Утверждаю
Начальник ГБУ РО «МИАЦ»
«_____» А.П.Бекетов

ПОЛИТИКА
информационной безопасности информационных систем персональных данных государственного бюджетного учреждения Ростовской области «Медицинский информационно-аналитический центр»

г. Ростов-на-Дону
2015 г.

ОПРЕДЕЛЕНИЯ

В настоящем документе используются следующие термины и их определения.

Автоматизированная система - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Аутентификация отправителя данных - подтверждение того, что отправитель полученных данных соответствует заявленному.

Безопасность персональных данных - состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Вирус (компьютерный, программный) - исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа - программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Вспомогательные технические средства и системы - технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

Доступ в операционную среду компьютера (информационной системы персональных данных) - получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.). исполняемых файлов прикладных программ.

Доступ к информации - возможность получения информации и ее использования.

Закладочное устройство - элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информативный сигнал - электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные) обрабатываемая в информационной системе персональных данных.

Информационная система персональных данных (ИСПДн) - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Использование персональных данных - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лип либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Источник угрозы безопасности информации - субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Контролируемая зона - пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Конфиденциальность персональных данных - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не

допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран - локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Нарушитель безопасности персональных данных - физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Неавтоматизированная обработка персональных данных - обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Недекларированные возможности - функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации - физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление,

изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Оператор (персональных данных) - государственный орган, муниципальный орган, юридическое или физическое лицо, *организующее* и (или) осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Технические средства информационной системы персональных данных - средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

Перехват (информации) - неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя. отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Политика «чистого стола» - комплекс организационных мероприятий, контролирующих отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа.

Пользователь информационной системы персональных данных - лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка - код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) блокировать аппаратные средства.

Программное (программно-математическое) воздействие - несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Раскрытие персональных данных - умышленное или случайное нарушение конфиденциальности персональных данных.

Распространение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных соях или предоставление доступа к персональным данным каким-либо иным способом.

Ресурс информационной системы - именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Специальные категории персональных данных - персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

Средства вычислительной техники - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) - лицо или процесс, действия которого регламентирующих правилами разграничения доступа.

Технический канал утечки информации - совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Угрозы безопасности персональных данных - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных

несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам - неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Уязвимость - слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АРМ	автоматизированное рабочее место информационная система
ИСПДн	персональных данных
КЗ	контролируемая зона
ЛВС	локальная вычислительная сеть
МЭ	межсетевой экран
НСД	несанкционированный доступ
ОС	операционная система
УБПДн	угрозы безопасности
СЗПДн	средства защиты персональных данных

I. ОБЩИЕ ПОЛОЖЕНИЯ

1. Политика информационной безопасности информационных систем персональных данных государственного бюджетного учреждения Ростовской области «Медицинский информационно-аналитический центр» (далее - Политика) разработана в целях реализации положений Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных па обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», иных нормативных правовых актов, руководящих и методических документов по информационной безопасности.

Настоящая Политика определяет основные цели и задачи построения системы защиты персональных данных от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, а также для минимизации ущерба от возможной реализации угроз безопасности ПДн (далее - УБПДн);

2. Действие Политики распространяется на всех должностных лиц, эксплуатирующих технические и программные средства ИСПДн.

3. Безопасность ПДн достигается путем исключения несанкционированного, в том числе случайного, доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДи, а также иных несанкционированных действий.

В ИСПДн обеспечивается доступность авторизованных пользователей к ПДн и связанным с ними ресурсам, осуществляется своевременное обнаружение и реагирование па УБПДн, а также предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

II.СИСТЕМА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. На основании результатов обследования условий обработки ПДн в ГБУ РО «МИАЦ», Переченя ИСПДн, Перечня ПДн, Акта классификации ИСПДн и установления уровня защищенности ПДн, Модели угроз безопасности ПДн при их обработке в ИСПДн, руководящих документов ФСТЭК и ФСБ России определяется необходимый уровень защищенности ПДн для каждой ИСПДн ГБУ РО «МИАЦ».

Па основании анализа актуальных угроз безопасности ПДи, описанных в Модели угроз безопасности ПДн при их обработке в ИСПДн и Отчете по результатам проверки условий обработки ПДн, делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн.

2. Для каждой ИСПДн составляется список используемых технических средств защиты, а так же программного обеспечения, участвующего в обработке ПДн в ИСПДн.

В список используемых технических средств защиты информации также включаются средства защиты.

Список функций защиты включает:

- управление и разграничение доступа пользователей;
- регистрацию и учет действий с информацией;
- обеспечение целостности данных;
- обнаружение вторжений.

3. В зависимости от уровня защищенности ПДн и актуальности угроз, СЗПДн может включать следующие технические средства:

- антивирусные средства для рабочих станций пользователей и серверов; -
средства межсетевого экранирования;
- средства криптографической защиты информации при передаче
защищаемой информации по каналам связи;
- средства защиты от НСД;
-средства обнаружения вторжений;

Ш. ТРЕБОВАНИЯ К ПОДСИСТЕМАМ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. СЗ ПДн включает в себя следующие подсистемы:

- управления доступом, регистрации и учета;
- обеспечения целостности и доступности;
- антивирусной защиты;
- анализа защищенности;
- криптографической защиты.

Подсистемы СЗ ПДн имеют различные функциональные возможности в зависимости от класса ИС ПДн и установленного уровня защищенности ПДн, определенных в Акте классификации ИС ПДн и установления уровня защищенности ПДн.

2. Подсистема управления доступом, регистрации и учета предназначена для реализации следующих функций безопасности:

- идентификация и проверка подлинности субъектов доступа при входе в ИС ПДн;
- идентификация терминалов, узлов сети, каналов связи, внешних устройств по логическим именам;
- идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;
- регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее останова;
- регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам.

Подсистема управления доступом реализуется с использованием специальных технических средств или их комплексов, обеспечивающих дополнительные меры по аутентификации и контролю (применение единых хранилищ учетных записей пользователей и регистрационной информации).

3. Подсистема обеспечения целостности и доступности предназначена для обеспечения целостности и доступности защищаемой информации при случайной или намеренной их модификации.

Подсистема реализуется с помощью организации резервного копирования обрабатываемых данных, а также резервированием ключевых элементов ИСПДн.

4. Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты серверов и автоматизированных рабочих мест пользователей ИСПДп.

Средства антивирусной защиты выполняют следующие функции:

- резидентный антивирусный мониторинг;
- антивирусное сканирование;
- централизованная (удаленная) установка (деинсталляция) антивирусного программного обеспечения, настройка, администрирование, просмотр отчетов и статистической информации но работе средств антивирусной защиты;
- автоматизированное обновление антивирусных баз;
- ограничение прав пользователя на остановку исполняемых задач и изменение нас троек антивирусного программного обеспечения;
- автоматический запуск средств антивирусной защиты после загрузки операционной системы.

Подсистема реализуется путем внедрения антивирусного программного обеспечения в ИСПДн.

5. Подсистема анализа защищенности предназначена для выявления уязвимостей, связанных с ошибками в конфигурации программного обеспечения ИСПДн, которые могут быть использованы нарушителем для реализации атаки на систему.

Функциональные возможности подсистемы реализуется программными и программно-аппаратными средствами.

Функциональные возможности подсистемы реализуются прохраммными и программно-аппаратными средствами.

6. Подсистема криптографической защиты предназначена для исключения несанкционированного доступа к защищаемой информации в ИСПДн при ее передаче по каналам связи сетей общего пользования и (или) международного обмена.

Подсистема реализуется путём внедрения в ИСПДн криптографических программно-аппаратных комплексов.

IV. ПОЛЬЗОВАТЕЛИ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. В Политике определены основные категории пользователей ИСПДи:

- администратор;

- оператор.

Па основании этих категорий устанавливаются группы пользователей ИСПДн и определяется их уровень доступа и полномочий.

2. Группы пользователей ИСПДн.

В ИСПДи ГБУ РО «МИАЦ» выделяются следующие группы пользователей, участвующих в обработке ПДн: администратор ИСПДн; администратор безопасности; оператор автоматизированного рабочего места.

2. Администратор ИСПДн сотрудник ГБУ РО «МИАЦ», ответственный за настройку, внедрение и сопровождение ИСПДн. Администратор ИСПДн обеспечивает функционирование подсистемы управления доступом ИСПДн и уполномочен осуществлять предоставление и разграничение доступа конечного пользователя (оператора АРМ) к элементам, хранящим ПДн.

Администратор ИСПДн обладает следующим уровнем доступа и знаний:

- обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;
- обладает полной информацией о технических средствах и конфигурации ИСПДн;
- имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;
- обладает правами конфигурирования и административной настройки технических средств ИСПДн.

3. Администратор безопасности – сотрудник ГБУ РО «МИАЦ», ответственный за функционирование СЗПДн, включая обслуживание и настройку административной, серверной и клиентской части программ.

Администратор безопасности обладает следующим уровнем доступа и знаний:

-обладает правами Администратора ИСПДи;

-обладает полной информацией об ИСПДн;

-имеет доступ к средствам защиты информации и протоколирования, а также к части ключевых элементов ИСПДн;

- имеет физический доступ к техническим средствам обработки информации и средствам защиты;

-не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

Администратор безопасности уполномочен:

- реализовывать политики безопасности в части настройки системы криптографической защиты информации, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь (оператор АРМ) - получает возможность работать с элементами ИСПДн;

-осуществлять настройки системы разграничения доступа к ПДн;

-осуществлять аудит средств защиты;

- знает, по меньшей мере, одно легальное имя доступа.

-устанавливать доверительные отношения своей защищенной сети с сетями других организаций, системой межведомственного электронного взаимодействия, взаимодействующими информационными системами.

4. Оператор АРМ – сотрудник ГБУ РО «МИАЦ, осуществляющий обработку ПДн. Обработка ПДн включает:

- возможность просмотра ПДн;

-ручной ввод ПДн в ИСПДн;

-формирование справок и отчетов по информации полученной из ИСПДн. Оператор не имеет полномочий па управление подсистемами обработки данных и СЗПДн.

Оператор ИСПДн обладает следующим уровнем доступа и знаний:

-обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;

-располагает конфиденциальными данными, к которым имеет доступ.

4. Технический специалист по обслуживанию - сотрудник другой организации, который осуществляет обслуживание и настройку периферийного оборудования ИСПДн. Технический специалист по обслуживанию не имеет доступа к ПДн, не имеет полномочий на управление подсистемами обработки данных и безопасности.

Технический специалист по обслуживанию обладает следующим уровнем доступа и знаний:

- обладает частью информации о системном и прикладном программном обеспечении ИСПДн;

- обладает частью информации о технических средствах и конфигурации ИСПДн;

- знает, по меньшей мере, одно легальное имя доступа.

5. Программист - разработчик (поставщик) прикладного программного обеспечения сотрудник другой организации, обеспечивающий сопровождение прикладного программного обеспечения на защищаемом объекте.

Программист-разработчик (поставщик) прикладного программного обеспечения:

- обладает информацией об алгоритмах и программах обработки информации на ИСПДн;

- обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения;

- может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИС ПДн.

6. На основании результатов проведения проверки, проводимой раз в три года, условий обработки ПДн администратором безопасности ИСПДн определяются и настраиваются права доступа к элементам ИСПДн для всех групп пользователей (настройка системы разграничения доступа к ПДн).

V. ТРЕБОВАНИЯ К ПЕРСОНАЛУ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Все сотрудники ГБУ РО «МИАЦ», являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

При вступлении нового сотрудника в ГБУ РО «МИАЦ» в должность начальник структурного подразделения обязан организовать его ознакомление с документами, регламентирующими требования по защите ПДн, а ответственный за организацию обработки ПДи обязан провести инструктаж по выполнению процедур, необходимых для санкционированного использования ИСПДн.

2. Сотрудники ГБУ РО «МИАЦ», использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать несанкционированного доступа к ним, а также возможности их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов (электронных ключей).

3. Сотрудники ГБУ РО «МИАЦ» должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации), парольная политика (Приложение №1 к настоящей Политике).

4. Сотрудники ГБУ РО «МИАЦ» должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица.

5. Сотрудникам ГБУ РО «МИАЦ» запрещается:

- устанавливать постороннее программное обеспечение;

- подключать личные мобильные устройства и носители информации, записывать на них защищаемую информацию;

- хранить защищаемую информацию и ПДн на внешних ресурсах, идентифицирован, физическое размещение которых не представляется возможным.

6. Установка, удаление, обновление программного обеспечения в ГБУ РО «МИАЦ» осуществляется только сотрудниками отдела программного обеспечения, сетевых технологий и защиты информации или сотрудниками сторонних организаций, с

которыми заключено Соглашение (договор) о конфиденциальности, либо Соглашение (договор) о соблюдении режима безопасности ПДн при выполнении работ в ИСПДн.

7. При работе с ПДн в ИСПДн, сотрудники ГБУ РО «МИАЦ» обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов автоматизированных рабочих мест или терминалов.

При завершении работы с ИСПДн сотрудники ГБУ РО «МИАЦ» обязаны провести блокировку ключом или эквивалентного средством контроля, например, доступом по паролю, если не используются более сильные средства защиты.

8. Сотрудники ГБУ РО «МИАЦ» обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, которые могут повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, ответственному за организацию обработки ПДн.

VI. ОТВЕТСТВЕННОСТЬ СОТРУДНИКОВ

1. В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством РФ ответственность.

Приложение №1 к Настоящей Политике

Парольная политика в ГБУ РО «МИАЦ»

Парольная политика представляет собой свод правил, рекомендаций и ограничений по предоставлению сотрудникам учреждения (а так же иным лицам, если это необходимо для выполнения функций ГБУ РО «МИАЦ», как учреждения) доступа к информационной системе ГБУ РО «МИАЦ», а также к специализированным программным ресурсам, входящих в ее состав.

В парольную политику также включается идентификатор пользователя (логин), который позволяет однозначно определить сотрудника, который под этим логином производит действия внутри информационной системы ГБУ РО «МИАЦ».

Для входа в информационную систему ГБУ РО «МИАЦ», а также в системы входящие в состав данной, используется логин и пароль.

Логин для постоянного доступа в информационную систему ГБУ РО «МИАЦ» – на период работы сотрудника в организации, составляется следующим образом: первый три буквы фамилии в «транслите» латинскими буквами, первая буква в нижнем регистре затем нижнее подчеркивание «_», затем первая буква имена в нижнем регистре. Если происходит совпадение с уже зарегистрированным логином, то перед нижним подчеркиванием добавляется следующая буква имени. В случаи смены пользователем информационной системы ГБУ РО «МИАЦ» фамилии или имени логин для доступа остаётся неизменным.

В срок до трёх дней сотрудниками отдела программного обеспечения, сетевых технологий и защиты информации выдаётся для нового сотрудника логин. О принятии нового сотрудника и необходимости для него доступа в ИС ГБУ РО «МИАЦ» сообщает начальник структурного подразделения, куда был принят сотрудник.

Логином для временного доступа (для тестирования ресурсов системы, проведения обучающих мероприятий и иных кратковременных действий в системе, а также для предоставления доступа к ресурсам системы на строго определенных срок) являются логины: «test» - для тестирования ресурсов системы и «temp» - временный (для временных целей).

Администрирование логинов и паролей для специализированных ресурсов внутри информационной системы осуществляется руководителями структурных подразделений в которых данная система эксплуатируется: таковыми системами являются пользовательские программы и приложения такие как «1С», «Барс», программа «Справки-ГАИ», официальный сайт ГБУ РО «МИАЦ» и прочие.

Для первого входа в информационную систему создается временный пароль – «miac» и затем без пробелов дата на момент создания учетной записи, который меняется пользователей на постоянный пароль, исходя из нижеуказанных требований:

Пароль для постоянного входа в информационную систему ГБУ РО «МИАЦ» формируется следующим образом:

- длина 8 и более символов;
- содержит минимум одну буквы верхнего и нижнего регистра;
- содержит цифры от 0 до 9;
- содержит специальные символы, отличные от букв и цифр (! № ? * и прочие);

- не содержит персональных данных пользователя, например не содержит имени учетной записи пользователя или частей полного имени пользователя длиной более двух стоящих рядом знаков;

- максимальный срок действия пароля 2 месяца.

Логин пользователя является открытой информацией. Пароль является закрытой информацией и известной только для пользователя. Пароли запрещено передавать или компрометировать т.е. писать на листочках и оставлять на столах или других легкодоступных местах. Сотрудники отдела программного обеспечения, сетевых технологий и защиты информации не должны знать и хранить пароли пользователей. В случае если пользователь забыл или по мнению сотрудников отдела программного обеспечения, сетевых технологий и защиты информации любым способом скомпрометировал свой пароль доступа в информационную систему ГБУ РО «МИАЦ», пишется докладная записка о данном инциденте на имя заместителя начальника по информатике ГБУ РО «МИАЦ».