АДМИНИСТРАЦИЯ КУЙБЫШЕВСКОГО МУНИЦИПАЛЬНОГО ОКРУГА

ПОСТАНОВЛЕНИЕ

«05» декабря 2025 г. № 214-п

пгт Розовка

ОБ УТВЕРЖДЕНИИ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В АДМИНИСТРАЦИИ КУЙБЫШЕВСКОГО МУНИЦИПАЛЬНОГО ОКРУГА

В соответствии с Федеральным законом от 20.03.2025 г. № 33-ФЗ «Об общих принципах организации местного самоуправления в единой системе публичной власти», статьями 6, 16 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Уставом муниципального образования «Куйбышевский муниципальный округ Запорожской области», Администрация Куйбышевского муниципального округа,

ПОСТАНОВЛЯЕТ:

1. Утвердить Политику информационной безопасности в Администрации Куйбышевского муниципального округа в соответствии с приложением 1 к настоящему постановлению.
2. Настоящее постановление вступает в силу со дня его подписания.
3. Контроль за исполнением настоящего постановления оставляю за собой.

Глава Куйбышевского муниципального округа **К.Г. Белов**

Приложение 1
к постановлению администрации
Куйбышевского муниципального
округа от 05.12.2025 № 214-п

ПОЛИТИКА
информационной безопасности в Администрации Куйбышевского муниципального округа

РАЗДЕЛ I.
ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Политика информационной безопасности в Администрации Куйбышевского муниципального округа (далее - Политика ИБ) разработана в целях установления безопасных способов обработки информации в электронном виде, в том числе в информационных системах (сайтах) Администрации Куйбышевского муниципального округа (далее - информационная система).

1.2. Настоящая Политика ИБ определяет в Администрации Куйбышевского муниципального округа (далее - Администрация) цели и задачи защиты информации, устанавливает методы защиты информации, которыми должны руководствоваться муниципальные служащие Куйбышевского муниципального округа, иные работники Администрации, 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 ИВ 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 структурных подразделениях Администрации, 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 ИВ распространяется на все структурные подразделения Администрации. При осуществлении санкционированного доступа к информационным ресурсам Администрации 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 ИВ являются Конституция Российской Федерации, Гражданский кодекс Российской

Федерации, Уголовный кодекс Российской Федерации, Кодекс Российской Федерации об административных правонарушениях, Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», иные нормативные правовые акты Российской Федерации, акты и документы Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности, Федеральной службы по надзору в сфере связи и массовых коммуникаций.

РАЗДЕЛ II.
ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. В настоящей Политике ИВ 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;

- 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 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 Куйбышевского муниципального округа (далее - оператор информационной системы) - функциональный орган или структурное подразделение Администрации, 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 структурном подразделении Администрации;

- 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;

- 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.

РАЗДЕЛ III.
ЦЕЛИ И ЗАДАЧИ ЗАЩИТЫ ИНФОРМАЦИИ В АДМИНИСТРАЦИИ, ОСНОВНЫЕ ВИДЫ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

3.1. Обеспечение информационной безопасности в Администрации (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 является вся информация, обрабатываемая в Администрации (структурных подразделениях Администрации) (далее - информация), независимо от ее местонахождения в информационной среде. В Администрации 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 являются:

- выявление и оценка потенциальных угроз информационной безопасности и уязвимостей 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 применяются:

- регламентация доступа в служебные помещения Администрации;

- разграничение доступа к техническим средствам и информационным ресурсам Администрации;

- 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.

РАЗДЕЛ IV.
РЕГЛАМЕНТАЦИЯ ДОСТУПА В СЛУЖЕБНЫЕ ПОМЕЩЕНИЯ АДМИНИСТРАЦИИ

4.1. Регламентация доступа в служебные помещения Администрации 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 осуществляется в соответствии с Положением о пропускном и внутриобъектовом режимах в административных зданиях (помещениях) Администрации Куйбышевского муниципального округа, утверждаемым правовым актом Администрации.

Доступ в помещения, в которых ведется обработка персональных данных, осуществляется в соответствии с порядком доступа муниципальных служащих Администрации Куйбышевского муниципального округа в помещения, в которых ведется обработка персональных данных, утверждаемым правовым актом Администрации.

РАЗДЕЛ V.
РАЗГРАНИЧЕНИЕ ДОСТУПА К ТЕХНИЧЕСКИМ СРЕДСТВАМ И ИНФОРМАЦИОННЫМ РЕСУРСАМ АДМИНИСТРАЦИИ

5.1. Разграничение доступа к техническим средствам и информационным ресурсам Администрации 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 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. К работе с информационными ресурсами Администрации допускаются служащие, ознакомленные с настоящей Политикой ИБ.

5.4. Для осуществления доступа к информационным ресурсам Администрации служащему создается учетная запись - присваивается уникальный идентификатор (имя, логин) и пароль доступа.

При увольнении учетная запись служащего блокируется.

Обязанность по созданию, блокированию учетных записей возлагается на системных администраторов.

5.5. 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.

5.6. При работе на АРМ служащие обязаны:

- работать только под своей учетной записью;
- блокировать доступ к АРМ при отсутствии на рабочем месте.

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

РАЗДЕЛ VI.
АНТИВИРУСНАЯ ЗАЩИТА

6.1. Антивирусная защита в Администрации 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 установке и регулярному обновлению антивирусного ПО, в том числе антивирусных баз, на АРМ и серверах Администрации возлагается на соответствующих системных администраторов.

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

- актуализация антивирусных баз на АРМ, подключенных к локальной сети Администрации, должна осуществляться ежедневно в автоматическом режиме через специальный сервер обновлений;
- актуализация антивирусных баз на АРМ, не подключенных к локальной сети Администрации, 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.

6.5. 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.

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

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

РАЗДЕЛ VII.
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 09.02.2005 № 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, 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 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 06.04.2011 № 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 в Администрации определяется руководителем Администрации.

Обязанность по выдаче носителей ключевой информации в Администрации возлагается на отдел организационной работы внутренней политики и приема граждан.

7.8. Владелец сертификата ключа проверки электронной подписи обязан:

обеспечить безопасное хранение носителя ключевой информации, исключающее бесконтрольный (несанкционированный) доступ к нему неуполномоченных 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.

РАЗДЕЛ VIII.
ОБЕЗЛИЧИВАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. Обезличивание персональных данных в Администрации 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 05.09.2013 № 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 Администрации, 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.

РАЗДЕЛ IX.
РЕГЛАМЕНТАЦИЯ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ПОЧТЫ

9.1. Система электронной почты Администрации (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 у несанкционированной рассылки информации, заражения информационных ресурсов Администрации 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.

9.4. Отправка, получение официальных запросов и ответов в целях исполнения своих функций Администрации осуществляется с использованием официального адреса электронной почты Администрации. Официальный адрес электронной почты Администрации размещается на официальном Интернет сайте Администрации в информационно-телекоммуникационной сети Интернет, на бланках Администрации.

9.5.Руководитель Администрации определяет специалистов, ответственных за работу с официальной электронной почтой Администрации.

9.6.При работе с электронной почтой служащие обязаны:

- перед отправкой тщательно проверять сообщения на отсутствие информации, указанной в подпункте 4пункта 9.7 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.

9.7.При работе с электронной почтой служащим запрещено: отправлять конфиденциальную информацию без:

- предварительного шифрования криптографическим ПО, разрешенным к использованию в Администрации;

- 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, 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 веб-сервисы Google, УаНоо, 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.

9.8.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 структурного подразделения Администрации.

РАЗДЕЛ X.
РЕГЛАМЕНТАЦИЯ РАБОТЫ В СЕТИ ИНТЕРНЕТ

10.1. Сеть Интернет в Администрации используется служащими для получения информации в рамках исполнения должностных обязанностей.

Регламентация работы в сети Интернет осуществляется с целью снижения риска заражения информационных ресурсов Администрации вирусами.

10.2. Организацию доступа к сети Интернет для нужд Администрации осуществляет отделом организационной работы, внутренней политики и приема граждан.

10.3. Доступ к сети Интернет предоставляется служащим с АРМ, закрепленного за служащим для исполнения должностных обязанностей, с использованием учетной записи служащего.

10.4. Угрозы, связанные с работой в сети Интернет:

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

10.5. Служащим запрещается:

- осуществлять действия, запрещенные законодательством Российской Федерации;
- отправлять конфиденциальную информацию без предварительного шифрования криптографическим ПО, разрешенным к использованию в Администрации;
- 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, 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 посредством иностранных интернет-сервисов, в том числе систем обмена мгновенными сообщениями, голосовой и видеоинформацией (WhatsApp, Skype и другие), социальных сетей (Facebook и другие), облачных сервисов (Google и другие);

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

10.7. Вся информация об информационных ресурсах, посещаемых служащим, автоматически протоколируется и при необходимости представляется системными администраторами руководителю Администрации, соответствующему руководителю структурного подразделения Администрации.

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

РАЗДЕЛ XI.
РЕГЛАМЕНТАЦИЯ СОЗДАНИЯ, ЭКСПЛУАТАЦИИ И ПРЕКРАЩЕНИЯ ЭКСПЛУАТАЦИИ ИНФОРМАЦИОННЫХ СИСТЕМ

11.1. Регламентация создания, эксплуатации и прекращения эксплуатации информационных систем направлена на упорядочение деятельности структурных подразделений Администрации 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 подразделения Администрации направляет предложение о создании информационной системы в отдел организационной работы, внутренней политики и приема граждан (далее – Отдел организационной работы).

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 принимает решение о целесообразности (об отсутствии целесообразности) создания информационной системы (далее – решение Отдела организационной работы), которое оформляется протоколом.

Протокол предоставляется Главе Куйбышевского муниципального округа в течение 5 рабочих дней с даты его подписания.

Глава Куйбышевского муниципального округа принимает решение о создании информационной системы с учетом решения Отдела организационной работы.

11.2.2. Принятие решения о прекращении эксплуатации информационной системы.

Руководитель структурного подразделения Администрации направляет Главе Куйбышевского муниципального округа предложение о прекращении эксплуатации информационной системы. Предложение о прекращении эксплуатации информационной системы предварительно согласовывается с заместителем главы Администрации, осуществляющим оперативное руководство по направлению деятельности.

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 Куйбышевского муниципального округа 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. Проект правового акта Администрации подготавливает оператор информационной системы.

11.2.4. Финансирование работ (услуг) по созданию информационной системы осуществляется за счет бюджета Куйбышевского муниципального округа на основании правового акта Администрации о создании информационной системы и муниципального контракта на оказание услуг по созданию информационной системы, заключенного в соответствии с требованиями Федерального закона от 05.04.2013 № 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 Р 59793-2021. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы стадии создания, утвержденным Приказом Федерального агентства по техническому регулированию и метрологии от 25.10.2021 № 1285-ст, 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. Правовой акт Администрации 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, 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 27.07.2006 № 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 информационные системы включаются в Реестр информационных систем Администрации, утвержденный постановлением Администрации (далее - Реестр информационных систем).

Основанием для включения информационной системы в Реестр информационных систем является правовой акт Администрации о вводе в эксплуатацию информационной системы.

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

11.8. Основанием для исключения информационной системы из Реестра информационных систем Администрации является правовой акт о прекращении эксплуатации информационной системы.

РАЗДЕЛ 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 осуществляется внутренний контроль:

12.1.1. использования технических средств, ПО, работы в сети Интернет в структурных подразделениях Администрации по поручению руководителей структурных подразделений Администрации.

12.1.2. обработки персональных данных в Администрации в соответствии с нормативными правовыми актами Администрации регламентирующими осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленных Федеральным законом «О персональных данных».

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 роспись в листе ознакомления (прохождения обучения) либо журнале ознакомления (прохождения обучения) с указанием фамилии, имени, отчества служащего и даты ознакомления (прохождения обучения) (П.).

Обязанность по организации ознакомления служащих с настоящей Политикой ИБ возлагается на руководителей структурных подразделений Администрации. Обязанность по обучению пользованию средствами антивирусного ПО возлагается на системных администраторов.

РАЗДЕЛ XIII.
ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЯ НАСТОЯЩЕЙ ПОЛИТИКИ ИБ

12.1. 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.

12.2. При обнаружении нарушения служащими настоящей Политики ИБ системный администратор устанавливает причины возникновения нарушения и направляет служебную записку о выявленном нарушении руководителю структурного подразделения Администрации.

Руководитель структурного подразделения Администрации принимает решение о необходимости привлечения служащего к ответственности.

Системный администратор ведет учет всех выявленных случаев нарушения безопасности информации.