Российская Федерация Псковская область
Администрация Палкинского района

ПОСТАНОВЛЕНИЕ

13.06.2023 г. 294
от _____. № _____
п. Палкино

Об утверждении Общей политики
информационной безопасности
администрации Палкинского района

В соответствии с Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Администрация района **ПОСТАНОВЛЯЕТ:**

1. Утвердить прилагаемые:
- Общую политику информационной безопасности администрации Палкинского района;
- Регламент утверждения правовых актов администрации Палкинского района о вводе в эксплуатацию, прекращении эксплуатации информационных систем и (или) определении порядка эксплуатации информационной системы (далее - Регламент).
2. Ознакомить служащих администрации района с настоящим постановлением под роспись.
3. Опубликовать настоящее постановление на официальном сайте муниципального образования «Палкинский район».
4. Контроль за исполнением постановления возложить на управляющего делами администрации района.

Глава Палкинского района О.С. Потапова

Верно: Костылева

Утверждена
постановлением администрации района
от 13.06.2023 г. № 294

Общая политика
информационной безопасности администрации Палкинского района

I. Общие положения

1.1. Настоящая Общая политика информационной безопасности администрации Палкинского района (далее - Политика ИБ) разработана в целях установления безопасных способов обработки информации в электронном виде, в том числе в информационных системах (сайтах) администрации Палкинского района (далее - информационная система).
1.2. Настоящая Политика ИБ определяет в администрации Палкинского района (далее - администрация района) цели и задачи защиты информации, устанавливает методы защиты информации, которыми должны руководствоваться муниципальные служащие администрации района, иные работники администрации района, 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.
Требования информационной безопасности, которые предъявляются администрацией района, соответствуют целям деятельности администрация района и предназначены для снижения рисков, связанных с информационной безопасностью, до приемлемого уровня.
1.3. Настоящая Политика ИБ применима ко всем техническим средствам (серверам, периферийному оборудованию, автоматизированным рабочим местам (далее - АРМ) и так далее), установленным в структурных подразделениях администрации района, 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 структурные подразделения администрации района.
При осуществлении санкционированного доступа к информационным ресурсам администрации района 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, Уголовный 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, акты и документы Федеральных служб.

2. 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 - компьютерная программа либо иная компьютерная информация, предназначенная для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации;
- доступность информации - состояние информации, при котором субъекты, имеющие санкционированные права доступа, могут реализовать их беспрепятственно;
- защита информации, деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию;
- защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых актов 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 система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;
- 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);
- информация, сведения (сообщения, данные) независимо от формы их представления;
- информация ограниченного доступа - информация, доступ к которой ограничен федеральными законами;
- инцидент информационной безопасности - любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность;

- конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;
- несанкционированное действие - действие субъекта в нарушение установленных в информационной системе регламентируемых правил обработки информации;
- обладатель информации - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;
- оператор информационной системы администрации района (далее - оператор информационной системы) - структурное подразделение администрации района, 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;
- персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных);
- 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 администрации района;
- 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».

Термины «электронная подпись, сертификат ключа проверки электронной подписи, владелец сертификата ключа проверки электронной подписи, ключ электронной подписи, ключ проверки электронной подписи, средства электронной подписи» используются в значениях, установленных Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

3. Цели и задачи защиты информации в администрации Палкинского района, основные виды угроз безопасности информации

3.1. Обеспечение информационной безопасности в администрации Палкинского района (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 является вся информация, обрабатываемая в администрации Палкинского района (структурных подразделениях администрации Палкинского района) (далее - информация), независимо от ее местонахождения в информационной среде.

В администрации Палкинского района 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 Палкинского района являются:
- выявление и оценка потенциальных угроз информационной безопасности и уязвимости объектов защиты;
- исключение либо минимизация выявленных угроз безопасности;
- предотвращение инцидентов информационной безопасности.

3.4. Угрозы безопасности информации могут быть реализованы за счет:
- утечки по техническим каналам утечки информации;
- несанкционированного доступа с использованием соответствующего программного обеспечения.

3.5. 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.

3.6. В качестве методов защиты информации в администрации Палкинского района применяются:
- регламентация доступа в служебные помещения администрации района;
- разграничение доступа к техническим средствам и информационным ресурсам администрации района;
- 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.

4. Регламентация доступа в служебные помещения администрации Палкинского района

4.1. Регламентация доступа в служебные помещения администрации Палкинского района 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 в помещения, в которых ведется обработка персональных данных, осуществляется в соответствии с порядком доступа муниципальных служащих администрации Палкинского района в помещения, в которых ведется обработка персональных данных, утвержденным постановлением администрации Палкинского района.

5. Разграничение доступа к техническим средствам и информационным ресурсам администрации Палкинского района

5.1. Разграничение доступа к техническим средствам и информационным ресурсам администрации Палкинского района 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 района служащему предоставляется АРМ. Программное обеспечение (далее - 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 Палкинского района, утвержденным постановлением администрации района.
Обработка персональных данных осуществляется с особенностями, установленными Положением о порядке обработки персональных данных в администрации Палкинского района, утвержденным постановлением администрации района.
5.4. К работе с информационными ресурсами администрации района допускаются служащие, ознакомленные с настоящей Политикой ИБ.
5.5. Для осуществления доступа к информационным ресурсам администрации района служащему создается учетная запись - присваивается уникальный идентификатор (имя, логин) и пароль доступа. Порядок доступа служащих к информационной системе устанавливается в соответствии с правовым актом администрации, определяющим порядок эксплуатации информационной системы. При увольнении учетная запись служащего блокируется. Обязанность по созданию, блокированию учетных записей возлагается на системных администраторов.
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 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) программное обеспечение (ПО).

6. Антивирусная защита

6.1. Антивирусная защита в администрации Палкинского района 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 приобретению лицензионных ключей антивирусного ПО, их обновлению, установке в администрации района возлагается на отдел организационной работы управления делами администрации района.
6.4. Обязанность по установке и регулярному обновлению антивирусного ПО, в том числе антивирусных баз, на АРМ и серверах администрации района возлагается на системного администратора.
6.5. При установке антивирусного ПО системным администратором должны выполняться следующие требования:
- актуализация антивирусных баз на АРМ, подключенных к локальной сети администрации района, должна осуществляться ежедневно в автоматическом режиме через специальный сервер обновлений;
- актуализация антивирусных баз на АРМ, не подключенных к локальной сети администрации района, 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 АРМ.
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 3-го числа месяца, следующего за отчетным, формируется информация о выявленных компьютерных атаках, уязвимости и поражениях вредоносным программным обеспечением информационных ресурсов по форме согласно приложению к настоящей Политике ИБ.

7. Криптографическая защита информации

7.1. Криптографическая защита информации (шифрование) применяется для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении, создания электронной подписи, проверки электронной подписи, создания ключа электронной подписи и ключа проверки электронной подписи.
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 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и

эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».
7.3. Необходимость криптографической защиты информации конфиденциального характера при ее обработке в информационной системе, выбор применяемых СКЗИ устанавливаются в зависимости от класса информационной системы в соответствии с правовым актом администрации Палкинского района, определяющим порядок эксплуатации информационной системы.
7.4. Шифрование осуществляется перед отправкой данных по незащищенным каналам связи или перед помещением на хранение в ненадежных хранилищах.
7.5. Электронная подпись в администрации Палкинского района используется:
- при совершении уполномоченными служащими юридически значимых действий в случаях, установленных действующим законодательством Российской Федерации;
- для ведения электронного документооборота, информация которого не относится к информации конфиденциального характера, в соответствии с порядком эксплуатации используемой системы электронного документооборота.
7.6. Электронная подпись выдается аккредитованным удостоверяющим центром служащим, уполномоченным обращаться за получением квалифицированного сертификата (далее - владелец сертификата ключа проверки электронной подписи), в порядке, установленном Федеральным законом от 06 апреля 2011 г. № 63-ФЗ «Об электронной подписи» и регламентом аккредитованного удостоверяющего центра. 7.7. Для хранения сертификата ключа проверки электронной подписи в форме электронного документа (далее - ключевая информация) владельцу сертификата ключа проверки электронной подписи выдается съемный носитель информации (далее - носитель ключевой информации) под подпись в журнале учета носителей ключевой информации.

Журнал учета носителей ключевой информации ведется и хранится ответственным за выдачу носителей ключевой информации. Ответственный за выдачу носителей ключевой информации определяется распоряжением администрации района.
7.8. Владелец сертификата ключа проверки электронной подписи обязан:
- обеспечить безопасное хранение носителя ключевой информации, исключающее бесконтрольный (несанкционированный) доступ к нему не уполномоченных лиц, а также непреднамеренное уничтожение носителя ключевой информации и (или) ключевой информации, хранящейся на нем;
- защищать паролем ключевую информацию, хранящуюся на носителе ключевой информации;
- подсоединять носитель ключевой информации к АРМ только для подписания электронных документов и в обязательном порядке извлекать из АРМ сразу после окончания работы с ним;
- соблюдать конфиденциальность ключевой информации, принимать меры для предотвращения утраты, раскрытия, искажения и несанкционированного использования ключевой информации;
- применять для формирования электронной подписи только действующий личный ключ электронной подписи.
7.9. Владельцу сертификата ключа проверки электронной подписи запрещается:
- отвечать на подозрительные письма с просьбой выслать ключ электронной подписи, пароль или другую конфиденциальную информацию;
- оставлять носители ключевой информации включенными в АРМ, в легкодоступных местах, в том числе на рабочих столах;
- знакомить или передавать носители ключевой информации лицам, к ним не допущенным;
- снимать несанкционированные копии ключевой информации;
- выводить ключи электронной подписи на дисплей или принтер;
- записывать на носители ключевой информации с ключами электронной подписи иную (постороннюю) информацию, в том числе рабочую.
7.10. При компрометации ключа электронной подписи - утрате доверия к тому, что используемый ключ электронной подписи обеспечивает безопасность информации, связанной с утерей (в том числе с последующим обнаружением), выходом из строя носителя ключевой информации, нарушением правил хранения, возникновением подозрений на утечку или искажение ключевой информации, владелец сертификата ключа проверки электронной подписи обязан:
- немедленно прекратить использование ключа электронной подписи при обмене электронными документами с другими пользователями;
- направить в установленном регламентом аккредитованного удостоверяющего центра порядке заявление об аннулировании сертификата ключа проверки электронной подписи;
- известить о факте утери (выходе из строя) ключа электронной подписи ответственного за выдачу носителей ключевой информации.
7.11. При увольнении или длительном отпуске владелец сертификата ключа проверки электронной подписи обязан:
- сдать ответственному за выдачу носителей ключевой информации носитель ключевой информации под подпись в журнале учета носителей ключевой информации;
- направить в установленном регламентом аккредитованного удостоверяющего центра порядке заявление об аннулировании сертификата ключа проверки электронной подписи.
7.12. Ответственный за выдачу носителей ключевой информации обязан:
- вести учет носителей ключевой информации;
- уничтожать в установленном порядке вышедшие из строя носители ключевой информации;
- убедиться в отсутствии информации на носителе ключевой информации перед его выдачей.

8. Обезличивание персональных данных

8.1. Обезличивание персональных данных в администрации района 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. Необходимость и метод обезличивания персональных данных, обрабатываемых в информационной системе

персональных данных (далее - ИСПДн), устанавливаются правовым актом администрации района, определяющим порядок эксплуатации ИСПДн.
8.3. При использовании процедуры обезличивания не допускается совместное хранение персональных данных и обезличенных данных.
8.4. Обезличивание персональных данных должно производиться перед внесением их в открытую информационную систему и (или) передачей по незащищенным каналам связи.

9. Регламентация использования электронной почты

9.1. Система электронной почты администрации Палкинского района (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 района 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, заражению вирусами;
- получение спама;
- иные угрозы.
9.4. Отправка, получение официальных запросов и ответов в целях исполнения своих функций структурными подразделениями администрации Палкинского района осуществляется с использованием официального адреса электронной почты администрации Палкинского района. Перечень официальных адресов электронной почты администрации Палкинского района утверждается распоряжением администрации района.
Официальный адрес электронной почты администрации района размещается на официальном Интернет-сайте администрации Палкинского района в информационно-телекоммуникационной сети Интернет, на бланках администрации Палкинского района.
9.5. Распоряжением администрации района определяются специалисты, ответственные за работу с официальной электронной почтой администрации Палкинского района.
9.6. Отправка, получение электронных сообщений в целях исполнения должностных обязанностей служащими осуществляется с использованием индивидуального электронного адреса служащего.
При увольнении служащего электронный почтовый ящик отключается с последующим автоматическим удалением.
9.7. При работе с электронной почтой служащие обязаны:
- перед отправкой тщательно проверять отправляемые сообщения;
- 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.
9.8. При работе с электронной почтой служащим запрещено:
- отправлять конфиденциальную информацию без предварительного шифрования криптографическим ПО, разрешенным к использованию в администрации Палкинского района;
- 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, терроризма, религиозных убеждений и верований, политических убеждений, национального происхождения, 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 запрещенные веб-сервисы или 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.
9.9. 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 управляющему делами администрации района.

10. Регламентация работы в сети Интернет

10.1. Сеть Интернет в администрации Палкинского района 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 района вирусами.
10.3. Организацию доступа к сети Интернет для нужд администрации района осуществляет отдел организационной работы управления делами администрации района.
10.4. Доступ к сети Интернет предоставляется служащим с АРМ, закрепленного за служащим для исполнения должностных обязанностей, с использованием учетной записи служащего.
10.5. Угрозы, связанные с работой в сети Интернет:
- легкость перехвата данных и фальсификации 1Р-адресов в сети Интернет;
- заражение вирусами;
- иные угрозы, выявляемые в процессе осуществления деятельности.
10.6. Служащим запрещается:
- осуществлять действия, запрещенные законодательством Российской Федерации;
- отправлять конфиденциальную информацию без предварительного шифрования криптографическим ПО, разрешенным к использованию в администрации Палкинского района;
- распространять информацию, содержащую подрывные, оскорбительные, неэтичные, незаконные материалы, включая оскорбительные комментарии по поводу расы, пола, цвета, инвалидности, возраста, терроризма, религиозных убеждений и верований, политических убеждений, национального происхождения, гиперссылки или другие ссылки на веб-сайты, 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;
- передавать информацию, обрабатываемую в администрации района, посредством иностранных интернет-сервисов, в том числе систем обмена мгновенными сообщениями, голосовой и видеоинформацией, социальных сетей, облачных сервисов.
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 об информационных ресурсах, посещаемых служащим, автоматически протоколируется и при необходимости представляется системным администратором управляющему делами администрации района, главе Палкинского района.
10.9. Доступ к сети Интернет может быть блокирован системным администратором без предварительного уведомления служащего при возникновении угрозы безопасности информации.

11. Регламентация создания, эксплуатации и прекращения эксплуатации информационных систем

11.1. Регламентация создания, эксплуатации и прекращения эксплуатации информационных систем направлена на упорядочение деятельности администрации Палкинского района по созданию информационных систем и обеспечению безопасности информации, содержащейся в информационных системах.
11.2. Принятие решения о создании информационной системы или решения о прекращении эксплуатации информационной системы:
11.2.1. Принятие решения о создании информационной системы.
Руководитель структурного администрации района направляет предложение о создании информационной системы в отдел организационной работы управления делами администрации района.
Предложение о создании информационной системы должно содержать:
- обоснование необходимости создания информационной системы, в том числе требования законодательства Российской Федерации, иных правовых актов;
- оценку (технико-экономической, социальной и другой) целесообразности создания информационной системы;
- цели и задачи информационной системы;
- категорию доступа обрабатываемой информации (общедоступная, конфиденциальная);
- оператора информационной системы.
Отдел организационной работы управления делами администрации района рассматривает предложение о создании информационной системы, принимает решение о целесообразности (об отсутствии целесообразности) создания информационной системы, которое оформляется протоколом. Протокол предоставляется главе Палкинского района в течение 5 рабочих дней с даты его подписания. Глава района принимает решение о создании информационной системы с учетом решения отдела организационной работы управления делами администрации района.
11.2.2. Принятие решения о прекращении эксплуатации информационной системы.
Руководитель структурного подразделения администрации направляет главе Палкинского района предложение о прекращении эксплуатации информационной системы. Предложение о прекращении эксплуатации информационной системы предварительно согласовывается с заместителем главы Администрации района, осуществляющим оперативное руководство по направлению деятельности, управляющим делами администрации района, начальником отдела организационной работы управления делами администрации района.
Предложение о прекращении эксплуатации информационной системы должно содержать:
- обоснование необходимости прекращения эксплуатации информационной системы, в том числе ссылки на изменение законодательства Российской Федерации, иных правовых актов, на основании которых функционировала

информационная система;
- предложения по архивированию, дальнейшему хранению, и (или) уничтожению (стиранию) информации, содержащейся в информационной системе, машинных носителей информации, используемых при эксплуатации информационной системы.

Глава Палкинского района принимает решение о прекращении эксплуатации информационной системы.

11.2.3. Решение о создании информационной системы или решение о прекращении эксплуатации информационной системы утверждается правовым актом администрации Палкинского района. Проект правового акта администрации района подготавливает оператор информационной системы.

11.2.4. Финансирование работ (услуг) по созданию информационной системы осуществляется за счет средств бюджета Палкинского района на основании правового акта администрации района о создании информационной системы и муниципального контракта на оказание услуг по созданию информационной системы, заключенного в соответствии с требованиями Федерального закона от 05 апреля 2013 г. № 44- ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд».

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», 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 администрации Палкинского района, разработанным и утвержденным в соответствии с регламентом утверждения правовых актов администрации Палкинского района о вводе в эксплуатацию, прекращении эксплуатации информационных систем и (или) определении порядка эксплуатации информационной системы (далее — Регламент).

Правовой акт администрации района 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 и (или) эксплуатация информационной системы;
- полномочия структурного подразделения администрации Палкинского района, реализуемые при эксплуатации информационной системы, и (или) задачи, решаемые в информационной системе;
- отнесение информационной системы к категории муниципальной 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. Все функционирующие в структурных подразделениях администрации Палкинского района информационные системы включаются в Реестр информационных систем администрации Палкинского района, утвержденный постановлением администрации района (далее - Реестр информационных систем).

Основанием для включения информационной системы в Реестр информационных систем является правовой акт администрации района о вводе в эксплуатацию информационной системы, изданный в соответствии с Регламентом.

11.7. Основанием для изменения информации об информационной системе, включенной в Реестр информационных систем, является правовой акт администрации района, определяющий порядок эксплуатации информационной системы.

11.8. Основанием для исключения информационной системы из Реестра информационных систем является правовой акт администрации района о прекращении эксплуатации информационной системы, изданный в соответствии с Регламентом.

11.9. Обязанность по ведению Реестра информационных систем возлагается на отдел организационной работы управления делами администрации района.

12. 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 Палкинского района осуществляется внутренний контроль:

12.1.1. использования технических средств, ПО, работы в сети Интернет в структурных подразделениях администрации района по поручению управляющего делами администрации района.

12.1.2. обработки персональных данных в администрации Палкинского района в соответствии с утвержденными постановлением администрации района Правилами осуществления внутреннего контроля соответствия обработки персональных данных в администрации Палкинского района требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами администрации Палкинского района.

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 отдел организационной работы управления делами администрации района. Обязанность по обучению пользованию средствами антивирусного ПО возлагается на системных администраторов.

13. Принципы обеспечения информационной безопасности

13.1. Принцип законности.
13.1.1. При выборе защитных мероприятий, реализуемых системой обеспечения информационной безопасности, должно соблюдаться действующее законодательство. 13.1.2. Принятые меры защиты не должны препятствовать доступу к защищаемой информации со стороны государственных или правоохранительных органов, если такой доступ необходим в случаях, предусмотренных законодательством.
13.1.3. Программно-технические средства, применяемые в администрации района, должны иметь соответствующие лицензии, официально приобретаться у представителей разработчиков этих средств.
13.2. Принцип системности.
При построении системы обеспечения информационной безопасности необходимо применять системный подход, который предполагает взаимосвязь процессов организации защиты информационных ресурсов администрации района, согласованное применение методов и средств защиты информационных ресурсов администрации района.
13.3. Принцип координации.
13.3.1. При организации действий по обеспечению информационной безопасности обеспечивается четкая взаимосвязь соответствующих структурных подразделений между собой, с представителями сторонних организаций, оказывающих услуги в рамках договорных обязательств.
13.3.2. При построении, внедрении и эксплуатации системы обеспечения информационной безопасности обеспечиваются условия для эффективной координации действий всех лиц, обеспечивающих информационную безопасность.
13.4. Принцип дружественности и простоты
13.4.1. Система обеспечения информационной безопасности в администрации района формируется таким образом, чтобы сделать максимально прозрачными для пользователей информационных систем администрации района процессы ее функционирования.
13.4.2. Система обеспечения информационной безопасности в администрации района выстраивается таким образом, чтобы ограничения организационного и технического характера, налагаемые на сотрудников администрации района в связи с реализацией защитных мер, существенно не затрудняли работу с ресурсами информационных систем администрации района.
13.5. Принцип превентивности.
Меры, применяемые администрации района с целью обеспечения информационной безопасности, должны носить упреждающий характер и не допускать реализацию соответствующих угроз и атак.
13.6. Принцип оптимальности и многоуровневости.
13.6.1. Выбор единых программно-технических средств с целью сокращения расходов на создание и поддержку функционирования компонентов системы обеспечения информационной безопасности.
13.6.2. Применение разнородных программно-технических средств защиты, с целью построения целостной системы обеспечения информационной безопасности и устранения возможных уязвимостей.
13.6.3. Использование для создания разных рубежей обеспечения информационной безопасности средств, которые имеют схожие друг с другом функции, но разработанные различными производителями и имеющие различную логику построения защитных механизмов.
13.7. Принцип экономической целесообразности.
13.7.1. Осуществление оценки уровня затрат на обеспечение безопасности, ценности информационных ресурсов и величины возможного ущерба для администрации района в случае нарушения конфиденциальности, целостности и доступности информационных ресурсов.
13.7.2. Выбор необходимого и достаточного уровня защиты информационных ресурсов, при котором затраты, риск и размер возможного ущерба являются приемлемыми.
13.8. Принцип непрерывности и недопустимости открытого состояния.
13.8.1. Система обеспечения информационной безопасности в администрации района строится таким образом, чтобы процесс защиты информационных систем администрации района осуществлялся непрерывно и целенаправленно на протяжении всего жизненного цикла информационных систем.
13.8.2. Система обеспечения информационной безопасности в администрации района при любых возникающих обстоятельствах либо полностью выполняет свои функции, либо полностью блокирует доступ.
13.9. Принцип профессионализма.
13.9.1. Привлечение для разработки и внедрения системы обеспечения информационной безопасности, при необходимости, специализированных организаций, наиболее подготовленных к конкретному виду деятельности и имеющих соответствующие лицензии на выполнения работ и практический опыт в данной области.
13.9.2. Организация профессиональной подготовки служащих для эксплуатации компонентов системы обеспечения

информационной безопасности.
13.10. Принцип выбора решений защиты.
13.10.1. Ориентация на применение современных высокотехнологичных решений и программно-технических средств защиты, хорошо зарекомендовавших себя, интуитивно понятных и не сложных в эксплуатации.
13.10.2. Использование оценки степени корректности функционирования и исполнения защитных функций, отказоустойчивости, проверки согласованности конфигурации различных компонентов и возможности осуществления централизованного администрирования при выборе решений по защите информационных систем.
13.11. Принцип развития.
13.11.1. Развитие и обновление на регулярной основе существующей системы обеспечения информационной безопасности.
13.11.2. Ориентация на преемственность принятых ранее решений по защите, на анализ функционирования информационных систем и самой системы обеспечения информационной безопасности.
13.12. Принцип персональной ответственности и разделения обязанностей.
13.12.1. Руководство администрации района определяет права и ответственность каждого конкретного служащего (в пределах его должностных обязанностей) за обеспечение безопасности информационных ресурсов администрации района.
13.12.2. Система обеспечения информационной безопасности администрации района обеспечивает разделение полномочий в информационных системах, обязанностей и ответственности между служащими, исключающее возможность нарушения критически важных для администрации района процессов или создания уязвимостей в защите информационных ресурсов.
13.13. Принцип минимизации привилегий пользователей.
Обеспечение пользователей привилегиями минимально достаточными для выполнения ими своих функций в администрации района, в соответствии со своими должностными обязанностями.

14. Зоны ответственности участников процесса обеспечения информационной безопасности

14.1. Руководство администрации района:
14.1.1. Создает условия, при которых каждый служащий администрации района знает свои обязанности и задачи в отношении информационных ресурсов и обеспечивает наличие необходимого разделения функций и полномочий в целях недопущения конфликта интересов.
14.1.2. Назначает служащих, ответственных за создание и использование средств защиты информации, обрабатываемой в администрации района, реализацию процессов обеспечения информационной безопасности, а также их контроля.
14.1.3. Обеспечивает достаточную численность и квалификацию персонала, ответственного за построение и поддержание процессов обеспечения информационной безопасности, внедрение и управление средств защиты информации, а также контроль и мониторинг текущего состояния системы обеспечения информационной безопасности администрации района.
14.1.4. Инициирует, осуществляет поддержку и контролирует выполнение всех процессов обеспечения информационной безопасности в администрации района. 14.1.5. Анализирует результаты работ по обеспечению информационной безопасности и на их основе принимает решения о необходимости развития системы обеспечения информационной безопасности, о возможности принятия остаточных рисков информационной безопасности, о выделении ресурсов, необходимых для реализации Политики информационной безопасности.
14.2. Отдел организационной работы управления делами администрации района:
14.2.1. Подготавливает предложения по доработке Политики информационной безопасности в части технического обеспечения информационных систем администрации района.
14.2.2. Разрабатывает процедуры эффективного управления техническими и программными средствами информационных систем и применяет их в практической деятельности в отношении всех систем, действующих в администрации района.
14.2.3. Организует проведение необходимого инструктажа сотрудников структурных подразделений в части вопросов безопасной эксплуатации информационных систем. 14.2.4. Обеспечивает защиту доступа ко всему серверному и коммутационному оборудованию, носителям информации, которые используются в соответствующих структурных подразделениях.
14.2.5. Осуществляет мероприятия по поддержке сопровождения и использования информационных систем.
14.2.6. Обеспечивает отказоустойчивость всего программно-аппаратного комплекса и процедуру регламентированного восстановления работоспособности после отказов компонентов.
14.2.7. Регулярно обновляет программные и программно-аппаратные комплексы СЗИ в администрации района.
14.2.8. Осуществляет поддержку функционирования информационных систем и принимает необходимые меры по конфигурированию систем для обеспечения необходимого уровня информационной безопасности администрации района.
14.2.9. Контролирует работоспособность устройств бесперебойного питания критичных для администрации района информационных систем.
14.2.10. Обеспечивает физическую защиту помещений, в которых располагаются критичные для администрации района информационные системы.
14.2.11. Обеспечивает сопровождение устройств контроля доступа в помещения администрации района.
14.2.12. Обеспечивают защиту информационных ресурсов администрации района от случайного или намеренного уничтожения, искажения, разглашения.
14.2.13. Контролирует выполнение установленных правил и процедур обеспечения информационной безопасности в администрации района.
14.3. Руководители структурных подразделений администрации района:
14.3.1. Обязаны соблюдать требования действующего законодательства Российской Федерации и внутренних

документов администрации района в части обеспечения информационной безопасности.
14.3.2. Обеспечивают контроль за соблюдением норм и правил обеспечения информационной безопасности в своем структурном подразделении и информируют управляющего делами администрации района о любых подозрительных событиях или нарушениях действующих правил обеспечения информационной безопасности. 14.3.3. Обеспечивают соответствие действий сотрудников подразделения Политике информационной безопасности, внутренним документам по информационной безопасности и любым другим распоряжениям администрации района по вопросам информационной безопасности.
14.3.4. Организуют проведение необходимого инструктажа по вопросам выполнения правил информационной безопасности для всех сотрудников своего структурного подразделения.
14.3.5. Контролируют выполнение сотрудниками структурного подразделения установленных правил в целях обеспечения физической безопасности компьютерного оборудования и носителей информации.
14.3.6. Своевременно информируют руководство о всех выявленных сбоях в работе информационных систем.
14.3.7. Контролируют доступ к необходимым информационными ресурсам сотрудников своего структурного подразделения в соответствии с потребностью в пределах служебных обязанностей.
14.4. Служащие администрации района:
14.4.1. Соблюдают и выполняют требования Политики информационной безопасности, соответствующих локальных актов, документов администрации района по вопросам информационной безопасности.
14.4.2. Соблюдают конфиденциальность данных, доступ к которым был ими получен. 14.4.3. Обеспечивают физическую безопасность всего технического оборудования и носителей информации, используемых в работе.
14.4.4. Не допускают самовольного подключения и использования в автоматизированной информационной системе личного компьютерного и цифрового оборудования, а также носителей информации.
14.4.5. Не допускают самовольную установку программного обеспечения на компьютеры, входящие в состав информационной системы.
14.4.6. Своевременно информируют руководителя своего структурного подразделения о всех случаях нарушения информационной безопасности и о всех выявленных сбоях в работе программных и программно-аппаратных средств.
14.4.7. Проявляют осмотрительность в отношении любых действий, которые могут повлечь за собой снижение уровня информационной безопасности.
14.5. Сторонние физические и юридические лица:
Соблюдают и выполняют требования Политики информационной безопасности, соответствующих локальных актов и документов администрации района и других распоряжений руководства по вопросам информационной безопасности при исполнении договорных обязательств.

15. Основные требования к процессам обеспечения информационной безопасности

15.1. Общие положения.
Методическое руководство, разработку конкретных требований по защите информации, согласование выбора средств вычислительной техники и связи, технических и программных средств защиты, организацию работ по выявлению возможностей и предупреждению утечки и нарушения целостности защищаемой информации осуществляет отдел организационной работы управления делами администрации района.
15.2. Физическая безопасность и безопасность на рабочем месте.
15.2.1 Система защиты зданий и помещений администрации района, объектов и технических средств информационных систем администрации района обеспечивает выполнение следующих функций:
- разграничение доступа служащих в помещения администрации района в соответствии с их полномочиями и функциональными обязанностями;
- регистрацию фактов входа служащих в помещения с повышенными требованиями к режиму их посещения (серверные помещения, архивы и т.д.);
- регистрацию фактов входа посторонних лиц в здания администрации района;
- предотвращение доступа посторонних лиц в помещения, где размещены аппаратные и сетевые ресурсы информационных систем;
- разрешительный режим вноса/выноса (ввоза/вывоза) компьютерного оборудования, средств записи и хранения информации.
15.2.2. Определяется перечень технических средств, находящихся в специальных контролируемых зонах.
15.2.3. К техническим средствам, которые выделяются в специальные контролируемые зоны необходимо отнести следующие группы ресурсов:
- основные информационные серверы и средства вычислительной техники, на которых осуществляется обработка и хранение информации ограниченного распространения;
- сетевое оборудование и серверы, обеспечивающие работу критических систем;
- файловые серверы, на которых хранятся данные, в том числе резервные;
- критичные для деятельности администрации района системы и коммуникационное оборудование, обеспечивающее внешние коммуникации администрации района. 15.2.4. Контролируемые зоны защищаются соответствующими системами контроля и управления доступом, обеспечивая доступ только авторизованному персоналу.
15.2.5. Доступ в контролируемые зоны сторонних лиц или представителей других организаций возможен только в сопровождении уполномоченного работника администрации района.
15.2.6. Размещение и эксплуатация рабочих станций, серверов и сетевого оборудования администрации района осуществляется в помещениях, оборудованных замками, средствами сигнализации и (при необходимости) постоянно находящихся под охраной или наблюдением.
15.2.7. Размещение технических средств вывода и отображения информации в помещениях администрации района производится с учетом исключения возможности визуального просмотра информации посторонними лицами и персоналом, не допущенным к работе с данной информацией.

15.2.8. Служащие администрации района на момент своего отсутствия на рабочем месте обязаны исключить возможность наличия на рабочем столе документов или носителей с защищаемой информацией.
15.2.9. Технические средства и оборудование должны размещаться и храниться таким образом, чтобы сократить возможный риск его повреждения и угрозы несанкционированного доступа.
15.2.10. Помещения администрации района должны быть оборудованы детекторами огня и дыма, огнетушителями, средствами охранно-пожарной сигнализации.
15.2.11. Основное техническое оборудование администрации района должно быть защищено от перебоев в подаче электроэнергии путем подключения к электросети с применением источников бесперебойного питания. Источники бесперебойного питания необходимо регулярно тестировать и проверять уполномоченным работникам администрации района в соответствии с рекомендациями производителя. 15.2.12. Пользователи портативных технических средств не должны оставлять техническое оборудование и носители информации без присмотра.
15.2.13. Портативные технические средства не должны оставаться за пределами контролируемой зоны администрации района дольше, чем того требует служебная необходимость, если иное не определено руководством администрации района.
15.3. Безопасность при работе с носителями информации.
15.3.1. В администрации района должны соблюдаться меры по безопасной работе с электронными носителями информации с целью контроля их использования, для предотвращения несанкционированного копирования и разглашения защищаемой информации, внесения изменений или уничтожения указанной информации, а также внесения изменений в работу информационных систем.
15.3.2. Служащие администрации района должны использовать электронные носители информации только для выполнения своих служебных обязанностей. Использование электронных носителей информации в администрации района в иных целях строго запрещено.
15.3.3. Электронные носители информации в администрации района должны быть учтены путем присвоения каждому носителю инвентаризационного номера и назначения владельца.
15.3.4. Электронные носители информации должны храниться в помещениях, исключающих получение к ним несанкционированного доступа при этом должен быть обеспечен контроль доступа к носителям.
15.3.5. Для контроля процессов использования и хранения электронных носителей информации разрабатывается порядок плановой инвентаризации носителей.
15.3.6. В случае кражи или потери электронных носителей информации, а также иных инцидентов, которые могут привести к разглашению защищаемой информации, должны проводиться мероприятия по расследованию указанных инцидентов.
15.3.7. При снятии электронного носителя информации с эксплуатации, все данные, хранящиеся на нем, должны быть гарантированно стерты.
15.3.8. При утилизации электронных носителей информации должна быть обеспечена невозможность восстановления записанной на них информации.
15.3.9. Факт уничтожения информации и утилизации носителя информации фиксируется в соответствии с порядком, установленным в администрации района. 15.4. Техническое обслуживание оборудования.
15.4.1. Технические средства всех систем администрации района должны проходить на регулярной основе сервисное обслуживание в соответствии с рекомендациями производителей оборудования.
15.4.2. Ремонт и сервисное обслуживание оборудования должны выполняться только квалифицированным персоналом.
15.4.3. Техническое обслуживание оборудования и систем сторонними организациями не должно приводить к риску нарушения конфиденциальности защищаемой информации.
15.5. Взаимодействие с третьими лицами.
В целях обеспечения информационной безопасности администрации района при взаимодействии с третьими лицами должны выполняться следующие мероприятия:
- заключение соглашения о неразглашении конфиденциальной информации;
- контроль за действиями третьих лиц;
- в договорах с третьими лицами предусматривать право администрации района на проведение аудита обеспечения безопасности той информации, которая передается третьим лицам.
15.6. Управление жизненным циклом информационных систем.
15.6.1. Мероприятия по управлению жизненным циклом автоматизированных информационных систем должны быть направлены на обеспечение информационной безопасности при вводе в действие, эксплуатации, сопровождении и модернизации, вывода из эксплуатации информационных систем, автоматизирующих деятельность администрации района.
15.6.2. Основой при выборе или разработке информационных систем должны являться технические задания, содержащие требования информационной безопасности для информационных систем.
15.6.3. Любое планируемое к внедрению изменение информационной системы предварительно должно быть протестировано на совместимость и отсутствие нарушений работоспособности системных компонентов.
15.6.4. Работы по модернизации автоматизированной информационной системы, в том числе по установке программного обеспечения и обновлений, должны проводиться в нерабочее время или время наименьшей рабочей нагрузки.
15.6.5. При выводе из эксплуатации автоматизированных информационных систем должно обеспечиваться гарантированное удаление обрабатываемой и хранимой в них информации с использованием специализированных программных средств или путем физического уничтожения носителей информации.
15.6.6. Все процедуры обеспечения информационной безопасности, установленные в администрации района в отношении информационных систем, должны выполняться и контролироваться ответственными за информационную безопасность лицами.
15.7. Антивирусная защита.
15.7.1. В целях предупреждения, обнаружения и устранения вредоносных программ в администрации района на

постоянной основе должны использоваться средства антивирусной защиты.
15.7.2. Обязательному антивирусному контролю должна подлежать любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация, хранимая на подключаемых съемных носителях, при непосредственном обращении к ней.
15.7.3. При установке программного обеспечения на серверы информационных систем администрации района или их обновлении должна автоматически выполняться предварительная проверка данного программного обеспечения на отсутствие вредоносного программного обеспечения.
15.7.4. Сигнатурные базы вредоносного программного обеспечения и антивирусные средства защиты должны регулярно обновляться.
15.7.5. Пользователи информационных систем администрации района не должны иметь возможность получения доступа к конфигурации антивирусного средства защиты или его отключения.
15.7.6. В администрации района необходимо определить процедуру для обработки и восстановления инфицированных данных и отслеживание источника заражения.
15.8. Контроль доступа к информационным системам.
15.8.1. Все служащие администрации района, допущенные к работе с информационными системами несут персональную ответственность за нарушения установленного порядка обработки информации, правил хранения, использования и передачи, находящихся в их распоряжении защищаемых ресурсов системы.
15.8.2. Уровень полномочий пользователя в информационной системе должен определяться в соответствии с его должностными обязанностями и производственной необходимостью.
15.8.3. Доступ пользователей к информационным системам администрации района должен контролироваться системным администратором.
15.8.4. Осуществление регулярного контроля выполнения политики и иных документов, касающихся регламентации допуска работников администрации района к информационным системам.
15.9. Идентификация и аутентификация.
15.9.1. Доступ пользователей к информационным системам должен предоставляться только после успешного завершения процедур идентификации, аутентификации и авторизации.
15.9.2. Получение пользователем имени в системе и парольной информации, которые обеспечивают доступ пользователя к ресурсам системы, должно осуществляться по представлению руководителей структурных подразделений.
15.10. Безопасность пароля.
15.10.1. С целью обеспечения защиты от несанкционированного доступа к информационным системам устанавливаются требования к выбору парольной информации, обеспечивающие достаточную степень стойкости паролей.
15.10.2. Для обеспечения конфиденциальности парольной информации пользователю запрещается хранить значения своих паролей на бумажном носителе в открытом виде и в свободном доступе.
15.10.3 Для обеспечения конфиденциальности парольной информации пользователям запрещается передавать значения своих паролей третьим лицам. 15.10.4. При вводе пароля пользователем для доступа к информационной системе администрации района должно исключаться отображение парольной информации на экране монитора в открытом виде.
15.10.5. Процедура смены парольной информации в информационных системах администрации района должна проводиться на регулярной основе.
15.11. Регистрация событий.
Осуществление регистрации событий безопасности на всех компонентах информационных систем администрации района, в которых обрабатывается, хранится или по средствам которых передается защищаемая информация.
15.12. Использование СКЗИ.
15.12.1. Решение об использовании СКЗИ в интересах защиты собственных информационных ресурсов принимается руководством администрации района в соответствии с законодательством Российской Федерации.
15.12.2. При эксплуатации СКЗИ и ключевой информации все сотрудники администрации района должны выполнять требования нормативных правовых актов, издаваемых федеральным органом исполнительной власти в области обеспечения безопасности, документов администрации района по обеспечению безопасности использования СКЗИ, а также эксплуатационной документации производителя СКЗИ.
15.13. Безопасность информационной сети.
15.13.1. Установление надлежащего контроля в отношении локальной вычислительной сети и всех внешних информационных коммуникаций администрации района для обеспечения защиты данных и защиты информационных систем администрации района от несанкционированного доступа.
15.13.2. Должны быть определены цели использования сети Интернет и требования к процедуре использования ресурсов сети Интернет. Использование сети Интернет служащими в личных целях строго запрещено.
15.13.3. Доступ к информационным сервисам сети Интернет предоставляется служащим администрации района только в случае производственной необходимости.
16.13.4. Контроль использования работниками ресурсов сети Интернет должен осуществляться уполномоченными работниками на постоянной основе.
16.14. Использование корпоративной электронной почты.
15.14.1. Система корпоративной электронной почты должна использоваться в администрации района с целью организации обмена электронными сообщениями между служащими, а также между служащими администрации района и внешними абонентами.
15.14.2. Предоставление и прекращение доступа к ресурсам корпоративной электронной почты должно осуществляться только на основе оформленной заявки. 15.14.3. В администрации района должно быть установлено специальное программное обеспечение, осуществляющее контроль всех входящих сообщений на наличие вредоносного программного обеспечения.
15.14.4. В администрации района должны быть предусмотрены механизмы архивирования и резервного копирования

корпоративной электронной почты в автоматическом режиме.
15.15. Резервное копирование и восстановление данных.
15.15.1. Осуществление резервного копирования для:
- файловых серверов и серверов приложений, критичных для деятельности администрации района;
- операционных систем файловых серверов и прикладных программ;
- приложений, критичных для деятельности администрации района;
- рабочих данных.
15.15.2. Частота и режим резервного копирования устанавливаются таким образом, чтобы обеспечить минимальную потерю данных и допустимое время восстановления.
15.15.3. Резервное копирование и восстановление ресурсов информационных систем администрации района должны проводить уполномоченные работники администрации района.
15.15.4. Резервное копирование должно осуществляться в автоматическом режиме с применением специализированного программно-аппаратного комплекса.

16. Основные требования к процессам управления информационной безопасностью

16.1. Управление рисками.
16.1.1. Выбор требований по информационной безопасности и защитных механизмов, применяемых в системе информационной безопасности, должен основываться на проведении анализа рисков нарушения основных свойств безопасности для наиболее критичных информационных ресурсов администрации района.
16.1.2. Основой оценки рисков должна быть оценка условий и факторов, которые могут стать причиной нарушения свойств целостности, конфиденциальности и доступности для ресурсов информационной системы администрации района.
16.1.3. Результатом проведения анализа рисков должен быть комплекс мер, направленных на снижение возможного негативного влияния на основную деятельность администрации района при реализации той или иной угрозы и обеспечивающих достаточный уровень защищенности информационных систем администрации района.
16.2. Управление инцидентами информационной безопасности.
16.2.1. Для обеспечения эффективного разрешения инцидентов информационной безопасности в администрации района, минимизации потерь и уменьшения риска возникновения повторных инцидентов должно осуществляться эффективное управление инцидентами информационной безопасности.
16.2.2. Для управления инцидентами информационной безопасности должна быть создана система учета произошедших инцидентов, которая представляет собой комплекс средств и мероприятий для сбора и консолидации информации об инцидентах.
16.2.3. В отношении каждого произошедшего инцидента должен выполняться его анализ и разработка эффективных мер реагирования на данный инцидент.
16.3. Мониторинг текущего уровня информационной безопасности.
16.3.1. Для обеспечения высокого уровня контроля в отношении системы обеспечения информационной безопасности в администрации района на постоянной основе должен проводиться комплексный анализ существующих защитных механизмов и возникающих инцидентов информационной безопасности, а также периодический аудит всей системы обеспечения информационной безопасности. 16.3.2. Процесс мониторинга системы обеспечения информационной безопасности должен включать в себя контроль организационных и технических защитных мер, анализ параметров конфигурации и настройки защитных механизмов.
16.3.3. При проведении контрольных мероприятий, связанных с оценкой функционирования защитных мер в администрации района, уполномоченные работники должны придерживаться следующих принципов:
- не нарушать функционирование текущей деятельности администрации района;
- действовать в соответствии с внутренними документами администрации района по информационной безопасности;
- не скрывать факты выявленных инцидентов и нарушений требований информационной безопасности;
- оформлять отчеты, подтверждающие выполнение мероприятий по обеспечению информационной безопасности.
16.3.4. Информация, полученная в ходе проведения контролирующих мероприятий о действиях, событиях и параметрах, имеющих отношение к функционированию защитных мер, должна консолидироваться и храниться в местах, исключающих получение к ней несанкционированного доступа.
16.3.5. Мониторинг данных о зарегистрированных событиях информационной безопасности должен проводиться, по возможности, с использованием встроенных механизмов настройки и аудита событий в программных и программно-технических средствах, используемых в информационных системах администрации района.
16.4. Аудит системы обеспечения информационной безопасности.
16.4.1. В целях оценки текущего уровня информационной безопасности уполномоченные работники администрации района на регулярной основе должны проводить аудит информационной безопасности.
16.4.2. Внутренние аудиты или самооценки должны выполняться, по возможности, служащими администрации района.
16.4.3. Результатом выполнения аудитов по информационной безопасности должны стать отчеты о выполненном аудите информационной безопасности, составляемые специалистами администрации района.
16.4.4. По результатам аудита определяются действия, необходимые для устранения обнаруженных несоответствий в процессе аудита и вызвавших их причин.
16.5. Управление персоналом.
16.5.1. Организация такого процесса управления персоналом, который обеспечит доверительное отношение к работникам, а также организует комплексное противодействие угрозам информационной безопасности, исходящим от персонала администрации района.
16.5.2. Выполнение обязательных проверок при приеме новых работников на работу с точки зрения достоверности сообщаемых ими данных и с позиции оценки их профессиональных навыков.
16.5.3. Организация работы в направлении повышения осведомленности и обучения в области информационной

безопасности.
16.5.4. Повышение осведомленности служащих администрации района:
- по существующей в администрации района политике информационной безопасности;
- по применяемым в администрации района защитным мерам;
- по правильному использованию защитных мер в соответствии с внутренними документами администрации района.

17. Ответственность за нарушения настоящей Политики информационной безопасности

17.1. 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.
17.2. При обнаружении нарушения служащими настоящей Политики ИБ системный администратор устанавливает причины возникновения нарушения и направляет служебную записку о выявленном нарушении управляющему делами администрации района, главе района. Глава района принимает решение о необходимости привлечения служащего к ответственности.
Системный администратор ведет учет всех выявленных случаев нарушения безопасности информации.

18. Заключение

18.1. Настоящая Политика является внутренним документом администрации, общедоступной и подлежит размещению на официальном сайте администрации.
18.2. Настоящая Политика подлежит изменению, дополнению в случае появления новых законодательных актов и специальных нормативных документов по обработке и защите персональных данных.
18.3. Контроль исполнения требований настоящей Политики осуществляется ответственным лицом за обеспечение безопасности персональных данных администрации.
18.4. Ответственность должностных лиц администрации, имеющих доступ к конфиденциальной информации, за невыполнение требований норм, регулирующих обработку и защиту информации, определяется в соответствии с законодательством Российской Федерации и внутренними документами администрации.

Приложение
к Общей политике информационной безопасности
администрации Палкинского района

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

	Форма проявления угрозы безопасное ти	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 антивирусным 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
постановлением администрации Палкинского района
от 13.06.2023 г. № 294

Регламент
утверждения правых актов администрации Палкинского района о вводе в эксплуатацию, прекращении эксплуатации информационных систем и (или) определении порядка эксплуатации информационной системы

№	Назначение правового акта администрации Палкинского района	Разработчик	Обязательное согласование	Вид правового акта администрации Палкинского района	Обязательная рассылка
1	2	3	4	5	6
Для информационных систем, оператором которых являются структурные подразделения администрации Палкинского района					
1.1	О вводе в эксплуатацию (вместе с определением порядка эксплуатации) вновь созданной информационной системы	Отдел организационной работы управления делами администрации района совместно с структурным подразделением администрации Палкинского района по направлению деятельности	Отдел организационной работы управления делами администрации района совместно с структурным подразделением администрации Палкинского района по направлению деятельности, правовое управление администрации района	Распоряжение администрации Палкинского района	Отдел организационной работы управления делами администрации района совместно с структурным подразделением администрации Палкинского района по направлению деятельности
1.2.	Об определении порядка эксплуатации информационной системы, включенной в Реестр информационных систем	Отдел организационной работы управления делами администрации района совместно с структурным подразделением администрации Палкинского района по направлению деятельности	Отдел организационной работы управления делами администрации района совместно с структурным подразделением администрации Палкинского района по направлению деятельности, правовое управление администрации района	Распоряжение администрации Палкинского района	Отдел организационной работы управления делами администрации района совместно с структурным подразделением администрации Палкинского района по направлению деятельности
1.3.	О прекращении эксплуатации информационной системы	Отдел организационной работы управления делами администрации района совместно с структурным подразделением администрации Палкинского района по направлению деятельности	Отдел организационной работы управления делами администрации района совместно с структурным подразделением администрации Палкинского района по направлению деятельности, правовое управление администрации района	Распоряжение администрации Палкинского района	Отдел организационной работы управления делами администрации района совместно с структурным подразделением администрации Палкинского района по направлению деятельности