Приложение № 7
к Приказу от 4 сентября 2023 г. № 12-од

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Настоящая Политика информационной безопасности (далее – Политика) муниципального бюджетного учреждения городского округа «Город Калининград» «Газета «Гражданин» (далее – Учреждение) разработана в соответствии с правилами, требованиями и принципами обеспечения информационной безопасности и является официальным документом.

Политика разработана в соответствии с требованиями:

– Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи»;

– Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

– Федерального закона от 14 июля 2022 г. № 266-ФЗ «О внесении изменений в Федеральный закон «О персональных данных», отдельные законодательные акты Российской федерации и признании утратившей силу части четырнадцатой статьи 30 Федерального закона «О банках и банковской деятельности»;

– Постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– приказа ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– Гражданского кодекса Российской Федерации;

– Устава муниципального бюджетного учреждения городского округа «Город Калининград» «Газета «Гражданин», утвержденного распоряжением администрации городского округа «Город Калининград» от 11 апреля 2023 г. № 73-р.

В Политике определены требования к работникам Учреждения, допущенным для работы с информацией в информационных системах (далее – ИС) Учреждения, степень ответственности таких работников, структура и необходимый уровень защищенности таких ИС, статус и обязанности работников, ответственных за обеспечение безопасности ИС Учреждения.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Под информационной безопасностью понимается состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность, целостность и доступность информации при ее обработке техническими средствами.

1.2. Политика информационной безопасности утверждается директором (главным редактором) Учреждения.

1.3. Требования настоящей Политики распространяются на всех работников Учреждения, а также иных лиц, взаимодействующих с Учреждением.

1.4. Актуализация настоящей политики проводится на регулярной основе не реже одного раза в год.

2. ЦЕЛИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1. Целями настоящей Политики являются:

а) обеспечение защиты информационных ресурсов Учреждения от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, её носители, процессы обработки и передачи данных;

б) минимизация ущерба от возможной реализации угроз информационной безопасности (далее – УИБ).

2.2. Безопасность информации, обрабатываемой в Учреждении, достигается путем исключения несанкционированного, в том числе случайного доступа к ней, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение информации, а также иных несанкционированных действий.

2.3. Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей Учреждения (работников, допущенных для выполнения своих должностных обязанностей в информационных системах).

2.4. В Учреждении осуществляется своевременное обнаружение и реагирование на УИБ и предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

2.5. Состав объектов защиты, перечень защищаемой информации, обрабатываемой в ИС Учреждения и подлежащей защите, утверждаются приказами директора (главного редактора) Учреждения.

3. ЗАДАЧИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1. Для достижения основных целей политики информационной безопасности Учреждения необходимо обеспечить эффективное решение следующих задач:

– своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности;

– создание механизма оперативного реагирования на угрозы информационной безопасности;

– соответствие процессов защиты информации требованиям Федерального законодательства, нормативно-методическим документам ФСБ России, ФСТЭК России;

– достижение адекватности мер по защите от угроз информационной безопасности;

– выявление, предупреждение и пресечение возможной противоправной и иной негативной деятельности работников Учреждения.

4. ОТВЕТСТВЕННОСТЬ ЗА ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1. Общее руководство обеспечением информационной безопасности осуществляет ответственный за организацию обработки персональных данных и выполнение мероприятий по обеспечению безопасности персональных данных в Учреждении далее – Ответственный).

4.2. Ответственность за организацию мероприятий по обеспечению информационной безопасности Учреждения и за соблюдение требований информационной безопасности несет Ответственный.

4.3. Ответственность за проведение технических мероприятий по обеспечению безопасности информации несет администратор информационной безопасности (далее – Администратор ИБ).

4.4. Ответственность за функционирование информационных систем Учреждения лежит на администраторе информационных систем.

4.5. Ответственные за информационную безопасность утверждаются приказами директора (главного редактора) Учреждения.

4.6. На работников, осуществляющих функции обеспечения информационной безопасности, возлагается решение следующих основных задач:

– определение требований к системе защиты информации;

– организация мероприятий по вопросам комплексной защиты информации Учреждения;

– контроль и оценка эффективности принятых мер и применяемых средств защиты информации;

– оказание методической помощи работникам Учреждения в вопросах обеспечения информационной безопасности;

– выбор и внедрение средств защиты информации, а также применение организационных мер в области информационной безопасности;

– информирование, обучение и повышение квалификации работников Учреждения в сфере информационной безопасности;

– расследование инцидентов информационной безопасности и взаимодействие с государственными контролирующими органами в области информационной безопасности.

Работники Учреждения, осуществляющие функции обеспечения информационной безопасности имеют следующие права:

– определять необходимость и разрабатывать нормативные документы, касающиеся вопросов обеспечения безопасности информации, включая документы, регламентирующие деятельность пользователей информационных систем Учреждения;

– получать информацию от пользователей информационных систем Учреждения по любым вопросам применения информационных технологий;

– участвовать в разработке технических решений по вопросам безопасности информации при проектировании и разработке новых информационных систем Учреждения;

– участвовать в испытаниях разработанных информационных систем по вопросам оценки качества реализации требований по обеспечению безопасности информации;

– контролировать деятельность пользователей информационных систем Учреждения по вопросам обеспечения информационной безопасности;

– подготавливать предложения руководству Учреждения по обеспечению требований информационной безопасности.

5. ИНФОРМАЦИОННЫЕ РЕСУРСЫ УЧРЕЖДЕНИЯ

5.1. В Учреждении выявлены и оценены все информационные системы, подлежащие защите информации в них.

5.2. Информационные системы Учреждения представлены информационными системами персональных данных (далее – ИСПДн) включающими в себя технические и программные средства обработки персональных данных (далее – ПДн), средства передачи и отображения информации, в том числе каналы информационного обмена и коммуникации, а также помещения, в которых размещены данные информационные системы.

6. СИСТЕМА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Система защиты персональных данных (далее – СЗПДн) Учреждения строится на основании:

– перечня персональных данных, подлежащих защите;

– актов обследования по результатам обследования информационных систем обработки персональных данных;

– актов определения уровня защищенности персональных данных при их обработке в информационных системах персональных данных;

– моделей угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

– локальных актов (приказов) Учреждения;

– организационно-распорядительной документации, относящейся к системе защиты информации и персональных данных Учреждения;

– руководящих и нормативных документов Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзора);

– руководящих документов ФСТЭК и ФСБ России.

На основании указанных документов определяется необходимый уровень защищенности ПДн каждой ИСПДн Учреждения.

На основании анализа актуальных угроз безопасности ПДн, описанных в модели угроз безопасности персональных данных делается заключение о необходимости использования технических средств защиты информации и проведения организационных мероприятий для обеспечения безопасности ПДн Учреждения.

6.2. При проведении работ по информационной безопасности в актах обследования информационных систем составляется перечень используемых технических и аппаратных средств, а также программного обеспечения, участвующего в обработке ПДн. Перечень всех элементов ИСПДн, включает в себя:

а) перечень основных технических средств и систем (далее – ОТСС);

б) перечень программного обеспечения, используемого в ИСПДн;

в) перечень каналов передачи данных, если по ним передаются ПДн.

В зависимости от уровня защищенности ИСПДн и актуальных угроз в СЗПДн включают следующие технические средства защиты информации (далее – ТСЗИ):

а) антивирусные средства для рабочих мест пользователей и серверов;

б) средства защиты информации от несанкционированного доступа;

в) средства межсетевого экранирования;

г) средства криптографической защиты информации, используемые при передаче защищаемой информации по открытым каналам связи (далее – СКЗИ).

Технические средства защиты информации, используемые в СЗПДн, должны обеспечивать следующие функции защиты информации:

а) управление и разграничение доступа пользователей;

б) регистрацию и учет действий с информацией;

в) целостность баз персональных данных;

г) обнаружение вторжений.

СЗПДн Учреждения должна включать в себя следующие подсистемы:

а) управления доступом, регистрацией и учетом;

б) обеспечения целостности и доступности;

в) антивирусной защиты;

г) криптографической защиты;

д) межсетевого экранирования;

е) анализа защищенности;

ж) обнаружения вторжений.

6.3. Подсистемы СЗПДн имеют различный функционал в зависимости от определенных уровней защищенности ИСПДн, определенных в актах определения уровня защищенности персональных данных при их обработке в информационных системах персональных данных Учреждения. Перечень используемых в Учреждении подсистем СЗПДн, и требований к ним, устанавливается в техническом задании на создание системы защиты информации информационных систем Учреждения.

7. ПОЛЬЗОВАТЕЛИ ИСПДн

7.1. Пользователи информационных систем обработки персональных данных (далее – ИСПДн) – работники Учреждения, осуществляющие обработку персональных данных.

7.2. Перечень пользователей, допущенных до работы с персональными данными (далее – ПДн), уровень их доступа и информированности утверждаются директором (главным редактором) Учреждения.

7.3. Пользователи имеют доступ к обработке ПДн, которая включает в себя: возможность просмотра ПДн, ручной ввод ПДн в ИСПДн, формирование справок и отчетов по информации, полученной из ИСПДн.

7.4. Пользователи не имеют полномочий для управления подсистемами обработки данных и СЗПДн.

7.5. Каждому пользователю ИСПДн, участвующему в обработке ПДн, присваивается уникальное имя (учетная запись пользователя), а также создается индивидуальный пароль.

7.6. Первоначальное значение пароля учетной записи пользователя устанавливает Администратор ИБ. В дальнейшем пароль к учетной записи пользователя должен меняться не реже одного раза в 60 дней.

7.7. Требования к выбору паролей

– длина пароля должна быть не менее 8 символов;

– в числе символов пароля должны присутствовать три из четырёх видов символов:

- буквы в верхнем регистре;
- буквы в нижнем регистре;
- цифры;
- специальные символы (! @ # $ % ^ & * ( ) - _ + = ~ [ ] { } | \ : ; ' " < > , . ? /);

– пароль не должен содержать легко вычисляемые сочетания символов, например,

- имена, фамилии, номера телефонов, даты;
- последовательно расположенные на клавиатуре символы («12345678», «QWERTY», и т.д.);
- общепринятые сокращения («USER», «TEST» и т.п.);
- повседневно используемые слова, например, имена или фамилии друзей, коллег, актёров или сказочных персонажей, клички животных;
- компьютерные термины, команды, названия организаций, web-сайтов, аппаратного или программного обеспечения;
- что-либо из вышеперечисленного в обратном написании;
- что-либо из вышеперечисленного с добавлением цифр в начале или конце;

– при смене пароля значение нового должно отличаться от предыдущего не менее чем в 4 позициях;

– для разных ИСПДн необходимо устанавливать собственные, отличающиеся пароли.

Вход в систему не должен выполняться автоматически. Покидая рабочее место, пользователь обязан заблокировать компьютер (используя комбинации Win+ «L» или Ctrl+Alt+Delete-«Блокировка компьютера»).

7.8. При работе с корпоративной системой электронной почты пользователям ИСПДн рекомендуется:

– перед началом работы удостовериться в том, что установленное на рабочем месте прикладное программное обеспечение, пакеты офисных приложений, средства антивирусной защиты, обновлены до актуальных версий;

– при работе исключить либо ограничить посещение ресурсов в сети Интернет, непосредственно не задействованных в исполнении служебных обязанностей;

– при получении либо обработке электронной корреспонденции удостовериться в ее получении от доверенного (известного) отправителя, исключить переход по URL-ссылкам и запуск вложений, если письмо получено из неизвестного источника.

– включить отображение расширения файлов в настройках операционной системы с целью предотвращения запуска вложений с подмененной пиктограммой;

– при получении электронной корреспонденции от имени службы поддержки с просьбой перейти по URL-ссылке, проверить данную информацию, связавшись с системным администратором;

– при запуске вложений с электронными документами (форматы doc, docx, xls, xlsx, и т.д.) не давать используемому офисному приложению разрешения на использование макросов;

– при получении электронного письма внимательно проверять электронный адрес отправителя на предмет его корректности. Исключить запуск вложений и переход по ссылкам, если адрес отправителя не соответствует заведомо известному, содержит ошибки в символах, опечатки, либо неверные доменные имена;

– исключить долговременное хранение важной информации в папке с отправленной электронной корреспонденцией, регулярно производить очистку данного раздела.

– по возможности защищать пересылаемые файлы путем их архивирования с добавлением пароля. Пароль для разархивирования файлов передавать получателю по иным каналам.

7.9. Проверка электронной почты и сетевых ресурсов Учреждения осуществляется антивирусным программным обеспечением на регулярной основе.

При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программного обеспечения, появление графических/звуковых эффектов, искажение данных, пропадание файлов, частого появления сообщений о системных ошибках и т.п.) пользователь должен известить Администратора ИБ. Администратор ИБ должен провести внеочередную полную проверку на вирусы рабочей станции пользователя, проверив, в первую очередь, работоспособность антивирусного программного обеспечения.

7.10. Для предупреждения антивирусного заражения рекомендуется:

– никогда не открывать файлы и не переходить по ссылкам, полученным в почтовых сообщениях от неизвестного или подозрительного отправителя;

– удалять подозрительные вложения, не открывая их, и очищать папки временного хранения, где содержатся удаленные сообщения;

– удалять спам, рекламу и другие бесполезные сообщения;

– не загружать файлы и программное обеспечение из подозрительных или неизвестных источников;

– периодически проводить резервное копирование важных данных и системной конфигурации, хранить резервные копии в безопасном месте.

8. ТРЕБОВАНИЯ К РАБОТНИКАМ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ПДн

8.1. Все работники Учреждения, являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдать принятый режим безопасности ПДн, а также быть ознакомленными с руководящими документами по информационной безопасности Учреждения.

8.2. При вступлении в должность нового работника, ответственный за организацию обработки персональных данных и выполнение мероприятий по обеспечению безопасности персональных данных Учреждения (далее – Ответственный) знакомит указанного работника с необходимыми документами, регламентирующими требования по защите ПДн, а также обучает его правилам работы с ПДн в ИСПДн.

8.3. Работники Учреждения под роспись знакомятся с должностными инструкциями, организационно-распорядительной документацией, относящейся к системе защиты ПДн Учреждения, настоящей Политикой, принятыми процедурами работы с элементами ИСПДн и СЗПДн, а также с Положением об обработке и защите персональных данных Учреждения.

8.4. Работники Учреждения, использующие технические средства аутентификации, в обязательном порядке обеспечивают сохранность идентификаторов (электронных ключей)
и не допускают несанкционированного доступа (далее – НСД) к ним, исключают возможность их утери и вероятность использования третьими лицами.

8.5. Работники Учреждения проинструктированы о необходимости следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

8.6. Работники Учреждения ознакомлены с правилами обеспечения надлежащей защиты оборудования ИСПДн, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица.

8.7. Работники Учреждения как пользователи ознакомлены с требованиями по безопасности ПДн и процедурами защиты оборудования ИСПДн, оставленного без присмотра, а также знают свои обязанности по обеспечению такой защиты.

8.8. Работники Учреждения ознакомлены с требованиями обеспечения отсутствия возможности просмотра ПДн третьими лицами с мониторов автоматизированных рабочих мест (далее – АРМ) или терминалов при работе с ПДн.

8.9. Работники Учреждения проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение.

8.10. Работники Учреждения ознакомлены с дисциплинарными взысканиями при нарушении требований безопасности работы с ПДн в соответствии с действующим федеральным законодательством Российской Федерации в области защиты информации и персональных данных.

8.11. Контроль по соблюдению режима безопасности обработки ПДн возложен на Ответственного в соответствии с приказом директора (главного редактора) Учреждения.

8.12. Работники Учреждения, допущенные к работам с техническими и криптографическими средствами защиты информации, проходят обучение по правилам работы, хранения и учета технических и криптографических средств защиты информации. Обучение проводит Администратор ИБ.

8.13. Допуск работников Учреждения к работе со средствами криптографической защиты информации происходит на основании приказа директора (главного редактора) Учреждения.

8.14. Работники Учреждения под роспись знакомятся с инструкциями, правилами, руководствами, принятыми процедурами работы с установленными средствами криптографической защиты информации.

8.15. Работники Учреждения, использующие средства криптографической защиты информации, в обязательном порядке обеспечивают их сохранность и не допускают НСД к ним, исключают возможность их утери и вероятность использования третьими лицами.

8.16. Работники Учреждения обязаны без промедления сообщать Администратору ИБ и Ответственному обо всех случаях работы в ИСПДн, которые могут повлечь за собой угрозу безопасности ПДн.

8.17. Работникам Учреждения ЗАПРЕЩАЕТСЯ:

а) устанавливать стороннее программное обеспечение;

б) подключать личные мобильные устройства и носители информации, а также записывать на них защищаемую информацию;

в) разглашать защищаемую информацию, которая стала им известна при работе в ИСПДн Учреждения, третьим лицам.

9. ДОЛЖНОСТНЫЕ ОБЯЗАННОСТИ РАБОТНИКОВ (ПОЛЬЗОВАТЕЛЕЙ ИСПДн)

9.1. Должностные обязанности пользователей ИСПДн Учреждения описаны в следующих организационно-распорядительных документах:

– руководстве ответственного за организацию обработки персональных данных и выполнение мероприятий по обеспечению безопасности персональных данных;

– руководстве администратора информационной безопасности;

– руководстве пользователя;

– инструкции по организации режима доступа в помещения, о порядке действий при несанкционированном проникновении в помещения и других нештатных ситуациях;

– Положении об обработке и защите персональных данных Учреждения;

– должностных инструкциях работников Учреждения.

10. ОТВЕТСТВЕННОСТЬ РАБОТНИКОВ, ОБРАБАТЫВАЮЩИХ ПДн В ИСПДн

10.1. Директор (главный редактор) Учреждения назначает ответственного за организацию обработки персональных данных и выполнение мероприятий по обеспечению безопасности персональных данных.

10.2. Ответственный получает указания непосредственно от директора (главного редактора) Учреждения и подотчетен ему.

10.3. Ответственный обязан:

а) осуществлять внутренний контроль за соблюдением работниками Учреждения законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

б) доводить до сведения работников Учреждения положения законодательства Российской Федерации о персональных данных, локальные акты по вопросам обработки персональных данных (приказы, руководства, инструкции), требования к защите персональных данных;

в) организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

10.4. Работники Учреждения ознакомлены с тем, что:

– моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, а также требований к защите персональных данных, подлежит возмещению в соответствии с законодательством Российской Федерации;

– возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков;

– лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом Российской Федерации и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

10.5. Для решения вопросов по расследованию инцидентов информационной безопасности, возникших при обработке ПДн и другой конфиденциальной информации, уничтожения документов, содержащих персональные данные, в Учреждении создается комиссия.

10.6. Состав комиссии утверждается приказом директора (главного редактора) Учреждения.

10.7. В состав комиссии включается Ответственный и Администратор ИБ.

10.8. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных, изложена в:

а) Кодексе об административных правонарушениях Российской Федерации (КоАП РФ) – статьи 5.27, 5.39, 13.11-13.14, 19.4-19.7, 19.20, 20.25, 32.2;

б) Уголовном кодексе Российской Федерации (УК РФ) – статьи 137, 140, 155, 183, 272, 273, 274, 292, 293;

в) Трудовом кодексе Российской Федерации (ТК РФ) – статьи 81, 90, 195, 237, 391.

11. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

11.1. Все работники Учреждения обязаны ознакомиться с настоящей Политикой.

11.2. Обязанность ознакомления работников Учреждения с настоящей Политикой лежит на ответственном за организацию обработки персональных данных и выполнение мероприятий по обеспечению безопасности персональных данных в муниципальном бюджетном учреждении городского округа «Город Калининград» «Газета «Гражданин».