Приложение №2
Утверждено
приказом директора
от 03.03.2025г №22/1

КОМПЛЕКТ ИНСТРУКЦИЙ
НА ИНФОРМАЦИОННЫЕ СИСТЕМЫ
в Государственном бюджетном учреждении Республики Крым «Центр социального обслуживания граждан пожилого возраста и инвалидов Бахчисарайского района»

г. Бахчисарай
2025

ИНСТРУКЦИЯ
ответственного за защиту информации в информационных системах в Государственном бюджетном учреждении Республики Крым «Центр социального обслуживания граждан пожилого возраста и инвалидов Бахчисарайского района»

1. Общие положения

Инструкция лица, ответственного за защиту информации информационных систем (далее - ИС) в Государственном бюджетном учреждении Республики Крым «Центр социального обслуживания граждан пожилого возраста и инвалидов Бахчисарайского района» (далее – Учреждение), разработана в соответствии с требованиями существующих законодательно - нормативных документов Российской Федерации и документов Учреждения в области безопасности информации.

Настоящая Инструкция закрепляет обязанности, права и ответственность лица, ответственного за защиту информации.

2. Обязанности лица, ответственного за защиту информации

Ответственный за защиту информации в Учреждении обязан:

- выполнять работы, связанные с обеспечением комплексной защиты информации на основе законодательства Российской Федерации;
- проводить сбор и анализ материалов Учреждении и эффективному использованию мер защиты информации и средств защиты информации (далее – СЗИ);
- анализировать существующие методы и средства, применяемые для контроля и защиты информации, и разрабатывать предложения по их совершенствованию и повышению эффективности этой защиты;
- участвовать в обследовании объектов защиты, их аттестации и классификации;
- разрабатывать и готовить к утверждению проекты нормативных и методических материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов;
- организовывать разработку и своевременное представление предложений для включения в соответствующие разделы перспективных и текущих планов работ и программ мер по контролю и защите информации;
- давать отзывы и заключения на проекты вновь строящихся и реконструируемых зданий и сооружений и другие разработки по вопросам обеспечения защиты информации;
- участвовать в рассмотрении технических заданий на проектирование, эскизных, технических и рабочих проектов, обеспечивать их соответствие действующим нормативным и методическим документам, а также в разработке новых принципиальных схем аппаратуры контроля, средств автоматизации контроля, моделей и систем защиты информации, оценке технико-экономического уровня и эффективности предлагаемых и реализуемых организационно-технических решений;

− определять потребность в технических средствах защиты и контроля, составлять заявки на их приобретение с необходимыми обоснованиями и расчетами к ним, контролировать их поставку и использование;

− осуществлять проверку выполнения требований межотраслевых и отраслевых нормативных документов по защите информации.

3. Функции ответственного за защиту информации

На специалиста ответственного за защиту информации возлагаются следующие функции:

− обеспечение комплексной защиты информации, соблюдения законодательства в области защиты информации ограниченного доступа;

− участие в обследовании, аттестации и классификации объектов защиты;

− разработка организационно-распорядительных документов, регламентирующих работы по защите информации;

− определение потребности в СЗИ и средствах контроля;

− проверка выполнения требований нормативных документов по защите информации.

4. Права ответственного за защиту информации

Специалист ответственный за защиту информации имеет право:

− знакомиться с проектами решений руководства Учреждения, касающимися его деятельности;

− вносить на рассмотрение руководства предложения по совершенствованию работы, связанной с обязанностями, предусмотренными настоящей инструкцией, получать от руководителей структурных подразделений, специалистов информацию и документы, необходимые для выполнения своих должностных обязанностей;

− привлекать специалистов всех структурных подразделений Учреждения, запрашивать от руководства Учреждения оказания содействия в исполнении своих должностных обязанностей и прав.

5. Ответственность лица, ответственного за защиту информации в Учреждении

За ненадлежащее исполнение или неисполнение настоящей Инструкции, а также за нарушение требований законодательства в области защиты информации лицо, ответственное за защиту информации, несет предусмотренную законодательством Российской Федерации ответственность.

ИНСТРУКЦИЯ
администратора информационной безопасности информационных систем в Государственном бюджетном учреждении Республики Крым «Центр социального обслуживания граждан пожилого возраста и инвалидов Бахчисарайского района»

1. Общие положения

Настоящий документ определяет основные обязанности, права и ответственность администратора информационной безопасности (далее – Администратор ИБ) информационных систем (далее - ИС) в Государственном бюджетном учреждении Республики Крым «Центр социального обслуживания граждан пожилого возраста и инвалидов Бахчисарайского района» (далее - Учреждение).

Администратор ИБ назначается приказом Руководителя Учреждения (далее - Руководитель). Назначение и освобождение от исполнения обязанностей согласовывается с ответственным за защиту информации.

Администратор ИБ непосредственно подчиняется ответственному за защиту информации.

Администратор ИБ осуществляет контроль выполнения требований нормативных документов в области защиты информации, осуществляет выполнение предусмотренных планом защиты ИС мероприятий по обеспечению безопасности информации при использовании на автоматизированных рабочих местах (далее - АРМ) ИС в Учреждении.

Администратор ИБ обеспечивает решение вопросов информационной безопасности дополнительно к своим непосредственным обязанностям.

2. Обязанности администратора ИБ

Администратор ИБ обязан:

- знать перечень и состав ИС в Учреждении, перечень задач, решаемых с их использованием;
- обеспечивать постоянный контроль за выполнением работниками Учреждения установленного комплекса мероприятий по обеспечению безопасности информации;
- контролировать целостность печатей (пломб) защищенных АРМ;
- в соответствии с принятой технологией работы в ИС проводить периодический анализ системных журналов средств защиты информации (далее – СЗИ) от несанкционированного доступа (далее – НСД), а также архивирование и хранение этих журналов;
- немедленно сообщать ответственному за защиту информации об имевших место в организации попытках НСД к информации и техническим средствам (далее - ТС) АРМ, а также принимать необходимые меры по устранению нарушений;

- обеспечивать соблюдение работниками Учреждения эксплуатирующими ИС и ответственными за установку, модификацию и техническое обслуживание программного обеспечения (далее - ПО) и аппаратных средств ИС утвержденного порядка проведения работ по установке и модернизации аппаратных и программных средств ИС в соответствии с «Инструкцией по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационных систем» Учреждения;
- обеспечивать строгое выполнение требований по обеспечению безопасности информации при техническом обслуживании АРМ ИС и отправке их в ремонт (контролировать затирание информации на магнитных носителях при передаче в другие отделы Учреждения, не владеющие правом доступа к ИС);
- вести «Журнал учета нештатных ситуаций, фактов вскрытия и опечатывания АРМ, выполнения профилактических работ, установки и модификации аппаратных, и программных средств защищенных АРМ» (приложение №4);
- присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию ИС;
- хранить технические паспорта ИС, контролировать их соответствие реальной конфигурации ИС и вести учет изменений аппаратно-программной конфигурации (архив документов, на основании которых были произведены данные изменения на АРМ);
- осуществлять периодический контроль за правильностью использования съемных носителей информации в ИС;
- вести учет, хранить, осуществлять прием и выдачу персональных идентификаторов пользователям, осуществлять периодический контроль за правильностью использования персональных идентификаторов пользователями ИС;
- проводить работу по выявлению возможных каналов вмешательства в процесс функционирования ИС и осуществления НСД к информации и техническим средствам АРМ и при выявлении таковых сообщать о них ответственному за защиту информации;
- проводить инструктаж работников Учреждения (пользователей средств вычислительной техники) по правилам работы с используемыми средствами и системами зашиты информации.

3.Права администратора ИБ

Администратор ИБ имеет право:

- требовать от работников Учреждения - пользователей ИС соблюдения установленных технологий обработки информации и выполнения инструкций по обеспечению безопасности и защите информации ИС;
- инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной

безопасности, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ИС;

- обращаться к ответственному за защиту информации с требованием прекращения работы пользователя в ИС при несоблюдении им установленной технологии обработки информации и невыполнении требований по безопасности;
- иметь физический доступ к машинным носителям информации;
- давать ответственному за защиту информации свои предложения по совершенствованию технических мер защиты.

4.Ответственность администратора информационной безопасности

На Администратора ИБ возлагается персональная ответственность за качество проводимых им работ по обеспечению защиты информации в Учреждении.

Администратор ИБ несет ответственность по действующему законодательству за разглашение сведений, составляющих информацию о персональных данных (далее - ПДн) либо другой конфиденциальной информации, ставшей известной ему по роду работы.

ИНСТРУКЦИЯ
системного администратора информационных систем

в Государственном бюджетном учреждении Республики Крым «Центр социального обслуживания граждан пожилого возраста и инвалидов Бахчисарайского района»

1. Общие положения

Настоящая инструкция определяет основные обязанности, права и ответственность системного администратора информационных систем (далее - ИС) в Государственном бюджетном учреждении Республики Крым «Центр социального обслуживания граждан пожилого возраста и инвалидов Бахчисарайского района» (далее - Учреждение).

Системный администратор ИС в пределах своих функциональных обязанностей, обеспечивает работоспособность автоматизированных рабочих местах (далее - АРМ) ИС и установленного программного обеспечения (далее – ПО).

Системный администратор назначается в установленном порядке приказом/распоряжением Руководителя Учреждения (далее - Руководитель).

Системный администратор в своей работе должен руководствоваться настоящей Инструкцией и следующими основными законодательными и нормативными правовыми актами Российской Федерации:

Федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных»;

Постановление Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

Приказы 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» и от 11.02.2013 года № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

локальные акты Учреждения;

иные нормативные акты Российской Федерации в области безопасности информации (ПДн).

2. Обязанности

— знать и выполнять требования действующих нормативных правовых актов Российской Федерации, а также локальных актов Учреждения, регламентирующих деятельность по защите конфиденциальной информации и персональных данных (далее - ПДн);

— устанавливать, настраивать и сопровождать необходимое для работы ИС ПО;

— обеспечивать функционирование и поддержание в рабочем состоянии ПО и АРМ в пределах возложенных на него обязанностей;

— выполнять резервирование и восстановление ПО;

— контролировать физическую сохранность оборудования ИС;

— не допускать установку, использование, хранение и распространение в ИС ПО, не связанных с выполнением функциональных задач;

— взаимодействовать с ответственным за защиту информации (организацию обработки ПДн) и администратором информационной безопасности (далее - Администратор ИБ) ИС при проведении работ, связанных с анализом и оценкой защищенности информации в ИС;

— докладывать ответственному за защиту информации (организацию обработки ПДн), Администратору ИБ ИС об обнаруженных недекларированных возможностях ПО, нарушениях и несанкционированном доступе (далее – НСД) пользователей;

— взаимодействовать с ответственным за защиту информации (организацию обработки ПДн), Администратором ИБ ИС по вопросам обеспечения правильной эксплуатации АРМ ИС;

— проводить инструктаж и консультации пользователей ИС по правилам работы и эксплуатации используемых АРМ.

3. Права

— требовать от пользователей ИС точного соблюдения установленной технологии обработки информации и выполнения правил по работе с техническими и программными средствами ИС;

— обращаться к ответственному за защиту информации (организацию обработки ПДн) и Администратору ИБ ИС с предложением о приостановке обработки конфиденциальной информации и ПДн в случаях грубых нарушений установленной технологии их обработки и/или функционирования программных и/или технических средств;

— докладывать непосредственному руководителю о нарушениях или невыполнении пользователями инструкций по работе с техническими и ПО ИС.

4. Ответственность

Системный администратор ИС несет ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством Российской Федерации.

ИНСТРУКЦИЯ
лица, ответственного за организацию обработки персональных данных

в Государственном бюджетном учреждении Республики Крым «Центр социального обслуживания граждан пожилого возраста и инвалидов Бахчисарайского района»

1. Общие положения

Должностная инструкция лица, ответственного за организацию обработки персональных данных (далее - ПДн) в информационных системах (далее - ИС) Государственного бюджетного учреждения Республики Крым «Центр социального обслуживания граждан пожилого возраста и инвалидов Бахчисарайского района» (далее - Учреждение), разработана в соответствии с Постановлением 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».

Настоящая Инструкция закрепляет обязанности, права и ответственность лица, ответственного за организацию обработки ПДн в Учреждении.

Лицо, ответственное за организацию обработки ПДн, в своей работе руководствуется Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», иными нормативными правовыми актами, настоящей Инструкцией, а также иными локальными нормативными актами Учреждения, регламентирующими вопросы обработки ПДн.

Лицо, ответственное за организацию обработки ПДн назначается приказом Руководителя Учреждения (далее - Руководитель).

2. Обязанности лица, ответственного за организацию обработки ПДн

Лицо, ответственное за организацию обработки ПДн обязано знать:

- перечень ПДн обрабатываемых в Учреждении;
- перечень информационных систем ПДн (далее – ИСПДн) Учреждения;
- перечень должностей работников Учреждения, замещение которых предусматривает осуществление обработки ПДн, либо осуществление доступа к ПДн;
- условия и технологический процесс обработки ПДн в Учреждении;
- законодательство Российской Федерации о ПДн, следить за его изменениями, своевременно и точно отражать изменения в локальных организационных актах по управлению средствами защиты информации (далее – СЗИ) в ИС и правилам обработки ПДн.

Лицо, ответственное за организацию обработки ПДн обязано:

- предоставлять на утверждение Руководителю Учреждения перечень должностей работников Учреждения замещение которых предусматривает осуществление обработки ПДн, либо осуществление доступа к ПДн и изменения к нему;

− участвовать в определении полномочий пользователей ИС (оформлении разрешительной системы доступа), минимально необходимых им для выполнения служебных (трудовых) обязанностей;

− контролировать выполнение мероприятий по защите информации в ИС;

− вносить свои предложения по совершенствованию мер защиты ПДн в ИС, разработке и принятии мер по предотвращению возможных опасных последствий нарушений, приводящих к снижению уровня защищённости ПДн вследствие неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн;

− проводить занятия и инструктажи с работниками Учреждения о порядке работы с ПДн и изучение руководящих документов в области обеспечения безопасности ПДн;

− контролировать соблюдение работниками Учреждения локальных документов, регламентирующих порядок работы с программным обеспечением (далее – ПО), техническими средствами (далее – ТС) и ПДн, машинными носителями информации;

− осуществлять внутренний контроль за соблюдением работниками Учреждения требований законодательства Российской Федерации в области ПДн, в том числе требований к защите ПДн;

− проводить разбирательства и составление заключений по фактам несоблюдения условий хранения носителей ПДн, нарушения правил работы с документами, содержащими ПДн, или по другим нарушениям, которые могут привести к снижению уровня защищённости ПДн;

− представлять интересы Учреждения при проверках надзорных органов в сфере обработки ПДн;

− выполнять иные мероприятия, требуемые нормативными документами по защите ПДн.

− осуществлять внутренний контроль за соблюдением работниками Учреждения законодательства Российской Федерации о ПДн, в том числе требований к защите ПДн;

− организовывать прием и обработку обращений и запросов субъектов ПДн или их представителей и осуществлять контроль за приемом и обработкой указанных обращений и запросов.

3. Права лица, ответственного за организацию обработки ПДн

Ответственный за организацию обработки ПДн в Учреждении имеет право:

− требовать от работников выполнения Федерального закона «О персональных данных» и принятых в соответствии с ним нормативными правовыми актами, а также локальных нормативно-правовых актов в части работы с ПДн;

− блокировать доступ к ПДн любых пользователей, если это необходимо для предотвращения нарушения режима защиты ПДн;

− проводить служебные расследования и опрашивать пользователей

по фактам несоблюдения условий хранения носителей ПДн, нарушения правил работы с ТС и ПО ИС, в том числе с СЗИ, или по другим нарушениям, которые могут привести к снижению уровня защищённости ПДн;

− привлекать к реализации мер, направленных на выполнение требований законодательства о ПДн, иных работников органа власти с возложением на них соответствующих обязанностей и закреплением ответственности;

− иметь доступ к информации, касающейся обработки ПДн в соответствующем структурном подразделении органа власти и включающей:

– цели обработки ПДн;

– категории обрабатываемых ПДн;

– категории субъектов, ПДн которых обрабатываются в ИС;

–правовые основания обработки ПДн;

– перечень действий с ПДн, общее описание используемых в центральном аппарате Роскомнадзора способов обработки ПДн;

– дату начала обработки ПДн;

– срок или условия прекращения обработки ПДн;

– сведения о наличии или об отсутствии трансграничной передачи ПДн в процессе их обработки;

– сведения об обеспечении безопасности ПДн в соответствии с требованиями к защите ПДн, установленными Правительством Российской Федерации.

5. Ответственность лица, ответственного за организацию обработки ПДн в Учреждении

За ненадлежащее исполнение или неисполнение настоящей Инструкции, а также за нарушение требований законодательства о ПДн лицо, ответственное за организацию обработки ПДн в Учреждении, несет предусмотренную законодательством Российской Федерации ответственность.

ИНСТРУКЦИЯ

по работе пользователей в информационных системах Государственного бюджетного учреждения Республики Крым «Центр социального обслуживания граждан пожилого возраста и инвалидов Бахчисарайского района»

Настоящая инструкция определяет общие положения работы пользователей в информационных системах (далее - ИС) Государственного бюджетного учреждения Республики Крым «Центр социального обслуживания граждан пожилого возраста и инвалидов Бахчисарайского района (далее – Учреждение) при обработке (наборе, редактировании и печати) информации ограниченного доступа.

В аттестованной и защищенной от несанкционированного доступа (далее - НСД) ИС осуществляется обработка информации ограниченного доступа.

Допуск пользователей для работы в ИС осуществляется в соответствии со списком лиц, допущенных к работе в ИС.

1. Учет работы пользователей в ИС производится в электронном журнале, формируемом средством защиты информации (далее – СЗИ) от НСД и контролируется администратором информационной безопасности (далее – Администратор ИБ).

2. Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИС, присвоенными ему Администратором ИБ.

3. Присвоение пользователю полномочий доступа к ресурсам компьютера и определение возможного времени работы пользователя в ИС осуществляется Администратором ИБ при первичной регистрации пользователя в ИС и отражается в «Разрешительной системе доступа (матрице доступа) ИС».

4. Пользователь отвечает за правильность включения и выключения технических средств (далее - ТС) ИС, входа в систему и все действия при работе в ИС. Время начала и окончания работы в ИС фиксируются в электронном журнале, формируемом СЗИ от НСД, и контролируется Администратором ИБ.

5. В процессе первичной регистрации для работы в ИС пользователь заявляет Администратору ИБ перечень необходимых для его работы ресурсов, и состав необходимого общесистемного программного обеспечения (далее – ПО) для решения поставленных задач.

6. Вход пользователя в систему осуществляется на основе предъявления логина (идентификатора) и ввода (по запросу системы) личного пароля длиной не менее 8-ми символов.

7. В целях предотвращения НСД посторонних лиц к ресурсам пользователя осуществляется периодическая (ежеквартальная) замена пароля пользователя. Периодическая смена личного пароля осуществляется пользователем самостоятельно, без участия Администратора ИБ. В случае

отказа системы в идентификации пользователя, либо неподтверждения личного пароля следует немедленно обратиться к Администратору ИБ.

8. При работе со съемными носителями пользователь каждый раз перед началом работы обязан проверить их на наличие вирусов с использованием штатных антивирусных программ, установленных в ИС, в соответствии с «Инструкция по организации антивирусной защиты информационных систем» Учреждения. В случае обнаружения вирусов на носителе пользователь обязан немедленно сообщить Администратору ИБ.

9. В случае оставления рабочего места на время рабочего дня пользователь обязан заблокировать ТС ввода/вывода информации в ИС с использованием функционала установленного СЗИ от НСД.

10. В процессе работы пользователю запрещается:

- использовать для постоянного хранения и обработки информации ограниченного доступа съемные накопители, не учтённые Администратором ИБ;
- осуществлять попытки НСД к ресурсам системы и других пользователей;
- пытаться подменять функции Администратора ИБ по перераспределению времени работы и полномочий доступа к ресурсам компьютера;
- покидать помещение с включенными (не заблокированными) ТС ввода/вывода информации в ИС до окончания рабочего дня.

11. По всем возникающим вопросам при работе в ИС необходимо обращаться к Администратору ИБ.

ИНСТРУКЦИЯ
по внесению изменений в списки пользователей и наделению их полномочиями доступа к ресурсам информационных систем Государственного бюджетного учреждения Республики Крым «Центр социального обслуживания граждан пожилого возраста и инвалидов Бахчисарайского района»

1. Порядок использования учетных записей пользователей

С целью соблюдения принципа персональной ответственности за свои действия каждому работнику Государственного бюджетного учреждения Республики Крым «Центр социального обслуживания граждан пожилого возраста и инвалидов Бахчисарайского района» (далее - Учреждение), допущенному к работе с конкретной подсистемой информационной системы (ИС) сопоставлено персональное уникальное имя (учетная запись пользователя), под которым он регистрируется и работать в системе. В случае производственной необходимости, некоторым работникам могут быть сопоставлены несколько уникальных имен (учетных записей).

Использование несколькими работниками при самостоятельной работе в ИС одного и того же имени пользователя («группового имени») **ЗАПРЕЩЕНО**.

2. Процедура регистрации учетных записей пользователей

Процедура регистрации (создания учетной записи) пользователя и предоставления (или изменения) ему прав доступа к ресурсам ИС инициируется приказом/распоряжением о допуске работника к работам в ИС или заявкой начальника/руководителя отдела, в котором работает данный работник, ответственному за защиту информации (форма заявки представлена в приложении 1 к данной Инструкции).

В заявке указывается:

− содержание запрашиваемых изменений (регистрация нового пользователя ИС, удаление учетной записи пользователя, расширение или сужение полномочий и прав доступа к ресурсам ИС ранее зарегистрированного пользователя);

− должность (с полным наименованием отдела), фамилия, имя и отчество работника;

− имя пользователя (учетной записи) данного работника;

− полномочия, которых необходимо лишить пользователя или которые необходимо добавить пользователю (путем указания решаемых пользователем задач в ИС).

Заявка визируется у Руководителя (далее - Руководитель) Учреждения, утверждается тем самым производственная необходимость допуска (изменения прав доступа) данного работника к необходимым для решения им указанных задач ресурсам ИС.

На основании заявки (задания) администратор информационной безопасности (далее – Администратор ИБ) Учреждения в соответствии с документацией на средства защиты информации (далее - СЗИ) производит необходимые операции по созданию (удалению) учетной записи пользователя, присвоению ему начального значения пароля и заявленных прав доступа к ресурсам ИС, включению его в соответствующие задачам группы пользователей и другие необходимые действия. Для всех пользователей должен быть установлен режим принудительного запроса смены пароля в соответствии с «Инструкцией по организации парольной защиты информационных систем».

По окончании внесения изменений в списки пользователей в заявке делается отметка о выполнении задания за подписями исполнителей.

Работнику, зарегистрированному в качестве нового пользователя системы, под роспись сообщается имя соответствующего ему пользователя, выдается персональный идентификатор (логин) и начальное значение пароля, которое он обязан сменить при первом же входе в систему.

Исполненная заявка хранится вместе с техническим паспортом на ИС у Администратора ИБ.

Приложение №1
к Инструкции по внесению изменений
в списки пользователей и наделению
их полномочиями доступа к ресурсам
информационных систем ГБУ РК
«ЦСО Бахчисарайского района»

ЗАЯВКА
на внесение изменений в списки пользователей ИС
_____
и наделение пользователя полномочиями доступа к ресурсам системы

Прошу зарегистрировать пользователем (исключить из списка пользователей, изменить полномочия пользователя) ИС
(ненужное зачеркнуть)

_____
(должность с указанием подразделения)

_____
(фамилия имя и отчество работника)

предоставив ему полномочия, необходимые (лишив его полномочий) необходимых для решения задач:
(ненужное зачеркнуть)

_____
_____
_____

Начальник _____
(наименование заказывающего отдела)

«___» _____ 20__ г. _____ _____
(дата) (подпись) (ФИО)

ЗАДАНИЕ
на внесение изменений в списки пользователей ИС

Администратору ИБ

_____
(ФИО исполнителя)

Произвести изменения в списках пользователей указанной ИС

Ответственный за защиту информации
_____.

«___» _____ 20__ г.

Обратная сторона заявки

Пользователь зарегистрирован (исключен из списка пользователей, изменены полномочия пользователя) ИС _____
(ненужное зачеркнуть)

Персональный идентификатор Touch Memory(eToken) номер _____ выдан (изъят)

Внесены следующие изменения:_____
_____

Администратор ИБ

«___» _____ 20__ г. _____ _____
(дата) (подпись) (ФИО)

Учетное имя, персональный идентификатор Touch Memory (eToken) и начальные значения паролей получил, о порядке смены пароля при первом входе в систему проинструктирован

Пользователь

_____ _____ «___» _____ 20__ г.
(подпись) (ФИО) (дата)

ИНСТРУКЦИЯ
по допуску лиц в помещения Государственного бюджетного учреждения Республики Крым «Центр социального обслуживания граждан пожилого возраста и инвалидов Бахчисарайского района», в которых ведется обработка информации ограниченного доступа

1.Общие положения

1.1. Настоящая инструкция разработана в целях обеспечения безопасности конфиденциальной информации и информации содержащей персональные данные (далее – информация ограниченного доступа), средств вычислительной техники информационных систем (далее - ИС), обрабатывающих информацию ограниченного доступа, материальных носителей информации ограниченного доступа, а так же обеспечения внутриобъектового режима Государственного бюджетного учреждения Республики Крым «Центр социального обслуживания граждан пожилого возраста и инвалидов Бахчисарайского района» (далее - Учреждение),

Объектами охраны Учреждения являются:

- помещения, в которых происходит обработка персональных данных и конфиденциальной информации, как с использованием средств автоматизации, так и без таковых;
- помещения, с ИС аттестованными по требованиям безопасности информации;
- помещения, в которых установлены компьютеры, сервера и коммутационное оборудование, участвующее в обработке информации ограниченного доступа;
- помещения, в которых хранятся материальные носители с информацией ограниченного доступа;
- помещения, в которых хранятся резервные копии информации ограниченного доступа. Бесконтрольный доступ посторонних лиц в указанные помещения должен быть исключён.

1.2. К следующим категориям объектов охраны Организации предъявляются ужесточённые требования по безопасности: помещения (далее – спецпомещения), в которых установлены средства криптографической защиты информации (далее – СКЗИ), предназначенные для шифрования информации ограниченного доступа (в том числе парольно-ключевая информация).

1.3. Ответственность за соблюдение положений настоящей инструкции несут сотрудники отделов, обрабатывающих информацию ограниченного доступа, а так же руководители отделов.

1.4. Контроль соблюдения требований настоящей инструкции возлагается на ответственного за защиту информации.

1.5. Все объекты охраны организации должны быть оборудованы охранной сигнализацией, либо предусматривать круглосуточное дежурство.

1.6. Ограждающие конструкции объектов охраны должны предполагать существенные трудности для нарушителя по их преодолению.

2. Допуск в помещения, в которых ведётся обработка информации ограниченного доступа

2.1. Доступ посторонних лиц в помещения, в которых ведётся обработка персональных данных, должен осуществляется только ввиду служебной необходимости. При этом, на момент присутствия посторонних лиц в помещении должны быть приняты меры по недопущению ознакомления посторонних лиц с информацией ограниченного доступа.

2.2. Допуск сотрудников в помещения, в которых ведётся обработка информации ограниченного доступа, оформляется после подписания сотрудником обязательства о неразглашении и проведении инструктажа ответственным за организацию обработки информации ограниченного доступа, либо администратором информационной безопасности.

2.3. В нерабочее время помещения, в которых осуществляется обработка персональных данных и конфиденциальной информации, должны ставиться на охрану. При этом все окна и двери в смежные помещения должны быть надёжно закрыты, парольно-ключевая информация, должны быть убраны в запираемые шкафы (сейфы), средства вычислительной техники выключены либо заблокированы.

3. Допуск лиц в спецпомещения

3.1. Спецпомещения выделяют с учётом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к СКЗИ. Помещения должны иметь прочные входные двери с замками, гарантирующими надёжное запирание помещений в нерабочее время. Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение посторонних лиц в спецпомещения, необходимо оборудовать металлическими решётками или ставнями, охранной сигнализацией и другими средствами, препятствующими неконтролируемому проникновению в спецпомещения.

3.2. Размещение, специальное оборудование, охрана и организация режима в спецпомещениях должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

3.3. Для предотвращения просмотра извне спецпомещений их окна должны быть защищены жалюзи или плотными занавесками.

3.4. Для хранения парольно-ключевых документов, эксплуатационной и технической документации, установочных пакетов СКЗИ, машиночитаемых носителей содержащих информацию ограниченного доступа, материальных носителей содержащих информацию ограниченного доступа не должно быть предусмотрено необходимое число надёжных металлических хранилищ, оборудованных внутренними замками с двумя экземплярами ключей и кодовыми замками или приспособлениями для опечатывания замочных скважин. Один экземпляр ключа от хранилища

должен находиться у ответственного за защиту информации, второй на посту охраны.

3.5. По окончании рабочего дня спецпомещение и установленные в нем хранилища должны быть закрыты, хранилища опечатаны.

3.6. Ключи от спецпомещений, а также ключ от хранилища, в котором находятся ключи от всех других хранилищ спецпомещения, в опечатанном виде должны быть сданы под расписку в соответствующем журнале службы охраны одновременно с передачей под охрану самих спецпомещений. Печати, предназначенные для опечатывания хранилищ, должны находиться у сотрудников, ответственных за эти хранилища.

3.7. При утрате ключа от хранилища или от входной двери в спецпомещение замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей. Факт изготовления новых ключей должен быть документально оформлен в виде акта в произвольной форме. Если замок от хранилища переделать невозможно, то такое хранилище необходимо заменить.

3.8. В обычных условиях спецпомещения и находящиеся в них опечатанные хранилища могут быть вскрыты только ответственным за обработку информацию ограниченного доступа.

При обнаружении признаков, указывающих на возможное несанкционированное проникновение в эти помещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено ответственному за защиту информации. Прибывший ответственный за организацию обработки персональных данных должен оценить возможность несанкционированного доступа к персональным данным, ключевым и другим документам, составить акт и принять, при необходимости, меры к локализации последствий.

3.9. Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего с СКЗИ, в спецпомещениях должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными СКЗИ.

3.10. На время отсутствия ответственного за обработку персональных данных указанное оборудование, при наличии технической возможности, должно быть выключено, отключено от линии связи и убрано в опечатываемые хранилища. В противном случае по согласованию с ответственным за обработку персональных данных необходимо предусмотреть организационно-технические меры, исключающие возможность ознакомления посторонних лиц с персональными данными.

ИНСТРУКЦИЯ
по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационных систем Государственного бюджетного учреждения Республики Крым «Центр социального обслуживания граждан пожилого возраста и инвалидов Бахчисарайского района»

1.Общие положения

Изменения в составе программного обеспечения (далее - ПО) информационных систем (далее - ИС) Государственного бюджетного учреждения Республики Крым «Центр социального обслуживания граждан пожилого возраста и инвалидов Бахчисарайского района» (далее - Учреждение) могут вноситься только с лицензионных дистрибутивных носителей информации, имеющих сертификат качества. Устанавливаемое ПО должно иметь необходимую эксплуатационную документацию.

При необходимости внесения изменений в программную среду подается служебная записка (заказ, запрос) от исполнителя (пользователя или оператора) начальнику структурного подразделения/отдела (форма заявки представлена в приложении 1 к данной Инструкции).

Изменения в программную среду должны производиться только на основании заявок начальников/руководителей отделов и структурных подразделений ответственному за защиту информации с указанием наименования ПО и обоснованием его необходимости при выполнении задания исполнителя.

Ответственность за обоснование необходимости внесения изменений в программную среду и использование нового ПО несут исполнители (пользователи или операторы).

Перед установкой нового ПО пользователь совместно с администратором информационной безопасности (далее – Администратор ИБ) производит антивирусный контроль дистрибутива.

Отладочные и экспериментальные работы (апробирование программ) проводится с применением неконфиденциальной (условной) информации в ИС в свободное от обработки персональных данных и конфиденциальной информации время.

После установки ПО осуществляется проверка его функционирования, делается отметка в журнале учета нештатных ситуаций, фактов вскрытия и опечатывания автоматизированных рабочих местах (далее - АРМ), выполнения профилактических работ, установки и модификации аппаратных и программных средств АРМ и составляется акт ввода в эксплуатацию, который подписывается всеми членами комиссии и утверждается.

В случае обнаружения недекларированных (не описанных в документации) возможностей ПО, исполнители (пользователи или операторы) немедленно докладывают начальнику/руководителю своего отдела и ответственному за защиту информации.

Дальнейшее использование ПО до получения специальных указаний прекращается.

Исполнители, в части их касающейся, обязаны знать документацию на программное средство и уметь правильно его эксплуатировать. Ознакомление и обучение пользователей работе с программным средством в пределах выполняемых функций проводит Администратор ИБ.

Начальная установка и настройка программного средства осуществляется Администратором ИБ согласно эксплуатационной документации.

Настройка прав доступа к устанавливаемому программному средству при использовании в составе ИС средств защиты выполняется Администратором ИБ в соответствии с установленной политикой безопасности.

После установки нового ПО Администратор ИБ вносит необходимые изменения в перечень программ, используемых в ИС, представленному в техническом паспорте на ИС.

Допуск новых пользователей к решению задач с использованием вновь развернутого ПО (либо изменение их полномочий доступа) осуществляется согласно «Инструкция по внесению изменений в списки пользователей и наделению их полномочиями доступа к ресурсам информационных систем» Учреждения.

2. Порядок технического обслуживания и ремонта технических средств ИС

Техническое обслуживание и ремонтные работы на технических средствах АРМ ИС должны осуществляться только уполномоченными работниками, назначенными ответственными за их обслуживание (сопровождение).

Вызов уполномоченных работников при возникновении нештатных ситуаций, осуществляется работниками Учреждения эксплуатирующими ИС.

К нештатным ситуациям относятся:

- выход из строя или неустойчивое функционирование узлов АРМ (например дисковода, видеокарты и т.п.) или периферийных устройств (например принтера, клавиатуры и т.п.) ИС;
- выход из строя системы электроснабжения ИС.

Техническое обслуживание и регламентные работы могут проводиться в плановом порядке. В этом случае работы проводятся на основании утвержденных руководством и согласованных с ответственным за защиту информации заявок.

Ответственность за соблюдение требований по обеспечению безопасности информации при проведении технического обслуживания и ремонтных работ на АРМ возлагается на Администратора ИБ.

Уполномоченные работники допускаются к ИС для разбора нештатных ситуаций при обнаружении сбоев в работе только для тестирования АРМ с использованием установленных в ИС тестовых средств.

По окончании выполнения данных работ составляется акт с указанием признаков проявления ситуации и содержанием выполненных работ по ее устранению.

При необходимости осуществления изменений аппаратной конфигурации ИС соответствующие работы выполняются по согласованию с организацией проводившей аттестационные испытания.

При изъятии АРМ, ее передача на склад, в ремонт или в другое подразделение для решения иных задач осуществляется только после того, как Администратор ИБ снимет с данной АРМ средства защиты информации (далее - СЗИ), жесткие диски и предпримет необходимые меры для затирания защищаемой информации, которая хранилась на дисках компьютера. Факт уничтожения данных, находившихся на диске компьютера оформляется актом за подписью ответственного за защиту информации (форма акта приведена в приложении 2 к данной Инструкции).

Оригиналы документов, на основании которых производились изменения в составе аппаратно-программных средств ИС и акты о внесении изменений в состав аппаратно-программных средств должны храниться вместе с техническими паспортами ИС.

3. Порядок выводы объекта информатизации из эксплуатации

Вывод ИС из эксплуатации возможен по следующим причинам:

отсутствия необходимости обработки информации ограниченного доступа в организации;

изменение условий функционирования ИС и технологии защищаемой информации, способных повлиять на степень защищенности информации;

Окончание действия «Аттестат соответствия требованиям безопасности информации» на ИС.

ИС выводится из эксплуатации на основании приказа Руководителя Учреждения.

4. Порядок проверки работоспособности системы защиты после установки (обновления) ПО ИС и внесения изменений в списки пользователей

После установки (обновления) ПО ИС или внесения изменений в списки пользователей системы Администратор ИБ обязан проверить работоспособность ИС и правильность настройки СЗИ, установленных на АРМ.

При установке нового (обновлении существующего) ПО Администратор ИБ обязан:

- установить права доступа пользователей системы к файлам ПО в соответствии с установленной политикой безопасности;
- подсчитать контрольные суммы файлов программных средств (при необходимости);
- если для пользователя, использующего установленное ПО, установлен режим замкнутой программной среды, необходимо с помощью СЗИ добавить в список разрешенных ему для запуска программ исполняемые модули данного пакета.

После осуществления данных действий необходимо проверить корректность функционирования системы защиты, для чего требуется произвести следующие действия:

- для каждого пользователя ИС, для которого установлен режим замкнутой программной среды, требуется проверить работоспособность установленного ПО и сохранение режима замкнутой программной среды;
- в режиме пользователя необходимо проверить возможность изменения вновь установленных (обновленных) файлов.
- для каждого пользователя необходимо проверить (при необходимости) разграничение доступа к вновь установленным (обновленным) файлам.

Приложение №1
к Инструкции по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационных систем ГБУ РК «ЦСО Бахчисарайского района»

ЗАЯВКА
на внесение изменений в состав программного обеспечения ИС _____

Прошу согласовать с администратором ИБ ИС организацию работ по установке ПО / изменению настроек используемого ПО ИС _____
(ненужное зачеркнуть)

_____
_____
(перечень ПО и необходимых настроек)

для решения задач:
_____
_____
следующим пользователям: _____
_____
_____
__

Начальник _____
(наименование заказывающего подразделения)

«___» _____ 20__ г. _____ _____
(дата) (подпись) (ФИО)

Обратная сторона заявки

Изменения ПО на ПЭВМ ИС произведены (не произведены) по следующей причине: _____
_____

Проделаны следующие работы: _____
_____
_____
_____

И проделаны следующие изменения в настройках средств защиты:_____
_____
_____

Отметка в журнале учета нештатных ситуаций, фактов вскрытия и опечатывания ПЭВМ, выполнения профилактических работ, установки и модификации аппаратных и программных средств защищенных ПЭВМ по факту работ сделана.

Администратор ИБ

«___» _____ 20__ г. _____ _____
(дата) (подпись) (ФИО)

Приложение №2
к Инструкции по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационных систем ГБУ РК «ЦСО Бахчисарайского района»

АКТ
о затирании остаточной информации,
хранившейся на диске компьютера

Все файлы, содержащие подлежащую защите информацию, находившиеся на НЖМД № _____, переданном _____
(с какой целью)

_____
_____
(кому: должность, Ф.И.О.)

_____

системного блока ПЭВМ марки _____
серийный №_____
уничтожены (затерты) посредством программы
_____.

Администратор ИБ

_____ _____
(Ф.И.О.) (подпись)

«____» _____ 20__г.

Ответственный за безопасность персональных данных

_____ _____
(Ф.И.О.) (подпись)

«____» _____ 20__г.

ИНСТРУКЦИЯ
по организации антивирусной защиты информационных систем Государственного бюджетного учреждения Республики Крым «Центр социального обслуживания граждан пожилого возраста и инвалидов Бахчисарайского района»

1. Общие положения

Настоящая Инструкция определяет требования к организации защиты информационных систем (далее - ИС) Государственного бюджетного учреждения Республики Крым «Центр социального обслуживания граждан пожилого возраста и инвалидов Бахчисарайского района» (далее - Учреждение) от воздействия защищаемых вирусов и устанавливает ответственность начальников и работников отделов, эксплуатирующих и сопровождающих ИС, за их выполнение.

К использованию в ИС допускаются только лицензионные и сертифицированные антивирусные средства, закупленные у разработчиков (поставщиков) указанных средств, рекомендованные к применению ответственным за защиту информации.

В случае необходимости использования антивирусных средств, не вошедших в перечень рекомендованных, их применение необходимо согласовать с ответственным за защиту информации.

Установка средств антивирусной защиты на автоматизированных рабочих местах (далее – АРМ) осуществляется администратором информационной безопасности (далее – Администратор ИБ) в соответствии с «Инструкцией по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационных систем» Учреждения. Настройка параметров средств антивирусной защиты осуществляется Администратором ИБ в соответствии с руководствами по применению конкретных антивирусных средств.

2. Применение средств антивирусного контроля

Антивирусный контроль всех дисков и файлов ИС после загрузки АРМ должен проводиться в автоматическом режиме (периодическое сканирование или мониторинг).

Периодически, не реже одного раза в месяц, должен проводиться полный антивирусный контроль всех дисков и файлов ИС (сканирование).

Обязательной антивирусной защите подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая информация на съемных носителях (магнитных дисках, CD-ROM и т.п.). Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

Файлы, помещаемые в электронный архив должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

Установка (изменение) системного и прикладного программного обеспечения (далее - ПО) осуществляется в соответствии с «Инструкция по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационных систем» Учреждения. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено Администратором ИБ на отсутствие вирусов. Непосредственно после установки (изменения) ПО АРМ должна быть выполнена антивирусная проверка жестких дисков АРМ лицом, установившим (изменившим) ПО, под контролем Администратора ИБ.

Факт выполнения антивирусной проверки после установки (изменения) ПО должен регистрироваться в специальном журнале за подписью лица, установившего (изменившего) ПО, и лица, его контролировавшего.

3. Действия работников при подозрении наличия компьютерного вируса

При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) работник отдела самостоятельно или вместе с Администратором ИБ должен провести внеочередной антивирусный контроль АРМ. При необходимости он должен привлечь Администратора ИБ для определения ими факта наличия или отсутствия компьютерного вируса.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов работники обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов начальника отдела и Администратора ИБ, владельца зараженных файлов, а также смежные отделы, использующие эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь администратора информационной безопасности);
- в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, передать зараженный вирусом файл на съемном носителе информации ответственному за защиту информации для дальнейшей передачи его в организацию, с которой заключен договор на антивирусную поддержку (при необходимости, для выполнения требований данного пункта привлечь Администратора ИБ);
- по факту обнаружения зараженных вирусом файлов составить служебную записку ответственному за защиту информации, в которой

необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

4. Порядок обновления антивирусных баз

Обновление антивирусных баз должно проводиться регулярно, с периодичностью определенной технологией работы в ИС.

Обновление антивирусных баз ИС АРМ имеющих подключение к сети международного телекоммуникационного обмена Интернет, осуществляется с сервера производителя антивирусного ПО ежедневно.

Обновлению подлежат только антивирусные базы.

5. Ответственность

Ответственность за организацию антивирусной защиты в отделах, эксплуатирующих ИС, в соответствии с требованиями настоящей Инструкции возлагается на начальников отделов.

Ответственность за проведение мероприятий антивирусного контроля в отделах и соблюдение требований настоящей Инструкции возлагается на ответственного за защиту информации в организации и всех работников, являющихся пользователями ИС.

Периодический контроль за состоянием антивирусной защиты в ИС, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции работниками Учреждения осуществляется ответственным за защиту информации.

ИНСТРУКЦИЯ
по организации парольной защиты информационных систем Государственного бюджетного учреждения Республики Крым «Центр социального обслуживания граждан пожилого возраста и инвалидов Бахчисарайского района»

1. Общие сведения

Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах (далее - ИС) Государственного бюджетного учреждения Республики Крым «Центр социального обслуживания граждан пожилого возраста и инвалидов Бахчисарайского района» (далее - Учреждения), а также контроль за действиями пользователей ИС при работе с паролями.

Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на администратора информационной безопасности (далее – Администратор ИБ).

2. Требования к паролям

Личные пароли при первоначальной регистрации пользователей должны назначаться Администратором ИБ ИС с учетом следующих требований (данные требования применимы в дальнейшем при смене паролей пользователями):

- длина пароля должна быть не менее 8 символов;
- в числе символов пароля обязательно должны присутствовать буквы и цифры;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;
- личный пароль пользователь не имеет права сообщать никому.

Владельцы паролей должны быть ознакомлены с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

Для генерации «стойких» значений паролей могут применяться специальные программные средства. Система генерации паролей должна исключать возможность ознакомления других работников с паролями пользователей.

3. Смена паролей

Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в 3 месяца.

Внеплановая смена личного пароля или удаление учетной записи пользователя ИС в случае прекращения его полномочий (увольнение, переход на другую работу внутри организации и т.п.) должна производиться Администратором ИБ немедленно после окончания последнего сеанса работы данного пользователя с системой.

Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри организации и другие обстоятельства) Администратора ИБ и других работников, которым по роду работы были предоставлены полномочия по управлению парольной защитой ИС.

4. Хранение и контроль

Хранение работником (исполнителем) значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе (запираемом ящике стола, шкафа, другом стационарном недоступном общему доступу месте), либо в сейфе у ответственного за защиту информации или у начальника отдела в опечатанном личной печатью пенале.

Повседневный контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на начальников отделов, периодический контроль – возлагается на Администратора ИБ.

В случае компрометации личного пароля пользователя ИС должны быть немедленно предприняты меры по изменению пароля и выявлению последствий компрометации.

ИНСТРУКЦИЯ
по проведению контроля состояния защиты информационных систем Государственного бюджетного учреждения Республики Крым «Центр социального обслуживания граждан пожилого возраста и инвалидов Бахчисарайского района»

Контроль состояния защиты информационной системы (далее - ИС) Государственного бюджетного учреждения Республики Крым «Центр социального обслуживания граждан пожилого возраста и инвалидов Бахчисарайского района» (далее - Учреждение) осуществляется в целях оценки организации защиты конфиденциальной информации и персональных данных, своевременного выявления и предотвращения технических каналов ее утечки, несанкционированного доступа (далее - НСД) к ней, оценки эффективности защиты.

Контроль осуществляет администратор информационной безопасности (далее – Администратор ИБ), либо ответственное лицо совместно с Администратором ИБ.

Рекомендуется проводить проверку не реже 1 раза в год.

Внеплановую проверку рекомендуется проводить после внесения изменений в систему защиты ИС, либо в ее состав.

Проверка осуществляется на основании приказа/распоряжения Руководителя Учреждения (далее - Руководитель).

Контроль состояния защиты ИС включает:

1. Рассмотрение актов ранее проведенных обследований и результатов оценки защищенности в ИС;
2. Выявление технических каналов утечки конфиденциальной информации и персональных данных (далее – информация ограниченного доступа) в ИС, каналов несанкционированного доступа (далее – НСД) к ней и специальных воздействий на нее;
3. Оценку эффективности проводимых мероприятий по технической защите информации ограниченного доступа;
4. Выявление и анализ нарушений установленных норм и требований по технической защите информации ограниченного доступа, и принятие мер по пресечению выявленных нарушений;
5. Разработку рекомендаций по устранению выявленных недостатков в организации и проведении работ по технической защите информации ограниченного доступа в ИС;
6. Проверку устранения недостатков, выявленных в результате контроля.

При проведении контроля подлежат проверке следующие вопросы:

1. Назначение приказом/распоряжением, сотрудников, обеспечивающих решение вопросов, связанных с защитой информации ограниченного доступа;

2. Наличие необходимых руководящих документов по защите информации ограниченного доступа;

3. Своевременность и правильность доведения требований руководящих документов по защите информации ограниченного доступа до сотрудников Организации, знание этих требований сотрудниками;

4. Наличие аттестатов на ИС и срок их действия;

5. Соответствие правильности обработки и хранения информации ограниченного доступа при использовании технических средств (далее - ТС) (СВТ, ТСПИ, оргтехники и т.п.), правильность распечатки документов и их учета инструкциям;

6. Наличие комплекта необходимых документов на технические средства, используемые при обработке информации ограниченного доступа;

7. Использование средств защиты информации ограниченного доступа в сетях связи и в ИС.

Несоответствие мер технической защиты информации ограниченного доступа установленным нормам и требованиям защиты такой информации считается нарушением.

При выявлении нарушений проверяющий (Администратор ИБ) обязан доложить ответственному за защиту информации о выявленных нарушениях.

Совместно с ответственным за защиту информации Учреждения принять необходимые меры по их устранению. При этом должен быть составлен план устранения недостатков, который согласовывается с ответственным за защиту информации в Учреждении (при необходимости с вышестоящим органом (по подчиненности объекта) и владельцем или распорядителем защищаемой информации).

Проверка считается законченной после выполнения всех мероприятий плана устранения нарушений и недостатков и положительных результатов проверки устранения недостатков.

По результатам проверки Администратором ИБ составляется акт, с которым ответственный за защиту информации ознакамливает Руководителя Учреждения.

Все документы, касающиеся проверки, хранятся у ответственного за защиту информации.

ИНСТРУКЦИЯ
по резервному копированию информации в информационных системах Государственного бюджетного учреждения Республики Крым «Центр социального обслуживания граждан пожилого возраста и инвалидов Бахчисарайского района»

1. Общие положения

Настоящий документ определяет порядок осуществления резервного копирования информационных ресурсов информационной системы (далее - ИС) Государственного бюджетного учреждения Республики Крым «Центр социального обслуживания граждан пожилого возраста и инвалидов Бахчисарайского района» (далее - Учреждение).

Процесс резервного копирования обеспечивает сохранение на резервных носителях информации, с целью ее восстановления при потере или порче на основном носителе, и является ключевым элементом защиты от умышленной и неумышленной потери данных.

Конкретные информационные ресурсы, подлежащие резервному копированию, порядок их копирования приводится в «Форме регламента резервного копирования» (далее – Регламент).

Регламент составляется администратором информационной безопасности (далее – Администратор ИБ) ИС в соответствии с положениями данной Инструкции.

Регламент должен содержать перечень информационных ресурсов, подлежащих резервному копированию, и график осуществления резервного копирования, составленный с учетом требований руководителей отделов организации и Администратора ИБ.

Резервное копирование осуществляется Администратором ИБ и контролируется ответственным за обеспечение безопасности информации.

Должностные лица Организации, задействованные в осуществлении резервного копирования информационных ресурсов ИС, знакомятся с основными положениями и приложениями Инструкции в части, их касающейся, по мере необходимости.

2. Периодичность и схема резервного копирования

При осуществлении резервного копирования используется два типа копирования: полное резервное копирование и инкрементальное резервное копирование.

Резервное копирование информационных ресурсов ИС осуществляется по трехуровневой схеме ротации.

В соответствии с трехуровневой схемой ротации:

- полное резервное копирование информационных ресурсов выполняется 15-16 числа каждого месяца (архив хранится в течение года и является архивом Уровня 1);

- полное резервное копирование информационных ресурсов выполняется в конце каждой недели (в пятницу) (архив хранится в течение календарного месяца и является архивом Уровня 2);

- полное резервное копирование информационных ресурсов выполняется в начале каждой недели, затем ежедневно на эту копию выполняется инкрементальное копирование (архив хранится в течение недели и является архивом Уровня 3).

3. Порядок резервного копирования

Администратор ИБ настраивает задания для программного обеспечения (далее – ПО), осуществляющего резервное копирование, на автоматическое выполнение в соответствии с перечнем информационных ресурсов подлежащих резервному копированию и графиком резервного копирования.

Перед выполнением задания резервного копирования Администратор ИБ проверяет доступность резервного носителя, а также наличие на нем свободного места для записи данных.

После завершения выполнения задачи резервного копирования Администратор ИБ должен извлечь резервный носитель, подписать его по формату «число, месяц, год, уровень № __» и поместить в сейф.

4. Хранение резервных копий

Хранение резервных копий должно быть организовано в отдельном от копируемых информационных ресурсов помещении, оснащенном соответствующими системами вентиляции, кондиционирования и отопления для поддержки требуемых параметров температуры, влажности и т.п.

Резервные носители должны храниться в кассетах или закрытых коробках на безопасном расстоянии от источников магнитных полей: блоков питания, телефонов, мониторов и т.п.

Доступ к хранилищу резервных копий должны иметь только Администратор ИБ и ответственный за защиту информации.

5. Восстановление после сбоя

В случае потери данных на основном носителе из хранилища извлекается накопитель с резервной копией информационных ресурсов, нуждающихся в восстановлении, от последнего произведенного резервного копирования.

В зависимости от характера и уровня повреждения информационных ресурсов, Администратор ИБ восстанавливает либо весь массив резервных данных, либо отдельные поврежденные или уничтоженные файлы и папки.

6. Порядок пересмотра инструкции

Инструкция подлежит полному пересмотру при изменении перечня решаемых задач, состава технических и программных средств ИС, приводящих к существенным изменениям технологии обработки информации.

Инструкция подлежит частичному пересмотру в остальных случаях. Частичный пересмотр проводится ответственным за обеспечение безопасности информации.

Полный плановый пересмотр данного документа также проводится регулярно, раз в год, с целью проверки соответствия положений данного документа реальным условиям применения их в ИС.

Частичный пересмотр данного документа проводится по письменному предложению Администратора ИБ.

Вносимые изменения не должны противоречить другим положениям Инструкции.

7. Ответственные за выполнения инструкции

Ответственность за выполнение резервного копирования и восстановление данных из резервных копий, а также за соблюдение периодичности и порядка выполнения резервного копирования возлагается на Администратора ИБ.

Ответственность за сохранность резервных копий возлагается на ответственного за защиту информации.

Ответственным за постоянный контроль выполнения требований данной Инструкции является ответственный за защиту информации.

ИНСТРУКЦИЯ
по обращению с защищаемыми носителями конфиденциальной информации в информационных системах Государственного бюджетного учреждения Республики Крым «Центр социального обслуживания граждан пожилого возраста и инвалидов Бахчисарайского района»

Данная Инструкция содержит обязательные для всех пользователей (исполнителей) и обслуживающего персонала информационных систем (далее - ИС) Государственного бюджетного учреждения Республики Крым «Центр социального обслуживания граждан пожилого возраста и инвалидов Бахчисарайского района»
(далее – Учреждение), обрабатывающих конфиденциальную информацию и персональные данные (далее - информация ограниченного доступа) и правила обращения с носителями, использующимися для записи информации ограниченного доступа.

Под защищаемыми носителями информации понимаются различные по физической структуре и конструктивному исполнению носители информации, используемые для записи и накопления информации с целью непосредственного ввода её на автоматизированном рабочем месте (далее - АРМ), обработки и передачи при помощи технических средств (далее - ТС).

Данной Инструкцией определяется порядок учета, хранения и обращения со съемными защищаемыми носителями информации ограниченного доступа и их утилизации. К съемным носителям информации относятся носители для однократной или многократной записи такие, как CD-R, CD-RW, DVD-R, DVD-RW, USB флеш-накопители, дискеты, съемные жесткие диски.

Также данная инструкция регламентирует порядок обслуживания и обеспечение безопасности несъемных электронных носителей информации ограниченного доступа, к которым относятся базы данных на жестких магнитных дисках, содержащие информацию ограниченного доступа.

Под безопасностью данных на электронных носителях понимается сохранение конфиденциальности, исключение несанкционированного доступа либо иных действий, в том числе не имеющих злого умысла, которые могут привести к потере, искажению, изменению, копированию и другим нежелательным действиям с информацией ограниченного доступа.

Организационное и техническое обеспечение безопасности информации ограниченного доступа, хранящейся на защищаемых носителях в ИС, с использованием допустимых программно-аппаратных методов защиты, контроль за действиями исполнителей и обслуживающего персонала при работе с указанными носителями возлагается на ответственного за защиту информации.

1. Все носители информации должны храниться в надежной, защищенной среде в соответствии с инструкциями производителей при температуре воздуха +17 – 25 °С и относительной влажности 50 – 55 %.

Специфика условий и режима хранения определяется типом носителей, но общими требованиями при хранении любых электронных носителей являются защита их от механических повреждений, деформаций, загрязнения, запыления, воздействия экстремальных температур и прямых солнечных лучей. Для магнитных носителей (дискет, жестких дисков и т. п.) необходимо дополнительно обеспечить защиту их от магнитных и электромагнитных воздействий окружающей среды, не размещать их в непосредственной близости к мощным источникам электромагнитных полей — электродвигателей, обогревателей и т. п.

2. Все находящиеся на хранении и в обращении съемные носители информации ограниченного доступа подлежат учёту. Каждый съемный носитель с записанными на нем информации ограниченного доступа должен иметь этикетку, на которой указывается его уникальный учетный номер.

3. Учет съемных носителей информации ограниченного доступа по форме осуществляет ответственный за защиту информации. При получении или передаче носителя делаются соответствующие записи в журнале учета.

4. При обработке информации ограниченного доступа пользователи ИС должны использовать только специально предназначенные для этого разделы (каталоги) электронных носителей или съемные маркированные носители.

5. При хранении носителей должны соблюдаться условия, обеспечивающие сохранность информации ограниченного доступа и исключающие несанкционированный доступ к ней.

6. Хранение работником носителей информации ограниченного доступа допускается только в личном сейфе, либо в сейфе уполномоченного сотрудника.

7. Работникам запрещается:

7.1 хранить съемные носители информации ограниченного доступа вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра в незапертом помещении или передавать на хранение другим лицам;

7.2 выносить съемные носители информации ограниченного доступа из служебных помещений для работы с ними на дому и т. д.

8. При отправке или передаче информации ограниченного доступа адресатам на съемные носители записываются только предназначенные адресатам данные. Вынос съемных носителей информации ограниченного доступа для непосредственной передачи адресату осуществляется только с письменного разрешения Руководителя Учреждения (далее - Руководитель) на основании запроса сторонней организации с обязательной регистрацией в «Журнал регистрации запросов на предоставление персональных данных».

9. Для защиты защищаемых носителей информации от несанкционированного доступа, использования или повреждения во время транспортировки из одной организации в другую необходимо использовать надежных курьеров и транспорт, а также упаковку, защищающую носители от постороннего вмешательства и позволяющую выявить попытки ее вскрытия.

10. О фактах утраты носителей информации ограниченного доступа либо разглашения содержащихся на них сведений немедленно ставится в известность Руководитель Учреждения. На утраченные носители составляется акт. Соответствующие отметки вносятся в журналы персонального учета съемных носителей информации ограниченного доступа.

11. Съемные носители информации ограниченного доступа, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей информации ограниченного доступа осуществляется уполномоченной комиссией. По результатам уничтожения носителей составляется акт (форма акта представлена в приложение 1 к данной Инструкции).

12. Носители, на которые осуществляется резервное копирование баз данных ИС, должны регулярно (не реже одного раза в 6 месяцев) проверяться на отсутствие сбоев уполномоченными сотрудниками. Процедуры резервного копирования и восстановления данных регламентированы в «Инструкция по резервному копированию информации в информационных системах» Учреждения.

13. При повторном использовании носителей информации ограниченного доступа предыдущее содержимое должно надежно удаляться администратором информационной безопасности.

14. Повседневный и периодический контроль за действиями исполнителей – пользователей ИС при работе с носителями информации ограниченного доступа возлагается на уполномоченных сотрудников.

Приложение №1
к Инструкции по обращению с
защищаемыми
носителями конфиденциальной информации
в информационных системах
ГБУ РК «ЦСО Бахчисарайского района»

УТВЕРЖДАЮ

Руководитель

_____

« ____»_____ 20___г.

АКТ

уничтожения съемных носителей персональных данных

Комиссия, наделенная полномочиями приказом директора ГБУ РК «ЦСО Бахчисарайского района» №____ от «____» _____ 20___ в составе:

1.
_____

2.
_____

3.
_____

провела отбор съемных носителей персональных данных, не подлежащих дальнейшему хранению:

№п/п	Дата	Учетный номер съемного носителя	Пояснения
1			
2			
…			

Всего съемных
носителей_____

(цифрами и прописью)

На съемных носителях уничтожена конфиденциальная информация путем стирания ее на устройстве гарантированного уничтожения информации _____(механического уничтожения, сжигания и т. п.).

Перечисленные съемные носители уничтожены путем_____ (разрезания, демонтажа и т. п.).

Председатель комиссии _____/Ф. И.О./

Члены комиссии _____/Ф. И.О./

ИНСТРУКЦИЯ
реагирования на инциденты информационной безопасности в информационных системах Государственного бюджетного учреждения Республики Крым «Центр социального обслуживания граждан пожилого возраста и инвалидов Бахчисарайского района»

1. Назначение настоящего документа

Настоящая Инструкция реагирования на инциденты информационной безопасности (далее - Инструкция) устанавливает порядок действий лиц, ответственных за обеспечение информационной безопасности в информационных системах Государственного бюджетного учреждения Республики Крым «Центр социального обслуживания граждан пожилого возраста и инвалидов Бахчисарайского района» (далее - Учреждение), при выявлении инцидента информационной безопасности в целях снижения его негативных последствий, а также порядок проведения расследования инцидента информационной безопасности (далее - инцидент).

Настоящий регламент разработан с учетом ГОСТ Р ИСО/МЭК ТО 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности».

2. Область действия настоящего документа

Руководство действиями, предусмотренными данной Инструкцией, осуществляет лицо, ответственное за обеспечение информационной безопасности в Учреждении (далее - Администратор ИБ).

3. Основные положения

3.1. Понятие «инцидент информационной безопасности» Инцидент информационной безопасности - это одно или серия событий, которое привело к уничтожению, модификации, копированию, распространению (только в отношении информации ограниченного доступа) информации, обрабатываемой на автоматизированных рабочих местах и (или) серверах Учреждения, а также блокировке доступа к ней.

Инциденты могут быть преднамеренными или случайными (например, являться следствием какой-либо человеческой ошибки или природных явлений) и вызваны как техническими, так и нетехническими средствами.

Следует отличать событие информационной безопасности от инцидента.

Событие информационной безопасности - идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение принятых организационно-распорядительных документов по защите информации или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности.

Событие может быть результатом случайных или преднамеренных попыток компрометации защитных мер, но в большинстве случаев событие само по себе не означает, что попытка в действительности была успешной и, следовательно, каким-то образом повлияла на конфиденциальность, целостность и (или) доступность, то есть не все события будут отнесены к категории инцидентов.

3.2. Выявление инцидента

Основными источниками, от которых администратор ИБ может получить сведения об инцидентах информационной безопасности, являются:

- сообщения от работников Учреждения о выявленных фактах нарушения информационной безопасности;
- результаты работы средств мониторинга информационной безопасности, результаты проверок и аудита (внутреннего или внешнего);
- журналы и оповещения операционных систем серверов и рабочих станций, антивирусной системы, системы резервного копирования и других систем и средств защиты информации.

Администратор ИБ должен регулярно информировать работников о необходимости немедленного его оповещения о возникновении инцидента с указанием контактной информации и способов предоставления информации.

3.3. Порядок действий администратора ИБ при обнаружении инцидента информационной безопасности

3.3.1. Анализ исходной информации и принятие решения о проведении

Разбирательства Администратор ИБ с момента получения информации о предполагаемом инциденте информационной безопасности незамедлительно проводит первоначальный анализ полученных данных.

По усмотрению администратора ИБ в случае если инцидент не привел к негативным последствиям в связи с уничтожением, модификацией, копированием, распространением (только в отношении информации ограниченного доступа) информации, обрабатываемой на автоматизированных рабочих местах и (или) серверах, а также блокировке доступа к ней (например, случайное удаление файлов с информацией, имеющей резервные копии, не имеет негативных последствий для деятельности Учреждения разбирательство может не проводиться.

В случае если инцидент привел к негативным последствиям, администратор ИБ собирает группу реагирования на инциденты информационной безопасности в целях совместного принятия решения о необходимости проведения разбирательства. В группу включаются компетентные сотрудники в области информационных технологий Учреждения.

В случае принятия группой решения о необходимости проведения разбирательства администратор ИБ информирует об инциденте информационной безопасности руководителя Учреждения.

3.3.2. Реагирование на инцидент информационной безопасности (устранение причин и последствий инцидента)

Администратор ИБ определяет и в кратчайшие сроки, не превышающие одного рабочего дня, инициирует первоочередные меры, направленные на локализацию инцидента и минимизацию его последствий. В случае если инцидент информационной безопасности связан с совершением компьютерных атак или внедрением вредоносного программного обеспечения, администратор ИБ Учреждения в целях совместной выработки и реализации мер по их локализации, устранению и ликвидации последствий должен незамедлительно информировать руководителя Учреждения.

3.3.3. Разбирательство (проведение служебного расследования) инцидента информационной безопасности

После локализации инцидента и восстановления штатного режима работы проводится разбирательство инцидента информационной безопасности.

Разбирательство представляет собой получение (сбор) необходимой информации об инциденте, доказательств факта возникновения инцидента, определение обстоятельств (деталей), способствовавших совершению инцидента, в целях определения причин возникновения инцидента, виновных лиц и меры ответственности за нарушение безопасности информации.

Важным является обеспечение сохранности и целостности доказательств факта возникновения инцидента для их представления на судебном процессе при необходимости привлечения лица, по вине которого произошел инцидент, к ответственности в соответствии с действующим законодательством Российской Федерации.

По результатам расследования администратор ИБ формирует заключение по расследованию инцидента, согласовывает его со всеми участниками разбирательства и передает имеющиеся материалы (в объеме, достаточном для принятия решения) руководителю Учреждения для решения вопроса о привлечении виновного в инциденте к ответственности.

3.3.4. Порядок документирования процедур

На основе собранной в процессе разбирательства информации администратор ИБ также заполняет отчет об инциденте в целях систематизации информации об инцидентах и ее дальнейшего анализа.

В отчете указывается следующая информация:

- Дата и время совершения инцидента.
- Источник информации, от которого администратор ИБ получил информацию об инциденте (в соответствии с п. 3.2 настоящего регламента).
- Ф.И.О. и должность лица, по вине которого произошел инцидент.

Если инцидент произошел по причине некорректной работы средств защиты информации или их некорректной настройки, ответственность за инцидент несет лицо, ответственное за установку, настройку и функционирование средств защиты информации.

Если инцидент произошел по причине некорректной работы программного обеспечения или технических средств, ответственность несут лицо, ответственное за функционирование программного обеспечения и технических средств.

В случае если инцидент произошел вследствие невыполнения работниками требований организационно-распорядительных документов по защите информации в Учреждении, персональную ответственность несут работники, нарушившие требования документов, в том числе работники, на которых возложен контроль соблюдения требований данных документов.

- Описание инцидента.

В данном разделе необходимо указать, какое из свойств информации было нарушено (конфиденциальность, целостность, доступность) в результате инцидента и указать функциональное воздействие инцидента на деятельность Учреждения:

- несуществующий - воздействие на способность Учреждения выполнять свои функции отсутствует;
- низкий - минимальный эффект; Учреждение все еще может выполнять все основные функции, но со сниженной эффективностью;
- средний – Учреждение потеряло способность обеспечить часть основных функции;
- высокий – Учреждение не в состоянии выполнять свои функции.

- Причины инцидента.

- Меры, принятые для устранения причин, последствий инцидента.

Данный пункт позволит в случае повторного возникновения инцидента в минимальные сроки устранить его.

По результатам формирования отчета об инциденте администратором ИБ заполняется Журнал учета инцидентов информационной безопасности.

Журнал позволяет вести статистику всех инцидентов информационной безопасности, которая является показателем эффективности функционирования системы защиты информации. Статистику инцидентов следует регулярно анализировать в рамках проведения оценки защищенности информационных систем.

3.3.5. Выработка корректирующих и превентивных мероприятий

По результатам разбирательства принимается решение о необходимости принятия дополнительных организационных и технических мер, направленных на предотвращение или минимизацию рисков возникновения подобных нарушений в будущем (в некоторых случаях последствия инцидента незначительны по сравнению с корректирующими и превентивными действиями, и тогда целесообразно не совершать дальнейших шагов после устранения последствий инцидента).

4. Ответственность

Каждый работник Учреждения несет персональную дисциплинарную, административную или уголовную ответственность за действия либо бездействия, повлекшие неправомерное уничтожение, блокирование, модификацию либо копирование информации, в соответствии с действующим законодательством Российской Федерации.