты с чужого почтового ящика или от чужого имени;

8.2.10. распространять посредством сообщений электронной почты информацию, содержащую персональные данные, служебные сведения ограниченного доступа, сведения, относящиеся к государственной тайне.

9. Порядок использования ИТКС Интернет в Администрации

9.1. Доступ к ИТКС Интернет в Администрации может предоставляться работникам в целях выполнения ими своих служебных обязанностей.

9.2. Подключение средств вычислительной техники к ИТКС Интернет выполняется администратором информационной безопасности.

9.3. Средства вычислительной техники, используемые для обработки сведений, составляющих государственную тайну, не могут быть подключены к ИТКС Интернет.

9.4. При использовании ИТКС Интернет работникам Администрации запрещено:

9.4.1. использовать предоставленный доступ к ИТКС Интернет в личных целях;

9.4.2. использовать специализированные аппаратные и программные средства, позволяющие работникам получить несанкционированный доступ к ИТКС Интернет;

9.4.3. совершать действия, направленные на нарушение функционирования элементов информационных систем;

9.4.4. публиковать, загружать и распространять материалы, содержащие:

информацию ограниченного доступа;

информацию, полностью или частично защищенную авторскими или другими правами, без разрешения владельца;

вредоносное программное обеспечение, предназначенное для нарушения, уничтожения либо ограничения функциональности любых аппаратных и программных средств, для осуществления несанкционированного доступа, а также серийные номера к коммерческому программному обеспечению и программное обеспечение для их генерации, пароли и прочие средства для получения несанкционированного доступа к платным интернет-ресурсам, а также ссылки на вышеуказанную информацию;

угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности и т.д.

9.5. При необходимости администратор информационной безопасности блокирует доступ к интернет-ресурсам, содержание которых не имеет отношения к исполнению служебных обязанностей.

10. Использование программного обеспечения в информационных системах Администрации

10.1. В Администрации для выполнения возложенных на неё функций разрешено применение ограниченного перечня коммерческого и свободного программного обеспечения.

10.2. Перечень программного обеспечения, разрешенного к использованию в Администрации определяется администратором информационной безопасности. Разрешенное к использованию программное обеспечение заносится в реестр разрешенного к использованию программного обеспечения в соответствии с Приложением 4 к Политике и утверждается Главой Удомельского городского округа.

10.3. Перечень программного обеспечения, устанавливаемого на средство вычислительной техники, определяется администратором информационной безопасности исходя из должностных обязанностей пользователя, а также функций информационной системы Администрации и

заносится администратором информационной безопасности в паспорт средства вычислительной техники в соответствии с Приложением 5 к Политике.

10.4. Установка и использование программного обеспечения, не занесенного в реестр разрешенного к использованию программного обеспечения, запрещается.

10.5. Все операции по установке, сопровождению, удалению программного обеспечения выполняются администратором информационной безопасности, или техническими специалистами других организаций, привлекаемыми на основании гражданско-правовых договоров, при непосредственном участии администратора информационной безопасности.

10.6. Эксплуатация программного обеспечения состоит из следующих этапов:

10.6.1. определение потребности в программном обеспечении;

10.6.2. приобретение программного обеспечения;

10.6.3. установка (внедрение) программного обеспечения;

10.6.4. поддержка и сопровождение программного обеспечения;

10.6.5. удаление (вывод из эксплуатации) программного обеспечения.

10.7. В ходе определения потребности в программном обеспечении руководителем структурного подразделения Администрации, в котором планируется эксплуатация данного программного обеспечения, готовится заявка на установку программного обеспечения на имя Главы Удомельского городского округа:

10.7.1. при необходимости организации нового рабочего места, оснащенного средствами вычислительной техники;

10.7.2. при необходимости выполнения работниками новых (дополнительных) обязанностей, для которых требуются дополнительное программное обеспечение или полная замена технических средств информационной системы;

10.7.3. при появлении качественно нового (альтернативного) программного обеспечения взамен уже используемых в составе информационных систем (при необходимости).

10.8. При наличии в Администрации необходимого программного обеспечения администратор информационной безопасности выполняет работы по его установке, за средством вычислительной техники закрепляются лицензии на установленное на нем программное обеспечение.

При отсутствии в Администрации запрошенного программного обеспечения или вакантных лицензий на коммерческое программное обеспечение (из перечня в реестре разрешенного к использованию программного обеспечения), руководитель структурного подразделения Администрации инициирует заявку на приобретение программного обеспечения.

10.9. При установке (внедрении) программного обеспечения администратор информационной безопасности:

10.9.1. обеспечивает оперативный учет лицензий вводящегося в эксплуатацию программного обеспечения, организует работы по установке программного обеспечения на средства вычислительной техники;

10.9.2. готовит два экземпляра паспорта средства вычислительной техники или вносит изменения в имеющийся паспорт средства вычислительной техники. Один экземпляр паспорта средства вычислительной техники остается у работника структурного подразделения Администрации, являющегося оператором средства вычислительной техники, другой хранится в архиве документов администратора информационной безопасности.

10.10. Любое изменение перечня установленного программного обеспечения отражается в паспорте средства вычислительной техники.

10.11. После установки программного обеспечения установочные комплекты (дистрибутивы) передаются администратору информационной безопасности.

10.12. Должностные лица, ответственные за эксплуатацию информационной системы, должны обеспечивать сохранность переданных им носителей с ключевой информацией, лицензионным программным обеспечением, сертификатов подлинности программного обеспечения.

10.13. Поддержка и сопровождение программного обеспечения выполняется администратором информационной безопасности, а при необходимости – техническими специалистами других организаций, привлекаемыми на основании гражданско-правовых договоров.

10.14. Осуществление поддержки и сопровождения программного обеспечения предусматривает, в том числе, выполнение следующих видов работ:

10.14.1. настройка установленного программного обеспечения;

10.14.2. установка обновлений программного обеспечения;

10.14.3. регламентированное создание резервных копий (архивирование) программного обеспечения и пользовательских данных (электронных документов, баз данных);

10.14.4. устранение неисправностей, связанных с использованием установленного программного обеспечения;

10.14.5. консультирование пользователей информационных систем.

10.15. Удаление (вывод из эксплуатации) программного обеспечения проводится в случаях:

10.15.1. окончания лицензионного срока использования программного обеспечения;

10.15.2. замены используемого программного обеспечения на альтернативное программное обеспечение или программное обеспечение более поздних версий;

10.15.3. прекращения использования программного обеспечения вследствие отсутствия необходимости, морального старения.

10.16. Вывод из эксплуатации выполняется администратором информационной безопасности, а при необходимости техническими специалистами других организаций, привлекаемыми на основании гражданско-правовых договоров.

10.17. При удалении (выводе из эксплуатации) программного обеспечения производится:

10.17.1. аудит программного обеспечения (далее – аудит) Администрации;

10.17.2. удаление выводимого из эксплуатации программного обеспечения со всех средств вычислительной техники информационных систем;

10.17.3. при необходимости подготовка и передача в структурное подразделение Администрации, осуществляющее бухгалтерский учет, акта вывода из эксплуатации программного обеспечения;

10.17.4. соответствующие отметки в паспортах средств вычислительной техники.

10.18. При необходимости администратор информационной безопасности организует хранение выведенного из эксплуатации программного обеспечения.

10.19. Аудит проводится в целях выявления несоответствия перечней фактически установленного программного обеспечения на средствах вычислительной техники перечням, зафиксированным в паспортах средств вычислительной техники. Аудит проводит администратор информационной безопасности.

10.20. При выявлении несоответствия перечня установленного программного обеспечения текущей версии паспорта средства вычислительной техники программное обеспечение, наименование которого отсутствует в паспорте средства вычислительной техники, подлежит немедленному удалению. Администратор информационной безопасности в этом случае вправе инициировать проведение служебной проверки для установления обстоятельств установки программного обеспечения, не предусмотренного паспортом средства вычислительной техники, а также выявления лиц, осуществивших эти действия.

10.21. Аудит проводится по мере необходимости, но не реже одного раза в 6 месяцев. Необходимость, время и область проведения аудита определяются в соответствии с настоящей Политикой заместителем Главы Администрации Удомельского городского округа, ответственным за организацию защиты информации.

11. Использование беспроводных сетей в информационных системах Администрации

11.1. В Администрации разрешено использование «гостевых» беспроводных сетей, физически не пересекающихся с локально-вычислительными сетями Администрации.

11.2. Запрещается подключение беспроводных сетей, а также доступ к локально-вычислительным сетям Администрации с различных устройств с использованием беспроводных сетей.

12. Использование носителей информации в информационных системах Администрации

12.1. Под использованием носителей информации в информационных системах понимается их подключение к информационным системам для приема, обработки, передачи информации между информационными системами и мобильными устройствами, носителями информации.

12.2. В информационных системах допускается использование только учтенных носителей информации, которые являются собственностью Администрации и подвергаются регулярной ревизии (контролю).

12.3. На учтенных носителях информации допускается использование коммерческого программного обеспечения, входящего в реестр разрешенного к использованию программного обеспечения.

13. Порядок регистрации должностных лиц в межведомственных системах Администрации

13.1. К межведомственным информационным системам Администрации относятся системы электронного документооборота, системы корпоративной электронной почты, реестр государственных служащих Удомельского городского округа, иные территориально распределенные межведомственные информационные системы Администрации (далее – межведомственные информационные системы).

13.2. Глава Удомельского городского округа направляет в областной исполнительный орган государственной власти Тверской области, уполномоченный на подключение к межведомственной информационной системе, заявку на регистрацию в межведомственной информационной системе должностных лиц, которая должна содержать:

13.2.1. наименование межведомственной информационной системы, в которой регистрируются должностные лица Администрации;

13.2.2. должности, фамилии, имена и отчества должностных лиц, регистрируемых в межведомственной информационной системе.

Заявка также может содержать другую определяемую областным исполнительным органом государственной власти Тверской области, уполномоченным на подключение к межведомственной информационной системе информацию, включаемую в идентификационные данные.

13.3. После получения от Администрации заявки на регистрацию должностных лиц в межведомственной информационной системе, ответственное должностное лицо областного исполнительного органа государственной власти Тверской области, уполномоченного на подключение к межведомственной информационной системе, регистрирует пользователей и проводит необходимые настройки.

13.4. Ответственное должностное лицо областного исполнительного органа государственной власти Тверской области, уполномоченного на подключение к межведомственной информационной системе, направляет необходимую ключевую информацию (ключевые файлы) администратору информационной безопасности Администрации, подавшего заявку.

13.5. При увольнении должностного лица, зарегистрированного в межведомственной информационной системе, Глава Удомельского городского округа в трехдневный срок со дня увольнения направляет в исполнительный орган государственной власти Тверской области, уполномоченный на подключение к межведомственной информационной системе, заявку

об исключении уволенного работника из пользователей межведомственной информационной системы.

14. Порядок использования средств криптографической защиты информации в Администрации

14.1. Работы по приобретению средств криптографической защиты информации проводятся Администрацией Удомельского городского округа по согласованию с уполномоченным областным исполнительным органом государственной власти Тверской области в сфере защиты информации.

14.2. Для работы с СКЗИ привлекаются уполномоченные должностные лица, назначенные соответствующим приказом Администрации, которые получают и используют сертификаты ключей проверки электронной подписи и ключи электронной подписи (далее – ключевая информация) и несут персональную ответственность за:

14.2.1. сохранение в тайне сведений конфиденциального характера, ставших им известными в процессе работы с СКЗИ;

14.2.2. сохранение в тайне содержания ключевой информации;

14.2.3. сохранность носителей ключевой информации и других документов о ключах, выдаваемых с ключевыми носителями.

14.3. В ИОГВ Тверской области, государственных учреждениях, унитарных предприятиях Тверской области, участвующих в информационном обмене электронными документами по телекоммуникационным каналам связи, должны быть обеспечены условия хранения носителей ключевой информации и карточки отзыва ключей, исключающие возможность доступа к ним посторонних лиц, несанкционированного использования или копирования ключевой информации и паролей отзыва ключей.

14.4. На средствах вычислительной техники информационных систем, на которых установлены средства шифрования и электронной подписи, не должно быть установлено и эксплуатироваться программное обеспечение, которое может нарушить функционирование программных СКЗИ. При обнаружении на рабочем месте, оборудованном СКЗИ, программного обеспечения, нарушающего работу указанных средств, работа с СКЗИ на данном рабочем месте должна быть прекращена и должны быть организованы мероприятия по анализу и ликвидации негативных последствий инцидента информационной безопасности.

14.5. При работе с СКЗИ не допускается:

14.5.1. разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей и принтер;

14.5.2. вставлять ключевой носитель в интерфейс технического средства информационной системы при проведении работ, не являющихся штатными процедурами использования ключей, а также в интерфейсы других технических средств информационной системы;

14.5.3. записывать на носителе ключевой информации постороннюю информацию;

14.5.4. вносить какие-либо изменения в программное обеспечение средств шифрования и электронной подписи;

14.5.5. использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации путем переформатирования (при наличии возможности).

14.6. Посторонние лица не должны допускаться к работе со средствами вычислительной техники, на которых установлены средства шифрования и электронной подписи.

14.7. Уполномоченные должностные лица Администрации, привлекаемые для работы с СКЗИ, отвечают за сохранность и конфиденциальность ключевой информации. В случае компрометации ключевой информации мероприятия по розыску и локализации последствий компрометации конфиденциальной информации, переданной с использованием СКЗИ, организует Глава Удомельского городского округа, а осуществляют уполномоченные должностные лица

Администрации, привлекаемые для работы с СКЗИ, и администратор информационной безопасности.

14.8. При компрометации ключевой информации должностного лица Администрации данное должностное лицо должно немедленно прекратить действия, связанные с использованием данной ключевой информации, и поставить в известность представителя удостоверяющего центра о факте компрометации.

15. Управление сетевой безопасностью при использовании сетевых ресурсов Администрации

15.1. Пользователям информационно-телекоммуникационной сети Администрации запрещается:

15.1.1. осуществлять попытки несанкционированного проникновения в чужие информационные системы;

15.1.2. производить попытки присвоения себе чужих сетевых атрибутов (в частности сетевых адресов, MAC-адресов сетевых карт);

15.1.3. предоставлять ресурсы своих технических средств посторонним пользователям для несанкционированного использования государственных информационных ресурсов Тверской области;

15.1.4. размещать в информационных системах коммерческие и лицензионные программные средства, мультимедийные и информационные материалы с нарушением соответствующих авторских прав;

15.1.5. распространять через информационно-телекоммуникационную сеть заведомо оскорбляющую честь и унижающую достоинство граждан информацию, материалы рекламного и коммерческого характера;

15.1.6. использовать внешний мультимедийный трафик типа интернет-видео, музыкальных сетевых радиостанций, а также трафик пиринговых сетей, если это не связано с исполнением служебных обязанностей. При возникновении трафика данного типа соответствующие сетевые коммуникации должны блокироваться администратором информационной безопасности без предупреждения пользователя.

15.2. На технических средствах информационных систем, используемых для работы в информационно-телекоммуникационной сети Администрации, рекомендуется устанавливать все обновления программного обеспечения.

15.3. Мероприятия по обеспечению безопасности должны проводиться в отношении всех объектов информационно-телекоммуникационной сети, в том числе и тех, которые подключены, но временно не используются.

15.4. При существенном падении скорости передачи данных в информационно-телекоммуникационной сети администратор информационной безопасности организует временную блокировку проблемного трафика до устранения самого проблемного трафика и вызвавших его причин.

15.5. Администратор информационной безопасности по согласованию с руководителем Администрации с целью защиты сетевой инфраструктуры и пользователей может блокировать спам и вирусные рассылки (как входящие, так и исходящие) вплоть до временного прекращения всех коммуникаций с хостами, вовлеченными в эти инциденты информационной безопасности (спамовые рассылки, вирусные и хакерские атаки), даже если это повлечет за собой временную невозможность доступа пользователей к легальным ресурсам этих хостов.

15.6. Особо крупные сетевые скачивания (дистрибутивы, ISO-образы дисков и т.п.) рекомендуется производить только с доверенных серверов и в нерабочее время, когда загрузка канала существенно меньше.

15.7. Системные часы серверов и персональных компьютеров информационно-телекоммуникационной сети Администрации синхронизируются с точным источником времени.

Информационная система Администрации настраивается таким образом, чтобы изменение настроек даты и времени было доступно только администратору информационной безопасности.

16. Обеспечение безопасности информации при ведении переговоров и использовании средств связи в Администрации

16.1. В целях обеспечения конфиденциальности телефонных переговоров в Администрации не рекомендуется передавать по телефону информацию, содержащую служебные сведения ограниченного доступа, персональные данные, данные о времени и местонахождении членов Правительства Тверской области, руководителей Администрации, если это не обусловлено служебной необходимостью.

16.2. В случае необходимости проведения конфиденциальных переговоров, такие переговоры проводятся в специально предназначенных для этого помещениях.

16.3. При необходимости обеспечения конфиденциальности информации при ведении переговоров в помещениях для проведения данных переговоров не должны находиться приборы, оборудование и технические средства, которые непосредственно не используются для обеспечения хода переговоров (телефоны городской сети, вычислительные средства информационных систем, телевизионные и радиоприемники и др.). Все мобильные телефоны рекомендуется оставлять за пределами помещения, где проводятся данные мероприятия.

16.4. Для предотвращения утечки акустической информации целесообразно использовать внешние шумы (специальное оборудование, работающее радио, телевизор и т.п.).

17. Обеспечение физической защиты информационных систем Администрации

17.1. Физическая защита информационных систем Администрации обеспечивается комплексом мер по оборудованию зданий (помещений) средствами охранной сигнализации, организации постов охраны, опечатыванию помещений, организации и соблюдению внутриобъектового и пропускного режимов, порядка доступа в служебные помещения, хранению ключей от служебных помещений.

17.2. Физический доступ к информационным системам посторонних лиц не допускается.

17.3. Время прохода работников в здания Администрации устанавливается правилами внутреннего служебного распорядка.

17.4. Пропускной режим Администрации устанавливается в соответствии с распоряжением Администрации Удомельского городского округа от 16.08.2018 № 913-ра «Об организации пропускного режима в административное здание Администрации Удомельского городского округа».

17.5. При отсутствии в помещениях работников Администрации двери в эти помещения должны быть закрыты на ключ. Вскрытие помещений при отсутствии лиц, имеющих на это право, осуществляется с разрешения руководителя отдела организационной работы и муниципальной службы Администрации.

17.6. В целях физической охраны серверов, информационных систем и баз данных, расположенных на выделенных технических средствах информационных систем, такие технические средства (при наличии возможности) размещаются в специально выделенных для этих целей помещениях. Доступ к таким техническим средствам ограничивается физически.

17.7. Двери помещений должны иметь достаточную степень защиты от возможного несанкционированного проникновения, быть исправными, хорошо подогнанными под максимально укрепленную дверную коробку.

Двери помещений и решетки на окнах (при их наличии) оснащаются замками и запирающими устройствами, обеспечивающими достаточную степень защиты от взлома. В качестве запирающих устройств, устанавливаемых на дверях и окнах, применяются врезные,

накладные замки, задвижки, засовы, шпингалеты и т.п. Для запирания оконных решеток допускается применять висячие замки.

17.8. Окна, фрамуги и форточки (стеклопакеты) всех помещений закрываются на надежные и исправные запоры. Стекла надежно закрепляются в пазах. Не допускается эксплуатация поврежденного остекления окон.

17.9. Ключи от замков на оконных решетках (при их наличии) и дверях запасных выходов располагаются в непосредственной близости от них, при этом принимаются меры, исключающие несанкционированный доступ к этим ключам посторонних лиц.

17.10. В Администрации наряду с рабочими комплектами ключей при необходимости предусматриваются дополнительные комплекты ключей от всех помещений, распашных металлических решеток (при их наличии), основных и запасных выходов. Запасные комплекты ключей с соответствующими бирками находятся у вахтера Администрации.

17.11. Все экземпляры ключей учитываются в журнале регистрации ключей к замкам помещений Администрации. В указанный журнал вносится фамилия и должность работников, от какого из помещений получены (сданы) ключи, с личной подписью работника, получившего (сдавшего) экземпляр ключа. Наличие неучтенных ключей не допускается. В случае утраты рабочих или запасных экземпляров ключей об этом немедленно ставится в известность Глава Удомельского городского округа.

17.12. При необходимости опечатывания помещений работникам выдаются номерные печати Администрации (далее – номерные печати). Выдача номерных печатей оформляется приказом Администрации и осуществляется под личную подпись в специальном журнале. работники, имеющие номерные печати, несут персональную ответственность за их сохранность. Проверки фактического наличия ключей от хранилищ и номерных печатей проводятся руководителем структурного подразделения Администрации не реже одного раза в месяц.

17.13. Должностные лица Администрации, осуществляющие сдачу помещений под охрану и их опечатывание, проверяют:

17.13.1. работоспособность средств охранной сигнализации (при ее наличии);

17.13.2. выключение освещения и потребителей электрической энергии (за исключением потребителей, питание которых необходимо непрерывно);

17.13.3. закрытие окон, решеток, форточек, закрытие и опечатывание дверей запасных выходов и размещение ключей от них в опечатанном виде рядом с дверями.

17.14. При необходимости опечатывания помещения печать на входную дверь в помещение проставляется на тонкий слой пластилина или специальной мастики таким образом, чтобы оттиск невозможно было снять и восстановить.

17.15. Ключи от помещений сдаются вахтеру Администрации.

17.16. При снятии помещений с охраны ответственные должностные лица:

17.16.1. после отключения сигнализации (при ее наличии) проверяют целостность печати на дверях и замках;

17.16.2. при обнаружении каких-либо повреждений замков, дверей, окон, форточек, фрамуг, не вскрывая их, вызывают представителей службы охраны и сообщают руководителю Администрации для составления акта осмотра и проведения служебной проверки.

17.17. Для обеспечения электробезопасности информационных ресурсов Тверской области подключение информационных систем к электрической сети осуществляется в соответствии с государственными стандартами Российской Федерации, строительными нормами и правилами, а также правилами технической эксплуатации электроустановок потребителей, утвержденными приказом Министерства энергетики Российской Федерации от 13.01.2003 № 6 «Об утверждении Правил технической эксплуатации электроустановок потребителей».

17.18. Электропитание подводится к оборудованию от центрального электрического щита через автоматические выключатели. В качестве дополнительной защиты информационных ресурсов используются устройства защитного отключения. Все автоматические выключатели и устройства защитного отключения монтируются в соответствии с нагрузкой, потребляемой оборудованием.

Силовые и телекоммуникационные кабели защищаются от возможного несанкционированного подключения или повреждения.

17.19. Все технические средства информационных систем подключаются к электропитанию через источники бесперебойного питания, обеспечивающие корректное выключение или продолжительную работу.

18. Обслуживание технических средств информационных систем Администрации

18.1. Еженедельное обслуживание технических средств информационных систем выполняется пользователем в соответствии с инструкцией по еженедельному техническому обслуживанию информационной системы (Приложение 6 к Политике).

18.2. Другие виды работ по техническому обслуживанию информационной системы выполняются администратором информационной безопасности, а при необходимости – техническими специалистами других организаций, привлекаемыми на основании гражданско-правовых договоров.

18.3. Ремонтные работы на технических средствах информационных систем осуществляются только администраторами информационной безопасности или техническими специалистами других организаций, привлекаемыми на основании гражданско-правовых договоров.

18.4. О факте выполнения работ по техническому обслуживанию информационных систем администратор информационной безопасности делает соответствующую отметку в журнале учета нештатных ситуаций, выполнения профилактических и ремонтных работ, установки и модификации технических средств и программного обеспечения по форме согласно Приложению 7 к Политике.

19. Управление инцидентами информационной безопасности в Администрации

19.1. Инциденты информационной безопасности подразделяются на:

19.1.1. внутренний инцидент – инцидент, источником которого является нарушитель, состоящий в служебных, трудовых и иных договорных отношениях с Администрацией Удомельского городского округа (далее – внутренний нарушитель). К наиболее распространенным внутренним инцидентам информационной безопасности относятся:

19.1.1.1. утечка сведений конфиденциального характера;

19.1.1.2. неправомерный доступ к информации;

19.1.1.3. удаление информации;

19.1.1.4. компрометация информации;

19.1.1.5. саботаж;

19.1.1.6. мошенничество в информационных системах, с участием внутреннего нарушителя;

19.1.1.7. аномальная сетевая активность;

19.1.1.8. аномальное поведение программного обеспечения;

19.1.1.9. использование средств вычислительной техники Администрации в личных целях или в мошеннических операциях;

19.1.2. внешний инцидент – инцидент, источником которого является нарушитель, не состоящий в служебных, трудовых и иных договорных отношениях с Администрацией Удомельского городского округа (далее – внешний нарушитель). К наиболее распространенным внешним инцидентам относятся:

19.1.2.1. мошенничество в информационных системах с участием внешнего нарушителя;

19.1.2.2. атаки типа «отказ в обслуживании» (DoS), в том числе распределенные (DDoS);

19.1.2.3. перехват и подмена трафика;

19.1.2.4. размещение конфиденциальной/провокационной информации в ИТКС Интернет, касающейся Администрации;

19.1.2.5. взлом, попытка взлома, сканирование сайтов ИОГВ Тверской области (государственных учреждений, унитарных предприятий Тверской области);

19.1.2.6. сканирование сети, попытка взлома сетевых узлов;

19.1.2.7. вирусные атаки;

19.1.2.8. неправомерный доступ к конфиденциальной информации;

19.1.2.9. анонимные письма (письма с угрозами).

19.2. Источником информации об инциденте информационной безопасности могут служить:

19.2.1. сообщения пользователей информационных систем;

19.2.2. уведомления компетентных органов;

19.2.3. данные, полученные на основании анализа электронных журналов регистрации информационных систем, систем защиты.

19.3. При получении сообщения об инциденте информационной безопасности по электронной почте или по телефонному звонку необходимо убедиться в достоверности полученной информации (например, путем совершения «обратного» звонка по указанным в сообщении телефонам, проверки данных, указанных в подписи сообщения или названных при звонке).

19.4. Работник, получивший информацию об инциденте информационной безопасности, сообщает об этом администратору информационной безопасности и руководителю структурного подразделения Администрации.

Администратор информационной безопасности обязан принять меры по локализации инцидента информационной безопасности и минимизации потерь от инцидента информационной безопасности для деятельности Администрации.

19.5. Администратор информационной безопасности регистрирует инцидент в журнале учета нештатных ситуаций, выполнения профилактических и ремонтных работ, установки и модификации технических средств и программного обеспечения.

19.6. Для анализа инцидентов информационной безопасности создается комиссия, в состав которой включаются:

19.6.1. заместитель Главы Администрации, ответственный за организацию защиты информации;

19.6.2. руководитель структурного подразделения Администрации, в котором произошел инцидент;

19.6.3. администратор информационной безопасности.

19.7. Комиссия собирает и анализирует все данные об обстоятельствах инцидента информационной безопасности (электронные письма, журналы событий информационных систем, показания работников и др.), устанавливает факт наличия (отсутствия) утечки информации ограниченного доступа и обстоятельства ей сопутствующие, определяет перечень лиц, виновных в нарушении предписанных мероприятий по защите информации, устанавливает причины и условия, способствовавшие нарушению.

19.8. По итогам работы комиссии заместитель Главы Администрации, ответственный за организацию защиты информации, готовит Главе Удомельского городского округа заключение, в котором указываются причина возникновения инцидента, последствия инцидента, лица, виновные в возникновении инцидента, предложения о наказании виновных лиц и мерах по недопущению подобных инцидентов в будущем.

20. Политика кадровой безопасности в Администрации

20.1. Обучение работников Администрации, имеющих право доступа к информационной системе, правильному обращению с информацией (базами данных), содержащейся в информационной системе, осуществляется должностным лицом, ответственным за эксплуатацию информационной системы, а также администратором информационной безопасности.

20.2. Обучение вопросам защиты информации должно предусматривать необходимость сохранения конфиденциальности всей информации, требующей обеспечения конфиденциальности, циркулирующей в информационной системе.

20.3. Все работники Администрации предупреждаются об условиях конфиденциальности информации о персональных данных субъектов персональных данных, содержащихся в информационных системах, способах и методах защиты информационных систем и недопустимости разглашения такой информации.

21. Политика безопасности при работе с третьими лицами в Администрации

21.1. Все действия по техническому обслуживанию, ремонту, установке и замене технических средств информационных систем, прокладке кабеля, переустановке и обновлению программного обеспечения проводятся исключительно с разрешения Главы Удомельского городского округа в присутствии администратора информационной безопасности.

21.2. Работы, указанные в пункте 20.1. настоящего раздела, регистрируются администратором информационной безопасности в журнале учета нештатных ситуаций, выполнения профилактических и ремонтных работ, установки и модификации технических средств и программного обеспечения.

21.3. При выполнении работ, указанных в пункте 20.1. настоящего раздела, администратор информационной безопасности не должен допускать установку поставщиками в информационных системах дополнительного программного обеспечения (бэкдоров) с целью защиты, изменения и обновления своих продуктов.

21.4. Отчуждаемые носители информации должны пройти полную очистку (безвозвратное стирание информации) с использованием общего или специального программного обеспечения.

Если произвести очистку информации невозможно, то носители информации должны быть физически уничтожены.

21.5. Перед передачей оборудования другим предприятиям и организациям необходимо удалить с него всю информацию, требующую обеспечения конфиденциальности.

21.6. Все работы, указанные в пункте 20.1. настоящего раздела, проводимые сторонними организациями, осуществляются только на основании гражданско-правовых договоров, в которых отдельным пунктом должно определяться обязательство о неразглашении полученной третьими лицами информации ограниченного доступа.

Приложение 1
к Политике информационной безопасности
Администрации Удомельского городского округа

Перечень информационных систем
Администрации Удомельского городского округа

№ п/п	Наименование информационной системы	Тип информационной системы в зависимости от категории информации	Масштаб информационной системы (федеральный, региональный, объектовый)	Количество пользователей информационной системы	Средства вычислительной техники информационной системы		Должностное лицо, ответственное за эксплуатацию информационной системы
					количество	№№ паспортов средств вычислительной техники	

Глава Удомельского городского округа

_____ _____
(подпись) (И.О. Фамилия)

Приложение 2
к Политике информационной безопасности
Администрации Удомельского городского округа

Перечень данных, подлежащих резервному копированию и хранению
Администрации Удомельского городского округа

№ п/п	Наименование данных, подлежащих резервному копированию	Расположение резервной копии	Периодичность копирования	Объем данных, подлежащих резервному копированию (Мбайт)	Срок хранения резервной копии

Глава Удомельского городского округа

_____ _____
(подпись) (И.О. Фамилия)

Приложение 3
к Политике информационной безопасности
Администрации Удомельского городского округа

Расписание резервного копирования
Администрации Удомельского городского округа

Еженедельное копирование

№ п/п	Ресурс	Понедельник	Вторник	Среда	Четверг	Пятница
1	Файловый сервер	Инкрементная копия 1 (23.00)	Инкрементная копия 2 (23.00)	Инкрементная копия 3 (23.00)	Инкрементная копия 4 (23.00)	Полная копия (23.00)
2						

Ежемесячное копирование

№ п/п	Ресурс	Пятница первой недели нового месяца
1	Файловый сервер	Полная копия последней недели прошедшего месяца (23.00)
2		

Годовое копирование

№ п/п	Ресурс	Пятница первой недели первого месяца нового года
1	Файловый сервер	Полная копия последней недели прошедшего месяца (23.00)
2		

Глава Удомельского городского округа _____ _____
(подпись) (И.О. Фамилия)

Приложение 4
к Политике информационной
безопасности Администрации
Удомельского городского округа

Реестр
разрешенного к использованию программного обеспечения
Администрации Удомельского городского округа
период действия с «___»_____ 20__ г. по «___»_____ 20__ г.

№ п/п	Дата включения в реестр	Производитель программного обеспечения	Название программного обеспечения	Область применения программного обеспечения	Количество лицензий на использование программного обеспечения
1	2	3	4	5	6

Глава Удомельского городского округа _____ (подпись) _____ (И.О. Фамилия)

Приложение 5
к Политике информационной
безопасности Администрации
Удомельского городского округа

Паспорт средства вычислительной техники

Номер: _____
Наименование информационной системы: _____
_____

ЭВМ:

Наименование:		Домен:	
Модель:		Сетевой адрес:	
Номер:			

Периферийное оборудование:

1.	Наименование:		Номер:	
	Модель:		Сетевой адрес:	
2.	Наименование:		Номер:	
	Модель:		Сетевой адрес:	
3.	Наименование:		Номер:	
	Модель:		Сетевой адрес:	

Пользователь:

ФИО:		Учетная запись:	
Адрес электронной почты:		Подразделение:	
Группа:		Примечание:	
Телефон:			

Системное программное обеспечение:

Название:	Серийный номер:

Прикладное программное обеспечение:

Издатель:	Продукт:	Серийный номер:

Резервное копирование:

Периодичность	Режим

Примечание: _____

Администратор информационной безопасности: _____ _____
_____ _____

Приложение 6
к Политике информационной
безопасности Администрации
Удомельского городского округа

Инструкция по еженедельному техническому обслуживанию информационной системы

1. Еженедельное техническое обслуживание технических средств информационной системы проводится пользователем не реже 1 раза в неделю в один и тот же день недели.

2. В ходе еженедельного технического обслуживания выполняются следующие виды работ:

2.1. осмотр состояния кабелей, розеток, разъемов;

2.2. удаление загрязнений с внешних поверхностей блоков:

1.1.1. клавиатуры;

1.1.2. манипулятора;

1.1.3. монитора;

1.1.4. принтера;

1.1.5. сканера;

1.1.6. других устройств;

2.3. диагностика технических средств информационной системы, в ходе которой проводятся:

2.3.1. проверка технических средств информационной системы на наличие вирусов с помощью средств антивирусной защиты;

2.3.2. резервное копирование данных;

2.3.3. очистка диска от временных и неиспользуемых файлов с помощью встроенных средств или специального стороннего программного обеспечения;

2.3.4. проверка диска на наличие ошибок;

2.3.5. дефрагментация диска;

2.3.6. проверка работоспособности клавиш клавиатуры и манипулятора;

2.3.7. пробная печать на принтере (при необходимости);

2.3.8. проверка работоспособности сетевого подключения.

3. Для удаления загрязнений в виде пыли с пластмассовых и металлических поверхностей технических средств используется ткань или специальные салфетки. С поверхности монитора жирные пятна удаляются специальными салфетками. Въевшиеся отложения с пластмассовых поверхностей удаляются мыльным раствором (при очистке клавиш необходимо исключить попадание водного раствора вовнутрь клавиатуры и манипулятора). Запрещается использовать для очистки мониторов с антибликовыми покрытиями любые растворы.

4. Перед удалением загрязнений с технических средств информационной системы их необходимо выключить.

5. При обнаружении повреждений электрических розеток, кабелей, в том числе заземления, необходимо срочно вызвать электрика.

6. При проведении технического обслуживания запрещается:

6.1. использовать для очистки жесткие предметы (авторучки, карандаши, ножи, линейки и др.);

6.2. подключать и отключать технические средства информационной системы при включенном электропитании;

6.3. снимать (открывать) крышки системных блоков.

7. При выявлении неисправностей технических средств информационной системы, или программного обеспечения пользователь информационной системы должен немедленно обратиться к администратору информационной безопасности.

Приложение 7
к Политике информационной безопасности
Администрации Удомельского городского округа

Журнал учета нештатных ситуаций, выполнения профилактических и ремонтных работ, установки
и модификации технических средств и программного обеспечения
Администрации Удомельского городского округа

№ п/п	Дата	№ технического средства	Краткое описание выполненной работы, нештатной ситуации	Наименование организации, выполнявшей работы, Ф.И.О. исполнителей и их подписи	Ф.И.О., подпись ответственного пользователя технического средства	Ф.И.О., подпись администратора информационной безопасности	Примечание (реквизиты и краткое содержание заявки)
1	2	3	4	5	6	7	8