ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Муниципальное казенное учреждение "Центр информационных технологий" городского округа город Уфа Республики Башкортостан

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Политика информационной безопасности (далее – Политика ИБ) Муниципального казенного учреждения "Центр информационных технологий" городского округа город Уфа Республики Башкортостан (далее – учреждение) определяет требования к сотрудникам учреждения по обеспечению информационной безопасности при работе с автоматизированным рабочем местом, информационными системами, информационными ресурсами и сервисами предоставляемыми посредством сети Администрации городского округа г. Уфа Республики Башкортостан (далее – сеть Администрации), а также описывают необходимые действия сотрудников по их соблюдению.

1.2. Цель и задачи

Целью настоящей Политики информационной безопасности является установление единых принципов и требований по обеспечению защиты информации в учреждении от внутренних и внешних угроз, а также определение организационных и технических мер по предотвращению несанкционированного доступа, разрушения, изменения, блокирования и других неправомерных действий в отношении информации.

Задачи по обеспечению информационной безопасности реализуются в рамках деятельности уполномоченных структурных подразделений и включают:
– внедрение технических и программных средств защиты информации;
– контроль соблюдения требований законодательства РФ в области ИБ;
– разработку и сопровождение внутренних нормативных документов по ИБ;
– обучение сотрудников вопросам защиты информации;
– выявление и реагирование на инциденты информационной безопасности.

1.3. Описание системы защиты

В целях реализации задач, определённых настоящей Политикой, в систему защиты входят следующие меры и средства защиты информации:

– организационно-распорядительная документация, регламентирующая обеспечение защиты информации;

– повышение осведомленности работников в области информационной безопасности и условиям работы с защищаемой информацией;

– разграничение прав доступа;

– средство антивирусной защиты;

– средства межсетевого экранирования;

– средства резервного копирования;

– применение средства криптографической защиты информации (далее - СКЗИ) и использование электронная подпись (далее – ЭП).

1.6. Порядок резервирования.

В учреждении осуществляется резервное копирование персональных данных, в целях обеспечения сохранности и восстановления данных при сбоях, повреждении или утрате.

Резервные копии создаются по утверждённому графику, хранятся на защищённых носителях с ограниченным доступом, защищаются от несанкционированного доступа, а также регулярно проверяются на целостность.

1.7. Порядок уничтожения информации в ИС, на машинных носителях информации.

Уничтожение информации осуществляется программным или физическим методом, исключающим возможность её восстановления. Выбор способа определяется типом носителя и уровнем конфиденциальности данных. Факт уничтожения оформляется соответствующим актом

1.8. Порядок обращения со средствами криптографической защиты информации.

Использование средств криптографической защиты информации (СКЗИ), включая электронную подпись, осуществляется в учреждении в соответствии с требованиями законодательства РФ, в том числе нормативных актов ФСБ России.

Применяются только сертифицированные СКЗИ, внесённые в реестр ФСБ. Учёт, установка, эксплуатация и уничтожение СКЗИ и ключевой информации осуществляются в соответствии с внутренними регламентами и с обязательным оформлением сопроводительной документации.

1.9. В учреждении применяются средства межсетевого экранирования для защиты сети от несанкционированного доступа и предотвращения угроз безопасности информации. Они обеспечивают фильтрацию трафика, контроль доступа и защищенное взаимодействия между внутренними и внешними ресурсами.

1.10. Применяется сертифицированное средство антивирусной защиты, внесённые в реестр ФСТЭК России, соответствующее требованиям безопасности и обеспечивающее защиту от вредоносного программного обеспечения.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Информационный ресурс	– любое системное или прикладное программное обеспечение, физические и виртуальные хранилища данных в электронном виде, средства чтения и записи электронных носителей информации.
Мобильное устройство	– любое легко перемещаемое вычислительное устройство, предназначенное и используемое для создания, получения, хранения, обработки и передачи информации. К ним относятся ноутбуки (в том числе планшетные портативные компьютеры), карманные портативные компьютеры (КПК), смартфоны, компьютерные записные книжки, сотовые телефоны
Конфиденциальная информация	— информация, доступ к которой ограничен в соответствии с законодательством, внутренними нормативными документами учреждения или договорными обязательствами. К конфиденциальной информации относятся сведения, не подлежащие разглашению третьим лицам, а также информация, разглашение, утрата или несанкционированный доступ к которой может нанести ущерб учреждению, её сотрудникам, контрагентам.
Администратор информационной безопасности (АИБ)	– сотрудники учреждения (сотрудники отдела информационной безопасности), назначенные ответственными за обеспечение информационной безопасности, техническое взаимодействие и участие в определении и нейтрализации последствий инцидентов информационной безопасности.
Носитель информации	– материальный предмет, на котором (или в котором) возможно разместить информацию в виде символов, образов, файлов и пр.
Съемный носитель информации	– электронный носитель информации, подключаемый к средствам компьютерной техники и используемый для хранения информации. К съемным носителям информации относятся дискеты, оптические (CD, DVD) диски, USB-носители, энергонезависимые карты памяти, фотоаппараты и т.п
Съемный носитель ключевой информации (ключевой носитель)	– электронный носитель информации, на котором содержатся криптографические ключи для шифрования и электронной подписи документов. К съемным носителям ключевой информации относятся Touch Memory («таблетка»), RuToken/eToken (в виде USB-носителя), гибкий магнитный диск (дискета) и пр.
Устройство ввода вывода информации	– выполненные как во внутреннем, так и во внешнем исполнении дисководы, приводы чтения и записи CD и DVD

	дисков, USB-порты и прочие переносные устройства, которые могут использоваться для выгрузки или загрузки информации в компьютер. Устройства вводавывода также являются информационными ресурсами.

3. НОРМАТИВНЫЕ ССЫЛКИ

3.1. В своей деятельности сотрудники учреждения, в том числе АИБ, должны руководствоваться нормативными правовыми актами в области защиты информации, включая:

3.1.1. Федеральный закон от 27 июля 2006 г. №152-ФЗ «О персональных данных»;

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

3.1.3. Приказ ФСТЭК России от 11 февраля 2013 г. №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

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

3.1.5. Методический документ ФСТЭК России от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах»;

3.1.6. Приказ ФСБ России от 10 июля 2014 г. №378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

3.1.7. Приказ ФАПСИ от 13 июня 2001 г. №152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

4. РАБОТА С ИНФОРМАЦИЕЙ ОГРАНИЧЕННОГО ДОСТУПА

4.1. Доступ к информации ограниченного доступа и ее передача.

4.1.1. Сотрудники учреждения обязаны не разглашать информацию ограниченного доступа в течение всего времени работы в учреждении, а также соблюдать требования законодательства Российской Федерации и внутренних нормативных документов учреждения, полученную в рамках осуществления функциональных полномочий лицам, не имеющим прав на доступ к данной информации.

Сотрудники несут ответственность за несанкционированное разглашение им информации ограниченного доступа в соответствии с действующим законодательством Российской Федерации.

4.1.2. Разовое (единовременное) предоставление доступа к конфиденциальной информации либо ознакомление с ней сотрудников, характер должностных обязанностей которых не связан с ее получением, использованием или обработкой, допускается только по согласованию с руководителем учреждения, имеющего право предоставления доступа к данной информации.

4.1.3. Предоставление постоянного (на постоянной основе) доступа к сетевым информационным ресурсам (Directum 5.0, Directum RX, 1С, Bitrix24, Рубины и т.д.) осуществляется в соответствии с разделом 6 настоящей Политики ИБ.

4.1.4. Передача документов на любых носителях, содержащих информацию ограниченного доступа, третьим лицам (клиентам, контрагентам и др.) без согласования с

руководителем учреждения и АИБ запрещена. При передаче необходимо удостовериться, что с получателем заключено Соглашение о неразглашении и защите конфиденциальной информации. 4.1.5. Не допускается работать с конфиденциальной информацией в случае возможности её просмотра посторонними лицами. Лица, не являющиеся сотрудниками учреждения, не должны видеть конфиденциальную информацию на экране компьютера. При необходимости сотрудникам следует закрыть или свернуть все окна с конфиденциальной информацией или заблокировать компьютер. Бумажные конфиденциальные документы следует перевернуть текстом вниз или убрать со стола.

4.1.6. Копирование, фотографирование или производить выписки из документов, содержащих конфиденциальную информацию, на любых носителях не допускается. Для выполнения этих действий необходимо получить письменное разрешение руководителя учреждения и разрешение АИБ.

5. РАБОТА С ПЕРСОНАЛЬНЫМ КОМПЬЮТЕРОМ

5.1. Сотруднику запрещается вскрывать персональный компьютер, используемый для работы (далее — компьютер), в том числе для самостоятельного устранения неисправностей, а также подключать к компьютеру любое оборудование, не связанное непосредственно с его должностными обязанностями (модемы, личные устройства и т.д.).

5.2. При отсутствии сотрудника на рабочем месте, даже на короткий период времени (более 1 минуты) сотрудник обязан блокировать доступ к компьютеру.

5.3. По окончанию рабочего дня сотрудник должен выключать компьютер, за исключением случаев, когда по объективным причинам, связанным с выполнением должностных обязанностей, необходимо оставить компьютер включенным.

5.4. Сотруднику запрещается самостоятельно изменять программную и аппаратную конфигурации компьютера. Список стандартного программного обеспечения и условия его установки для каждой категории сотрудников определяются иными нормативными и распорядительными документами учреждения. Сотрудник может запросить разрешение на установку необходимого дополнительного ПО в виде служебной записки на имя руководителя учреждения.

5.5. Сотруднику запрещается отключать и/или удалять установленные средства защиты (в том числе антивирусное программное обеспечение), а также изменять настройки данных устройств.

5.6. Выполнение операций в информационных ресурсах, последствия которых сотруднику неизвестны из-за отсутствия знаний по работе с данным ресурсом, использование компьютера для мошенничества и других видов противоправной деятельности, а также применение средств для несанкционированного доступа к ресурсам учреждения запрещаются

5.7. Самостоятельно осуществлять подключение, отключение, переключение и перенастройку сетевых элементов компьютера запрещается (подключение каких-либо сетевых карт, подключение компьютера в другую сетевую розетку и т.д.). Ответственность за соблюдение этого правила возлагается на начальников отделов, в случае если рабочее место сотрудника находится в другом структурном подразделении Администрации это возлагается на самого сотрудника, в обязанности которого и так входит перенастройка компьютеров.

6. ДОСТУП К ИНФОРМАЦИОННЫМ РЕСУРСАМ

6.1. Доступ к информационным ресурсам предоставляется сотрудникам только на основании служебной записки.

6.2. До начала работы в вычислительной сети учреждения сотрудник обязан ознакомиться с настоящей Политикой ИБ.

6.3. Сотрудник обязан периодически производить смену используемых им паролей, смену пароля нужно осуществлять не реже чем 1 раз в 90 дней.

6.4. При создании пароля сотрудник должен выбирать сложные пароли, состоящие не менее чем из 8 символов и обязательно содержащие как буквы, так и цифры, а по возможности — специальные знаки (!»№;%:?*()_ и т.п.). Пароль не должен быть очевидным, то есть не должен содержаться в каком-либо словаре. Не следует использовать в качестве пароля свою фамилию, даты рождения, имена детей, номера своих телефонов, паспортов и других документов и т.п., а также любые общеизвестные и/или легко угадываемые сокращения. Запрещается использовать в качестве пароля имя пользователя (идентификатор доступа).

6.5. Сотрудникам запрещается использовать в служебных целях пароли, ранее применявшиеся для доступа к личным устройствам, почтовым сервисам, интернет-ресурсам и иным информационным системам, не связанным с профессиональной деятельностью. Также не допускается указание служебных логинов и паролей при регистрации на сторонних интернет-ресурсах, не имеющих прямого отношения к исполнению должностных обязанностей, в том числе на ресурсах, предусматривающих открытый доступ к указанной информации для третьих лиц (например, форумы, социальные сети, интернет-магазины и иные подобные площадки).

6.6. Запрещается записывать пароли в местах, доступных для визуального просмотра, а также хранить их в открытом виде на электронных носителях, за исключением ключевых носителей, к которым предъявляются отдельные требования (подробности приведены в разделе 8.3 настоящей Политики ИБ).

6.7. Сотрудникам запрещается передавать кому-либо свои логины и пароли кому-либо, включая администраторов и непосредственного руководителя. для доступа к любому информационному ресурсу. Исключение составляют случаи, когда отсутствие сотрудника на рабочем месте (например, при болезни, вынужденном отсутствии и т.п.) может привести к приостановке работы учреждения. В этом случае, возможен сброс пароля. После выхода на работу сотрудник обязан сменить пароль, который был использован другим сотрудником, при доступе к информационным ресурсам.

6.8. Запрещается осуществлять доступ к информационным ресурсам с использованием чужого логина и пароля (за исключением случаев, описанных в п. 6.7 настоящей Политики ИБ). Для доступа к информационным ресурсам сотруднику следует использовать только персональный (собственный) идентификатор доступа и пароль. В случаях, когда технологически предусмотрено использование общих для нескольких сотрудников логина и пароля, использование единого идентификатора возможно при обязательном согласовании с администратором информационного ресурса. В этом случае руководитель учреждения является ответственным за контроль использования общего идентификатора доступа. Использовать несколькими сотрудниками одних и тех же персональных идентификаторов доступа в один промежуток времени запрещается.

6.9. Сотрудники, у которых доступ к информационным ресурсам осуществляется через электронную цифровую подпись, не должны оставлять электронный ключ, подключенным к компьютеру, в случае их отсутствия на рабочем месте.

6.10. В случае увольнения сотрудника или изменения его должностных обязанностей непосредственный руководитель такого сотрудника обязан обратиться к руководителю учреждения с просьбой дать указание Администратору информационных систем на отключение (изменение) прав доступа такого сотрудника.

7. РАБОТА С СЕТЬЮ ИНТЕРНЕТ

7.1. Доступ сотрудников к сети Интернет предоставляется только в связи с необходимостью осуществления ими своих непосредственных должностных обязанностей.

7.2. Сотрудникам учреждения запрещается посещать сайты, не связанные с выполнением должностных обязанностей, включая социальные сети, развлекательные ресурсы, форумы и другие сайты, не имеющие отношения к работе. Внешние интернет-ресурсы не должны использоваться для передачи служебной информации и документов или

для личной переписки. Для работы с конфиденциальной информацией следует использовать только сайты и сервисы, которые поддерживают защищённое соединение, такие как SSL и TLS, также необходимо применить госшифрование.

7.3. С целью недопущения заражения локальной вычислительной сети учреждения компьютерными вирусами, сотрудникам запрещается самостоятельно загружать из сети Интернет какое-либо программное обеспечение и исполняемые файлы (.exe, .scr, .js, .jse и т.д.).

8. РАБОТА С УСТРОЙСТВАМИ ВВОДА-ВЫВОДА И СЪЕМНЫМИ НОСИТЕЛЯМИ ИНФОРМАЦИИ

8.1. Устройства ввода-вывода

8.1.1. Устройства ввода-вывода, имеющие функции записи информации на носители, устанавливаются (подключаются) на рабочие компьютеры сотрудников учреждения только в исключительных случаях, когда это необходимо для выполнения их должностных обязанностей. Для установки и подключения таких устройств требуется оформить служебную записку непосредственному руководителю, в которой должно быть подробно обосновано, почему этот доступ необходим.

8.1.2. Сотрудник, имеющий подключенное устройство ввода-вывода с функциями записи, несет персональную ответственность за его использование только для целей, указанных в служебной записке.

8.2. Съемные носители информации.

8.2.1. Подключение съемных носителей должно осуществляться только для непосредственной работы с ними. В случае отсутствия сотрудника на рабочем месте, все съемные носители информации должны быть извлечены и/или отсоединены сотрудником от компьютера. Оставлять указанные носители в не присоединённом/неподключенном состоянии в местах открытого доступа и на столах без присмотра запрещено. Сотрудник должен убирать съемные носители в закрываемое на ключ место хранения или забирать с собой.

8.2.2. Сотрудники, которые используют съёмные носители информации, должны предъявлять их по требованию АИБ для проверки. Если носитель больше не используется, подлежит ремонту или сдаче, нужно обратиться в АИБ, чтобы удалить с него всю информацию. При увольнении или изменении должностных обязанностей, не связанных с работой с носителями, сотрудник должен сдать их ответственному сотруднику.

8.2.3. Самостоятельное приобретение съемного носителя для служебных целей возможно только с разрешения непосредственного руководителя. Сотрудник обязан зарегистрировать приобретенный носитель у АИБ перед его использованием. Использование незарегистрированных носителей информации запрещено.

8.2.4. Сотруднику запрещается передавать используемые съемные носители информации посторонним лицам или другим сотрудникам учреждения без согласования непосредственного руководителя такого сотрудника.

8.3. Съемные носители ключевой информации

8.3.1. Все съемные носители ключевой информации (далее - ключевые носители) сотрудник должен хранить в сейфе, запираемом на ключ шкафе, либо ином недоступном для посторонних лиц месте.

8.3.2. За каждым ключевым носителем приказом по учреждению должен быть закреплен ответственный сотрудник. В случае необходимости выдачи ключевого носителя другим сотрудникам, ответственный сотрудник обязан согласовать передачу и/или списки сотрудников, имеющих право использовать данный ключевой носитель, с АИБ. За каждым ключевым н

8.3.3. Сотруднику запрещается сообщать кому-либо пароли доступа (если таковые имеются) к используемым ключевым носителям, а также использовать записанный на ключевом носителе ключ для подписи каких-либо электронных документов (файлов) кроме

тех, которые предусмотрены технологическим процессом в указанной системе документооборота

8.3.4. В случае компрометации криптографического ключа, т.е. обоснованного подозрения, что используемый ключ стал доступен постороннему лицу, пользователь обязан прекратить применение ключевого носителя, немедленно сообщить о факте компрометации (возможной компрометации) отделу информационной безопасности и непосредственному руководителю и действовать по их указанию.

8.3.5. Сотруднику запрещается хранить электронную цифровую подпись в реестре, на других съемных носителях, в памяти компьютера и т.д., только на съемном носителе ключевой информации.

8.3.6. При работе с ключевыми носителями должны, в том числе, соблюдаться требования, указанные в разделе 8.2 настоящей Политики ИБ.

9. РАБОТА С МОБИЛЬНЫМИ УСТРОЙСТВАМИ

9.1. Общие правила работы с мобильными устройствами

9.1.1. Сотрудникам запрещается подключать личные/не рабочие мобильные устройства к локальной сети и использовать их для работы с информацией ограниченного доступа.

9.1.2. Личные/не рабочие смартфоны и мобильные телефоны запрещаются использовать для работы с конфиденциальной информацией, за исключением рабочих устройств с установленными средствами защиты информации.

9.1.3. Запрещается включать порты мобильных устройств, работающие на основе технологий беспроводной связи (IrDA, Wi-Fi, Bluetooth, WiMAX), а также подключать мобильные устройства к сетям сторонних организаций и сетям общего пользования, включая Интернет. Запрещается оставлять карманные портативные компьютеры, сотовые телефоны и другие мобильные устройства на столах или в местах открытого доступа без присмотра.

9.1.4. В случае утери или кражи корпоративного мобильного устройства, сотрудник обязан немедленно письменно сообщить об этом своему непосредственному руководителю и АИБ, после чего составить и передать АИБ актуальный (т. е. на момент утери или кражи) перечень содержащейся в мобильном устройстве информации ограниченного доступа.

9.2. Особенности работы с ноутбуками.

9.2.1. Передача ноутбука другим сотрудникам запрещена. В случае необходимости его использования другим сотрудником следует обратиться к системному администратору для перенастройки устройства либо согласовать возможность совместного использования с АИБ.

9.2.2. Сотрудник несет личную ответственность за сохранность выданного ноутбука. Оставлять ноутбук без присмотра, передавать посторонним лицам, а также оставлять без контроля других сотрудников запрещено. При использовании вне учреждения необходимо перевозить ноутбук в специальной сумке, не оставлять в автомобиле или общественных местах.

9.2.3. При использовании ноутбука для работы с информацией ограниченного доступа в общественных местах сотрудник обязан размещать его таким образом, чтобы предотвратить просмотр информации на экране сторонними лицами.

9.2.4. Во избежание потери информации, хранимой на ноутбуке, сотруднику следует осуществлять копирование информации в сетевые каталоги.

9.2.5. При работе с ноутбуками должны соблюдаться те же правила, что и при работе с персональными компьютерами, определенные в п. 5.1-5.5, 5.7 настоящей Политики ИБ.

9.2.6. При хранении на ноутбуке конфиденциальной информации необходимо обеспечить ее защиту от раскрытия в случае кражи устройства (например, с помощью криптографического преобразования жесткого диска и защиты от загрузки с внешних носителей).

10. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ТРЕБОВАНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

10.1. Контроль и мониторинг соблюдения настоящей Политики информационной безопасности (ИБ) и требований информационной безопасности осуществляются АИБ в соответствии с установленными данной Политикой процедурами. АИБ имеет право проверять выполнение положений настоящей Политики и требовать их соблюдения всеми сотрудниками организации

10.2. По всем фактам нарушения сотрудниками настоящей Политики ИБ и требований информационной безопасности АИБ проводит детальное служебное расследование, результаты которого доводятся до непосредственного руководителя сотрудника, а также до вышестоящего руководителя. По результатам расследования может быть принято решение о привлечении сотрудника, допустившего нарушение, к ответственности в соответствии с Правилами внутреннего трудового распорядка и Трудовым кодексом Российской Федерации. Порядок принятия такого решения определяется Трудовым кодексом РФ и внутренними нормативными актами учреждения.