АДМИНИСТРАЦИЯ ГОРОДА ПЕРМИ

РАСПОРЯЖЕНИЕ

30.06.2016 № 79

Об утверждении Политики информационной безопасности администрации города Перми

В целях исполнения положений статьей 6, 16 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»:

1. Утвердить прилагаемые:

1.1. Политику информационной безопасности администрации города Перми;

1.2. Регламент утверждения правовых актов города Перми о вводе в эксплуатацию, выводе из эксплуатации (ликвидации) информационных систем и (или) определении порядка эксплуатации информационной системы (далее – Регламент).

2. Руководителям функциональных и территориальных органов, функциональных подразделений администрации города Перми:

обеспечить ознакомление муниципальных служащих, иных работников администрации города Перми, замещающих должности, не отнесенные к должностям муниципальной службы, с настоящим распоряжением под подпись до 31 июля 2016 г.;

являющихся операторами информационных систем, включенных в Реестр информационных систем администрации города Перми, утвержденный распоряжением администрации города Перми от 27 марта 2015 г. № 43, до 31 декабря 2016 г. организовать издание правовых актов города Перми, определяющих порядки эксплуатации информационных систем, в том числе сайтов, в соответствии с утвержденным настоящим распоряжением Регламентом.

3. Настоящее распоряжение вступает в силу с даты подписания.

4. Контроль за исполнением распоряжения возложить на руководителя аппарата администрации города Перми Анисимову Е.Л.

Глава администрации города Перми Д.И. Самойлов

УТВЕРЖДЕНА
распоряжением администрации
города Перми
от 30.06.2016 № 79

ПОЛИТИКА
информационной безопасности администрации города Перми

I. Общие положения

1.1. Настоящая Политика информационной безопасности администрации города Перми (далее – Политика ИБ) разработана в целях установления безопасных способов обработки информации в электронном виде, в том числе в информационных системах (сайтах) администрации города Перми (далее – информационная система).

1.2. Настоящая Политика ИБ определяет в администрации города Перми цели и задачи защиты информации, устанавливает методы защиты информации, которыми должны руководствоваться муниципальные служащие администрации города Перми, иные работники администрации города Перми, замещающие должности, не отнесенные к должностям муниципальной службы (далее – служащие), при обработке информации в электронном виде, в том числе в информационных системах, ответственность служащих за нарушение требований настоящей Политики ИБ.

Действие настоящей Политики ИБ не применяется к отношениям, связанным с обеспечением безопасности информации, составляющей государственную тайну.

1.3. Настоящая Политика ИБ применима ко всем техническим средствам (серверам, периферийному оборудованию, автоматизированным рабочим местам (далее – АРМ) и так далее), установленным в функциональных и территориальных органах, функциональных подразделениях администрации города Перми, ко всем процессам обработки информации с использованием указанных технических средств, кроме технических средств, на которых обрабатывается информация, составляющая государственную тайну (далее – объекты защиты).

1.4. Действие настоящей Политики ИБ распространяется на все функциональные и территориальные органы, функциональные подразделения администрации города Перми.

При осуществлении санкционированного доступа к информационным ресурсам администрации города Перми органами государственной власти, иными органами местного самоуправления, государственными, муниципальными учреждениями требования по безопасности информации устанавливаются в соглашении об информационном взаимодействии.

1.5. Правовыми основаниями настоящей Политики ИБ являются Конституция Российской Федерации, Гражданский кодекс Российской Федерации, Уголов-

ный кодекс Российской Федерации, Кодекс Российской Федерации об административных правонарушениях, Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», иные нормативные правовые акты Российской Федерации, документы Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности, Федеральной службы по надзору в сфере связи и массовых коммуникаций.

II. Термины и определения

В настоящей Политике ИБ используются следующие термины и определения:

вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения;

вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных;

доступность информации – состояние информации, при котором субъекты, имеющие санкционированные права доступа, могут реализовать их беспрепятственно;

защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации;

идентификатор (имя, логин) – набор символов, представляющий уникальное наименование объекта или субъекта в информационной системе, позволяющее однозначно идентифицировать пользователя при входе его в систему, определить его права в ней, фиксировать действия и тому подобное;

информационная безопасность – состояние защищенности информационной среды;

информационная среда – совокупность условий для технологической переработки и эффективного использования информационных ресурсов (в том числе технические средства, программное обеспечение, телекоммуникации, уровень подготовки пользователей, формы контроля, документопотоки, процедуры, регламенты, юридические нормы, иные факторы, воздействующие на информационные процессы и информационные системы);

информационные ресурсы – отдельные документы, массивы документов, в том числе содержащиеся в информационных системах (архивах, фондах, банках данных, других информационных системах);

инцидент информационной безопасности – любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность;

несанкционированное действие – действие субъекта в нарушение установленных в информационной системе регламентируемых правил обработки информации;

оператор информационной системы администрации города Перми (далее – оператор информационной системы) – функциональный, территориальный орган или функциональное подразделение администрации города Перми, определяющий цели и порядок эксплуатации информационной системы;

пароль – конфиденциальная последовательность символов, связанная с субъектом и известная только ему, позволяющая его аутентифицировать, то есть подтвердить соответствие реальной сущности субъекта предъявляемому им при входе идентификатору;

профиль – набор установок и конфигураций, специфичный для данного субъекта или объекта и определяющий его работу в информационной системе;

системный администратор – лицо, обеспечивающее выполнение функций по обеспечению работы компьютерной техники, сети и программного обеспечения в функциональном, территориальном органе, функциональном подразделении администрации города Перми. Для функциональных подразделений администрации города Перми функции системного администратора выполняют специалисты управления информационных технологий администрации города Перми (далее – УИТ);

угроза безопасности информации – потенциально возможное событие, действие, процесс или явление, которое может привести к нарушению конфиденциальности, целостности, доступности информации, а также неправомерному тиражированию, которое наносит ущерб собственнику, владельцу или пользователю информации;

уязвимость – свойство информационной системы, обусловливающее возможность реализации угроз безопасности, обрабатываемой в ней информации;

целостность информации – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими санкционированное право на изменение информации.

Термины «информация, информационная система, информационная система персональных данных, конфиденциальность информации, обладатель информации, сайт в сети Интернет (далее – сайт), спам, обезличивание персональных данных, общедоступная информация» используются в значениях, установленных Федеральными законами от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 10 сентября 2007 г. № 575 «Об утверждении Правил оказания телематических услуг связи».

III. Цели и задачи защиты информации в администрации города Перми, основные виды угроз безопасности информации

3.1. Обеспечение информационной безопасности в администрации города Перми (защита информации) – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и (или) непреднамеренных воздействий на защищаемую информацию, ее носители, процессы обработки.

3.2. Защищаемой информацией в администрации города Перми является вся

информация, обрабатываемая в администрации города Перми (функциональных (территориальных) органах (подразделениях) администрации города Перми) (далее – информация) независимо от ее местонахождения в информационной среде.

В администрации города Перми обрабатывается информация различных уровней конфиденциальности:

общедоступная (открытая) информация, для которой требуется обеспечение доступности и целостности;

информация ограниченного распространения, доступ к которой ограничивается в соответствии с действующим законодательством Российской Федерации (далее – конфиденциальная информация), и наравне с доступностью и целостностью требуется обеспечение конфиденциальности.

Уровень конфиденциальности устанавливается обладателем информации.

3.3. Основными задачами защиты информации в администрации города Перми являются:

выявление и оценка потенциальных угроз информационной безопасности и уязвимостей объектов защиты;

исключение либо минимизация выявленных угроз безопасности;

предотвращение инцидентов информационной безопасности.

3.5. Угрозы безопасности информации могут быть реализованы за счет:

утечки по техническим каналам утечки информации;

несанкционированного доступа с использованием соответствующего программного обеспечения.

3.6. Угрозы безопасности информации могут проявляться в виде инцидентов информационной безопасности:

утрата информации, оборудования или устройств;

системные сбои или перегрузки;

противоправные и (или) ошибочные действия служащих при работе на АРМ;

нарушение правил обработки информации, в том числе разглашение паролей доступа к информационным ресурсам, которые повлекли или могли повлечь нарушение конфиденциальности, целостности и (или) доступности информации;

нарушение физических мер защиты;

неконтролируемые изменения систем;

сбои программного обеспечения, отказы в обслуживании сервисов, средств обработки информации, оборудования;

нарушение правил доступа;

внедрение вредоносных программ.

3.7. В качестве методов защиты информации в администрации города Перми применяются:

регламентация доступа в служебные помещения администрации города Перми;

разграничение доступа к техническим средствам и информационным ресурсам администрации города Перми;

применение антивирусной защиты;

применение криптографической защиты информации;
применение обезличивания персональных данных;
регламентация использования электронной почты;
регламентация работы в сети Интернет;
регламентация создания и эксплуатации информационных систем;
проведение внутреннего контроля и обучение служащих.

IV. Регламентация доступа в служебные помещения администрации города Перми

4.1. Регламентация доступа в служебные помещения администрации города Перми осуществляется в целях:

обеспечения физической сохранности носителей информации, оборудования;

исключения возможности несанкционированного доступа в служебные помещения, в том числе в которых ведется обработка конфиденциальной информации.

4.2. Доступ служащих и посетителей в административные здания (помещения) администрации города Перми осуществляется в соответствии с Положением о пропускном и внутриобъектовом режимах в административных зданиях (помещениях) администрации города Перми, утвержденным распоряжением администрации города Перми от 03 декабря 2015 г. № СЭД-01-32-55.

Доступ в помещения, в которых ведется обработка персональных данных, осуществляется в соответствии с Порядком доступа муниципальных служащих администрации города Перми в помещения, в которых ведется обработка персональных данных, утвержденным распоряжением администрации города Перми от 24 августа 2012 г. № 81.

V. Разграничение доступа к техническим средствам и информационным ресурсам администрации города Перми

5.1. Разграничение доступа к техническим средствам и информационным ресурсам администрации города Перми направлено на предотвращение получения информации, обрабатываемой в электронном виде, в том числе в информационных системах, с нарушением регламентируемых нормативными правовыми актами или владельцами информации правил, следствием которых может быть нарушение конфиденциальности, целостности и (или) доступности информации.

5.2. Для работы с информационными ресурсами администрации города Перми служащему предоставляется АРМ.

ПО АРМ устанавливается и обновляется системным администратором со специальных ресурсов или съемных носителей в соответствии с лицензионным соглашением.

При передаче АРМ другому служащему производится удаление профиля пользователя АРМ.

5.3. Доступ к конфиденциальной информации, в том числе персональным данным, осуществляется в соответствии с Положением о порядке обращения

со сведениями конфиденциального характера в администрации города Перми, утвержденным постановлением администрации города Перми от 22 августа 2007 г. № 347.

Обработка персональных данных осуществляется с особенностями, установленными Положением об обработке и организации защиты персональных данных в администрации города Перми, утвержденным распоряжением администрации города Перми от 28 ноября 2011 г. № 194-р.

5.4. К работе с информационными ресурсами администрации города Перми допускаются служащие, ознакомленные с настоящей Политикой ИБ.

5.5. Для осуществления доступа к информационным ресурсам администрации города Перми служащему создается учетная запись – присваивается уникальный идентификатор (имя, логин) и пароль доступа.

Порядок доступа служащих к информационной системе устанавливается в соответствии с правовым актом города Перми, определяющим порядок эксплуатации информационной системы.

5.6. Для защиты своих паролей служащие обязаны:

соблюдать конфиденциальность пароля – не сообщать пароль другим лицам, в том числе другим служащим, не хранить пароли в легкодоступных местах (на столе, стене, терминале и так далее);

выбирать трудно угадываемый пароль – использовать в пароле строчные и прописные буквы, цифры, специальные символы, не использовать в качестве пароля свои фамилию, имя, отчество, цифровые ряды или повторяющиеся цифры (123456, 111111 и так далее);

использовать в пароле не менее 8 символов;

в случае компрометации пароля немедленно изменить пароль.

5.7. При работе на АРМ служащие обязаны:

работать только под своей учетной записью;

блокировать доступ к АРМ при отсутствии на рабочем месте.

5.8. Служащим запрещается самостоятельно устанавливать на АРМ дополнительные технические средства и (или) ПО.

VI. Антивирусная защита

6.1. Антивирусная защита в администрации города Перми применяется с целью защиты информационных ресурсов и ПО от несанкционированных действий (утраты, модификации, изменения) путем внедрения в информационную среду вирусов, вредоносных программ (далее – вирус) посредством использования специализированного ПО (далее – антивирусное ПО).

6.2. Антивирусное ПО должно быть развернуто на всех технических средствах, подверженных воздействию вирусов (АРМ, серверах). Антивирусные механизмы должны быть актуальными, постоянно включенными. Должны вестись журналы протоколирования событий. Отключение антивирусного ПО или отказ от автоматического обновления антивирусных баз не допускается.

6.3. Обязанность по своевременному получению и предоставлению функциональным (территориальным) органам администрации города Перми лицензи-

онных ключей антивирусного ПО возлагается на УИТ.

6.4. Обязанность по установке и регулярному обновлению антивирусного ПО, в том числе антивирусных баз, на АРМ и серверах функциональных (территориальных) органов (подразделений) администрации города Перми возлагается на соответствующих системных администраторов.

6.5. При установке антивирусного ПО системным администратором должны выполняться следующие требования:

актуализация антивирусных баз на АРМ, подключенных к локальной сети администрации города Перми, должна осуществляться ежедневно в автоматическом режиме через специальный сервер обновлений;

актуализация антивирусных баз на АРМ, не подключенных к локальной сети администрации города Перми, должна осуществляться с использованием съемных носителей информации не реже одного раза в неделю;

проверка критических областей АРМ, заражение которых вирусами может привести к серьезным последствиям, должна проводиться автоматически при каждой его загрузке.

6.6. Некоторые признаки проявления вируса:

прекращение работы или неправильная работа ранее успешно функционировавшего ПО;

медленная работа АРМ;

невозможность загрузки операционной системы;

нетипичная работа ПО;

вывод на экран непредусмотренных сообщений или изображений;

подача непредусмотренных звуковых сигналов;

частые зависания и сбои в работе АРМ;

частое появление сообщений о системных ошибках;

исчезновение файлов, каталогов или искажение их содержимого;

изменение даты и времени модификации файлов;

изменение размеров файлов;

неожиданное значительное увеличение количества файлов на диске;

существенное уменьшение размера свободной оперативной и дисковой памяти.

6.7. Для исключения заражения вирусами и обеспечения надежного хранения информации в электронном виде служащие обязаны:

убедиться, что на АРМ установлено и включено антивирусное ПО;

незамедлительно сообщить системному администратору о нарушениях работы антивирусного ПО;

перед использованием проверять съемные носители информации на наличие вирусов средствами установленного на АРМ антивирусного ПО;

при переносе на свой АРМ файлов в архивированном виде проверять их до и после разархивации на жестком диске, ограничивая область проверки только вновь записанными файлами;

использовать антивирусное ПО для входного контроля всех файлов (исполняемых файлов, файлов данных, сообщений электронной почты и так далее), получаемых из компьютерных сетей, а также на съемных носителях информации;

в случае установки или изменения ПО при возникновении подозрения на наличие вирусов проверять на наличие вирусов жесткие диски АРМ, запуская антивирусное ПО для тестирования файлов, памяти и системных областей дисков.

6.8. Служащим запрещается:

открывать приложения и документы в письмах, получаемых по электронной почте, если имеются сомнения в надежности отправителя и (или) отправления;

переходить по ссылкам в спам-письмах;

загружать файлы с сайтов, если имеются сомнения в надежности сайта и (или) загружаемого файла.

6.9. При возникновении подозрения на наличие вирусов служащие обязаны:

приостановить все операции, связанные с обработкой файлов на АРМ;

запустить антивирусное ПО для тестирования файлов, памяти и системных областей дисков;

о факте обнаружения вирусов немедленно сообщить системному администратору, владельцам зараженных или поврежденных вирусами файлов, другим пользователям, использующим зараженные файлы в работе;

провести анализ необходимости дальнейшего использования зараженных вирусом файлов;

провести самостоятельно или совместно с системным администратором лечение зараженных файлов, в случае обнаружения не поддающегося лечению вируса удалить инфицированный файл и проверить работоспособность компьютера.

6.10. Служащие допускаются к работе на АРМ только после обучения пользованию средствами антивирусного ПО в соответствии с разделом 12 настоящей Политики ИБ.

6.11. Ежемесячно не позднее 03 числа месяца, следующего за отчетным, функциональные и территориальные органы администрации города Перми направляют в УИТ информацию о фактах заражения вирусами серверов, АРМ по форме согласно приложению к настоящей Политике ИБ.

VII. Криптографическая защита информации

7.1. Криптографическая защита информации (шифрование) применяется для обеспечения конфиденциальности информации при хранении в ненадежных хранилищах и (или) передаче ее по незащищенным каналам связи (телефон, факс, электронная почта и так далее).

7.2. Применение средств криптографической защиты информации (далее – СКЗИ) для шифрования конфиденциальной информации должно осуществляться с учетом требований приказа Федеральной службы безопасности Российской Федерации от 09 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».

7.3. Необходимость криптографической защиты информации конфиденциального характера при ее обработке в информационной системе, выбор применя-

емых СКЗИ устанавливаются в зависимости от класса информационной системы в соответствии с правовым актом города Перми, определяющим порядок эксплуатации информационной системы.

7.4. Шифрование осуществляется перед отправкой данных по незащищенным каналам связи или перед помещением на хранение в ненадежных хранилищах.

VIII. Обезличивание персональных данных

8.1. Обезличивание персональных данных в администрации города Перми проводится в целях обеспечения защиты от несанкционированного распространения персональных данных при размещении в информационных системах, не предназначенных для обработки персональных данных (далее – открытые информационные системы), и (или) передаче по незащищенным каналам связи.

8.2. Обезличивание персональных данных должно осуществляться с учетом требований и методов, утвержденных приказом Роскомнадзора от 05 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных».

8.3. Необходимость и метод обезличивания персональных данных, обрабатываемых в информационной системе персональных данных (далее – ИСПДн), устанавливаются правовым актом города Перми, определяющим порядок эксплуатации ИСПДн.

8.4. При использовании процедуры обезличивания не допускается совместное хранение персональных данных и обезличенных данных.

8.5. Обезличивание персональных данных должно производиться перед внесением их в открытую информационную систему и (или) передачей по незащищенным каналам связи.

IX. Регламентация использования электронной почты

9.1. Система электронной почты администрации города Перми (далее – электронная почта) используется в информационных целях, в том числе оповещения, организации работы, обеспечения внутренних и внешних коммуникаций.

9.2. Регламентация использования электронной почты осуществляется с целью снижения риска умышленной или неумышленной несанкционированной рассылки информации, заражения информационных ресурсов администрации города Перми вирусами.

9.3. Угрозы, связанные с электронной почтой:

возможность создания писем с фальшивыми адресами;

возможность нарушения конфиденциальности электронных писем;

возможность изменения в процессе передачи содержимого электронных писем;

осуществление сетевых атак посредством отправки упакованного в архив сообщения, распаковка которого приводит к выводу системы из строя, заражения вирусами;

получение спама.

9.4. Использование электронной почты в целях исполнения должностных обязанностей служащими осуществляется с использованием индивидуального электронного адреса служащего в домене gorodperm.ru.

При увольнении служащего электронный почтовый ящик отключается с последующим автоматическим удалением.

9.5. При работе с электронной почтой служащие обязаны:

перед отправкой тщательно проверять сообщения на отсутствие информации, указанной в пункте 9.6 настоящей Политики ИБ;

периодически удалять из электронного почтового ящика ненужные сообщения и перемещать необходимые сообщения в архивные почтовые папки;

проверять сообщения электронной почты на наличие вирусов;

использовать шифрование, обезличивание конфиденциальной информации при ее отправке.

9.6. При работе с электронной почтой служащим запрещено:

отправлять конфиденциальную информацию без предварительного шифрования криптографическим ПО, разрешенным к использованию в администрации города Перми;

отправлять персональные данные без предварительного обезличивания или шифрования;

отправлять сообщения с иного электронного почтового ящика или от имени другого служащего без предоставления полномочий;

использовать электронную почту для создания, отправки, пересылки или хранения любых подрывных, оскорбительных, неэтичных, незаконных материалов, включая оскорбительные комментарии по поводу расы, пола, цвета, инвалидности, возраста, сексуальной ориентации, порнографии, терроризма, религиозных убеждений и верований, политических убеждений, национальном происхождении, гиперссылок или других ссылок на веб-сайты, содержащие указанные материалы, массовые рассылки спама;

рассылать компьютерные коды, файлы или ПО, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования, вирусы или другое злонамеренное ПО, программы для осуществления несанкционированного доступа, серийные номера к программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в сети Интернет, ссылки на указанную информацию;

перехватывать, изменять, удалять, сохранять или публиковать сообщения иных служащих, кроме случаев, санкционированных руководителями или в целях администрирования систем;

использовать веб-сервисы Google, Gmail, Hotmail, Yahoo, Яндекс или подобные почтовые системы третьих сторон («вебмайл») для отправки и (или) получения служебной корреспонденции;

загружать и запускать исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным ПО, переходить по активным ссылкам, полученным от отправителей, если имеются сомнения

в надежности отправителя и (или) полученного сообщения.

9.7. Содержимое электронного почтового ящика служащего может быть проверено системным администратором без предварительного уведомления служащего в случае подозрения на осуществление рассылки писем, содержащих вредоносное ПО, спам, информацию, распространение которой запрещено правовыми актами. Информация о выявленных нарушениях направляется служащему и руководителю соответствующего функционального (территориального) органа (подразделения) администрации города Перми.

X. Регламентация работы в сети Интернет

10.1. Сеть Интернет в администрации города Перми используется служащими для получения информации в рамках исполнения должностных обязанностей.

10.2. Регламентация работы в сети Интернет осуществляется с целью снижения риска заражения информационных ресурсов администрации города Перми вирусами.

10.3. Организацию доступа к сети Интернет для нужд администрации города Перми осуществляет УИТ.

10.4. Доступ к сети Интернет предоставляется служащим с АРМ, закрепленным за служащим для исполнения должностных обязанностей.

10.5. Угрозы, связанные с работой в сети Интернет:

легкость перехвата данных и фальсификации IP-адресов в сети Интернет;

заражение вирусами.

10.6. Служащим запрещается:

осуществлять действия, запрещенные законодательством Российской Федерацией;

отправлять конфиденциальную информацию без предварительного шифрования криптографическим ПО, разрешенным к использованию в администрации города Перми;

распространять информацию, содержащую подрывные, оскорбительные, неэтичные, незаконные материалы, включая оскорбительные комментарии по поводу расы, пола, цвета, инвалидности, возраста, сексуальной ориентации, порнографии, терроризма, религиозных убеждений и верований, политических убеждений, национальном происхождении, гиперссылок или других ссылок на вебсайты, содержащие указанные материалы, массовые рассылки спама;

самостоятельно устанавливать на АРМ дополнительное ПО, полученное в сети Интернет;

загружать и запускать исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным ПО;

открывать страницы сайтов, если имеются сомнения в надежности сайта и (или) имеются уведомления о возможном заражении вирусами.

10.7. Служащие обязаны при обнаружении попыток несанкционированного доступа и (или) при подозрении на наличие вируса немедленно прекратить работу в сети Интернет и сообщить системному администратору.

10.8. Вся информация о ресурсах, посещаемых служащим, автоматически протоколируется и при необходимости представляется системными администраторами руководителям.

10.9. Доступ к сети Интернет может быть блокирован системным администратором без предварительного уведомления служащего при возникновении угрозы безопасности информации.

XI. Регламентация создания и эксплуатации информационных систем

11.1. Регламентация создания и эксплуатации информационных систем направлена на упорядочение деятельности функциональных (территориальных) органов (подразделений) администрации города Перми по созданию информационных систем и обеспечению безопасности информации, содержащейся в информационных системах.

11.2. Решение о целесообразности создания или ликвидации информационной системы принимается Советом по информационным технологиям при главе администрации города Перми на основании предложения руководителя функционального (территориального) органа (подразделения) администрации города Перми о создании (ликвидации) информационной системы и оформляется протоколом в соответствии с Положением о Совете по информационным технологиям при главе администрации города Перми, утвержденным распоряжением администрации города Перми от 30 ноября 2010 г. № 188-р.

11.3. Процесс создания информационной системы осуществляется в соответствии с ГОСТ 34.601-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы стадии создания, утвержденным постановлением Госстандарта СССР от 29 декабря 1990 г. № 3469, и представляет собой совокупность упорядоченных во времени, взаимосвязанных, объединенных в стадии и этапы работ, выполнение которых необходимо и достаточно для создания информационной системы.

11.4. Информационная система вводится в эксплуатацию правовым актом города Перми, разработанным и утвержденным в соответствии с Регламентом утверждения правовых актов города Перми о вводе в эксплуатацию, выводе из эксплуатации (ликвидации) информационных систем и (или) определении порядка эксплуатации информационной системы (далее – Регламент).

Правовой акт города Перми о вводе в эксплуатацию информационной системы должен определять порядок эксплуатации информационной системы.

11.5. Порядок эксплуатации информационной системы должен содержать:

полное наименование информационной системы;

цель создания информационной системы;

законы и иные правовые акты, на основании которых ведется обработка информации в информационной системе;

полномочия органа местного самоуправления, реализовываемые при эксплуатации информационной системы;

отнесение информационной системы к категории муниципальная или иной в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 149-ФЗ

«Об информации, информационных технологиях и о защите информации»;

перечень обрабатываемой информации, в том числе персональных данных (при наличии), перечень разделов (для сайтов);

требования по обеспечению безопасности обрабатываемой информации (конфиденциальности, целостности, доступности);

наименование оператора информационной системы, его права и обязанности;

перечень участников, пользователей информационной системы, их права и обязанности;

порядок обеспечения доступа к информационной системе;

иную информацию, определяющую особенности эксплуатации информационной системы.

11.6. Порядок эксплуатации ИСПДн разрабатывается с учетом требований, установленных распоряжением администрации города Перми от 01 июля 2013 г. № 91 «О вводе в эксплуатацию информационных систем персональных данных администрации города Перми и утверждении Порядка подготовки и утверждения порядков эксплуатации информационных систем персональных данных администрации города Перми».

11.7. Все функционирующие в функциональных (территориальных) органах (подразделениях) администрации города Перми информационные системы включаются в Реестр информационных систем администрации города Перми, утвержденный распоряжением администрации города Перми от 27 марта 2015 г. № 43 (далее – Реестр информационных систем).

Основанием для включения информационной системы в Реестр информационных систем является правовой акт города Перми о введении в эксплуатацию информационной системы, изданный в соответствии с Регламентом.

11.8. Основанием для изменения информации об информационной системе, включенной в Реестр информационных систем, является правовой акт города Перми, определяющий порядок эксплуатации информационной системы.

11.9. Основанием для исключения информационной системы из Реестра информационных систем является правовой акт города Перми о прекращении эксплуатации (ликвидации) информационной системы, изданный в соответствии с Регламентом.

11.10. Обязанность по ведению Реестра информационных систем возлагается на УИТ.

XII. Проведение внутреннего контроля и обучение служащих

12.1. В целях выявления угроз безопасности информации, нарушений настоящей Политики ИБ и принятия мер, направленных на предотвращение угроз и нарушений, в администрации города Перми осуществляется внутренний контроль:

12.1.1. использования технических средств, ПО, работы в сети Интернет в функциональных (территориальных) органах (подразделениях) администрации города Перми по поручению руководителя аппарата администрации города

Перми, руководителей функциональных (территориальных) органов (подразделений) администрации города Перми;

12.1.2. обработки персональных данных в администрации города Перми в соответствии с утвержденными распоряжением администрации города Перми от 24 августа 2012 г. № 81 Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленными Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами администрации города Перми.

12.2. Ознакомление служащих с настоящей Политикой ИБ производится при:

приеме на работу;

изменении настоящей Политики ИБ;

обнаружении действий служащих, которые повлекли или могли повлечь нарушение безопасности информации.

12.3. Обучение служащих пользованию средствами антивирусного ПО производится при:

приеме на работу;

изменении антивирусного ПО;

заражении АРМ вирусами.

12.4. Ознакомление служащих с настоящей Политикой ИБ и обучение пользованию средствами антивирусного ПО осуществляется под подпись в листе ознакомления (прохождения обучения) либо журнале ознакомления (прохождения обучения) с указанием фамилии, имени, отчества служащего и даты ознакомления (прохождения обучения).

Обязанность по организации ознакомления служащих с настоящей Политикой ИБ возлагается на руководителей функциональных (территориальных) органов (подразделений) администрации города Перми.

Обязанность по обучению пользованию средствами антивирусного ПО возлагается на системных администраторов.

XIII. Ответственность за нарушения настоящей Политики ИБ

13.1. Служащие в рамках должностных обязанностей и полномочий несут ответственность в соответствии с действующим законодательством Российской Федерации за:

невыполнение требований настоящей Политики ИБ;

действия или бездействие, ведущие к нарушению информационной безопасности;

действия или бездействие, ведущие к нарушению действующего законодательства Российской Федерации в области информационных технологий.

13.2. При обнаружении нарушения служащими настоящей Политики ИБ системный администратор устанавливает причины возникновения нарушения и направляет служебную записку о выявленном нарушении руководителю функционального (территориального) органа (подразделения) администрации

города Перми.

Руководитель функционального (территориального) органа (подразделения) администрации города Перми принимает решение о необходимости привлечения служащего к ответственности.

Системный администратор ведет учет всех выявленных случаев нарушения безопасности информации.

Приложение
к Политике информационной
безопасности администрации
города Перми

ИНФОРМАЦИЯ
о выявленных компьютерных атаках, уязвимостях и поражениях вредоносным программным обеспечением информационных ресурсов

№	Форма проявления угрозы безопасности	Дата проявления	Количество зараженных автоматизированных рабочих мест (АРМ)/ серверов	Наименование угрозы безопасности[1]	Объект угрозы безопасности[2]	Источник угроз безопасности[3]	Мероприятия по устранению угрозы безопасности[4]
1	2	3	4	5	6	7	8

---

[1] Указывается в случае наличия информации об угрозе безопасности (компьютерной атаки, уязвимости или вредоносного программного обеспечения).

[2] Объектом угрозы безопасности могут быть файлы, службы, библиотеки и другие возможные объекты АРМ пользователя, сервера или информационной системы (ресурс). Требуется указать: установленная операционная система, средства защиты, объекты угрозы безопасности. Указывается в случае наличия информации.

[3] Источником угрозы безопасности может быть электронная почта, локальная вычислительная сеть, Интернет, внешние запоминающие устройства и другие источники.

[4] Указать перечень проводимых мероприятий по устранению угрозы (сканирование и лечение антивирусном программным обеспечением, обновление или удаление программного обеспечения, установка дополнительных средств защиты и другие возможные мероприятия), результат проведенных мероприятий по устранению угрозы безопасности (устранено/не устранено).

УТВЕРЖДЕН
распоряжением администрации
города Перми
от 30.06.2016 №79

РЕГЛАМЕНТ
утверждения правовых актов города Перми о вводе в эксплуатацию, выводе из эксплуатации (ликвидации) информационных систем и (или) определении порядка эксплуатации информационной системы

№	Назначение правового акта города Перми	Разработчик	Обязательное согласование	Вид правового акта города Перми	Обязательная рассылка
1	2	3	4	5	6
1	Для муниципальных межведомственных информационных систем, оператором которых являются функциональные органы администрации города Перми				
1.1	О вводе в эксплуатацию (вместе с определением порядка эксплуатации) вновь созданной информационной системы	функциональный орган администрации города Перми (по направлению деятельности)	управление информационных технологий администрации города Перми; правовое управление администрации города Перми	распоряжение администрации города Перми	управление информационных технологий администрации города Перми; функциональные и территориальные органы, функциональные подразделения администрации города Перми, являющиеся участниками информационной системы
1.2	Об определении порядка эксплуатации ин-	функциональный орган адми-	управление информационных техноло-	распоряжение администрации города	управление информационных техноло-

1	2	3	4	5	6
	формационной системы, включенной в Реестр информационных систем администрации города Перми	нистрации города Перми (по направлению деятельности)	гий администрации города Перми; правовое управление администрации города Перми	Перми	гий администрации города Перми; функциональные и территориальные органы, функциональные подразделения администрации города Перми, являющиеся участниками информационной системы
1.3	О выводе из эксплуатации (ликвидации) информационной системы	функциональный орган администрации города Перми (по направлению деятельности)	управление информационных технологий администрации города Перми; правовое управление администрации города Перми	распоряжение администрации города Перми	управление информационных технологий администрации города Перми; функциональные и территориальные органы, функциональные подразделения администрации города Перми, являющиеся участниками информационной системы
2	Для ведомственных информационных систем, оператором которых являются функциональные (территориальные) органы администрации города Перми				
2.1	О вводе в эксплуатацию (вместе с опреде-	функциональный орган адми-	управление информационных техноло-	приказ руководителя функционального	управление информационных техноло-

1	2	3	4	5	6
	лением порядка эксплуатации) вновь созданной информационной системы	нистрации города Перми	гий администрации города Перми	(территориального) органа администрации города Перми	гий администрации города Перми; функциональные и территориальные органы, функциональные подразделения администрации города Перми, являющиеся участниками информационной системы
2.2	Об определении порядка эксплуатации информационной системы	функциональный орган администрации города Перми	управление информационных технологий администрации города Перми	приказ руководителя функционального (территориального) органа администрации города Перми	управление информационных технологий администрации города Перми; функциональные и территориальные органы, функциональные подразделения администрации города Перми, являющиеся участниками информационной системы
2.3	О выводе из эксплуатации (ликвидации) информационной системы	функциональный орган администрации города Перми	управление информационных технологий администрации города Перми	приказ руководителя функционального (территориального) органа администрации	управление информационных технологий администрации города Перми;

1	2	3	4	5	6
				города Перми	функциональные и территориальные органы, функциональные подразделения администрации города Перми, являющиеся участниками информационной системы
3	Для муниципальных межведомственных информационных систем, оператором которых являются функциональные подразделения администрации города Перми				
3.1	О вводе в эксплуатацию (вместе с определением порядка эксплуатации) вновь созданной информационной системы	управление информационных технологий совместно с функциональным подразделением администрации города Перми (по направлению деятельности)	управление информационных технологий администрации города Перми; функциональное подразделение (по направлению деятельности); правовое управление администрации города Перми	распоряжение администрации города Перми	управление информационных технологий администрации города Перми; функциональные и территориальные органы, функциональные подразделения администрации города Перми, являющиеся участниками информационной системы
3.2	Об определении порядка эксплуатации информационной системы, включенной в Ре-	управление информационных технологий совместно с функ-	управление информационных технологий администрации города Перми;	распоряжение администрации города Перми	управление информационных технологий администрации города Перми;

1	2	3	4	5	6
	естр информационных систем	циональным подразделением администрации города Перми (по направлению деятельности)	функциональное подразделение (по направлению деятельности); правовое управление администрации города Перми		функциональные и территориальные органы, функциональные подразделения администрации города Перми, являющиеся участниками информационной системы
3.3	О выводе из эксплуатации (ликвидации) информационной системы	функциональное подразделение администрации города Перми (по направлению деятельности)	управление информационных технологий администрации города Перми; функциональное подразделение (по направлению деятельности); правовое управление администрации города Перми	распоряжение администрации города Перми	управление информационных технологий администрации города Перми; функциональные и территориальные органы, функциональные подразделения администрации города Перми, являющиеся участниками информационной системы
4	Для ведомственных информационных систем, оператором которых являются функциональные подразделения администрации города Перми				
4.1	О вводе в эксплуатацию (вместе с определением порядка эксплуатации) вновь создан-	управление информационных технологий совместно с функ-	управление информационных технологий администрации города Перми;	распоряжение руководителя аппарата администрации города Перми	управление информационных технологий администрации города Перми,

1	2	3	4	5	6
	ной информационной системы	циональным подразделением администрации города Перми (по направлению деятельности)	функциональное подразделение (по направлению деятельности); правовое управление администрации города Перми		функциональное подразделение (по направлению деятельности)
4.2	Об определении порядка эксплуатации информационной системы, включенной в Реестр информационных систем	управление информационных технологий совместно с функциональным подразделением администрации города Перми (по направлению деятельности)	управление информационных технологий администрации города Перми; функциональное подразделение (по направлению деятельности); правовое управление администрации города Перми	распоряжение руководителя аппарата администрации города Перми	управление информационных технологий администрации города Перми, функциональное подразделение (по направлению деятельности)
4.3	О выводе из эксплуатации (ликвидации) информационной системы	функциональное подразделение администрации города Перми (по направлению деятельности)	управление информационных технологий администрации города Перми; функциональное подразделение (по направлению деятельности); правовое управление администрации горо-	распоряжение руководителя аппарата администрации города Перми	управление информационных технологий администрации города Перми, функциональное подразделение (по направлению деятельности)

1	2	3	4	5	6
			да Перми		