

УТВЕРЖДАЮ
Директор ОАУСО «Холмский КЦ»

С. А. Сафонова
«09» декабря 2016 г.



ИНСТРУКЦИЯ
администратора информационной безопасности
информационных систем персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

Администратор информационной безопасности информационной (далее – АИБ) системы персональных данных (далее – ИСПДн) назначается приказом директора ОАУСО «Холмский КЦ». Он руководствуется требованиями нормативных документов Российской Федерации, ведомственных организационно-распорядительных документов, локальных актов ОАУСО «Холмский КЦ», настоящей Инструкцией, а также другими распорядительными документами в части, его касающейся.

АИБ ИСПДн в пределах своих функциональных обязанностей обеспечивает работоспособность ИСПДн, безопасность информации, обрабатываемой, передаваемой и хранимой при помощи средств вычислительной техники (далее – СВТ) в ИСПДн ОАУСО «Холмский КЦ».

Должностные лица, задействованные в обеспечении функционирования ИСПДн, могут быть ознакомлены с основными положениями и приложениями Инструкции в части, их касающейся, по мере необходимости.

В случае увольнения, АИБ ИСПДн обязан передать директору ОАУСО «Холмский КЦ», которые находились в его распоряжении в связи с выполнением им служебных обязанностей во время работы в ОАУСО «Холмский КЦ».

2. ОБЯЗАННОСТИ АДМИНИСТРАТОРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИСПДн

Администратор информационной безопасности ИСПДн обязан:

- знать перечень установленных в подразделении СВТ и перечень задач, решаемых с их использованием;
- осуществлять контроль изменений (в том числе и несанкционированных) аппаратного обеспечения АРМ и серверов;
- устанавливать и настраивать средства защиты информации, а также выполнять другие возложенные на него работы в соответствии с распорядительными, инструктивными и методическими материалами в части, его касающейся;
- рассматривать целесообразность применения новых технологий для повышения эффективности функционирования ИСПДн;
- выполнять своевременное обновление средств защиты персональных данных (ПДн) по мере выявления таких обновлений;
- обеспечивать контроль за выполнением пользователями требований «Инструкции пользователя ИСПДн»;
- осуществлять контроль работы пользователей ИСПДн, выявление попыток НСД к защищаемым информационным ресурсам и техническим средствам ИСПДн. При выявлении фактов несанкционированного доступа – фиксировать данные в «Журнале учета нештатных ситуаций»;
- осуществлять настройку средств защиты, выполнять другие действия по изменению элементов ИСПДн;
- осуществлять учет всех защищаемых носителей информации с помощью их любой маркировки и с занесением учетных данных в «Журнале учета носителей персональных данных». Учетные носители информации выдавать пользователям под подпись в «Журнале учета выдачи электронных носителей персональных данных». Использование неучтенных носителей ПДн, равно как их выдача/прием без записи в соответствующем журнале – категорически запрещается;
- осуществлять текущий и периодический контроль работы средств и систем защиты информации;
- осуществлять текущий контроль технологического процесса обработки защищаемой информации;
- периодически осуществлять тестирование всех функций системы защиты с помощью тестовых программ, имитирующих попытки НСД, а также при изменении программной среды персонала ИСПДн;
- участвовать в проведении служебных расследований фактов нарушения или угрозы нарушения безопасности защищаемой информации;
- участвовать в проведении работ по восстановлению работоспособности средств и систем защиты информации;

- вести «Журнал учета нештатных ситуаций», учитывать факты вскрытия и обечатывания персональных электронно-вычислительных машин (ПЭВМ), выполнения профилактических работ, установки и модификации аппаратных и программных средств ПЭВМ;
- проводить проверку регистраций событий безопасности;
- проводить обучение персонала и пользователей вычислительной техники правилам работы с СВТ и средствами защиты информации с отметкой в «Журнале учета инструктажей по вопросам защиты» по следующим вопросам:
 - а) обеспечение антивирусной защиты при работе в информационных системах персональных данных;
 - б) порядок парольной защиты при работе в информационных системах персональных данных; участвовать в разработке нормативных и методических материалов, связанных с функционированием СВТ и применением средств защиты информации, выполнением мероприятий по обеспечению защиты информации;
- в случае возникновения нештатных ситуаций (сбоев в работе ПОБИ) немедленно докладывать ответственному за обеспечение безопасности и обработки ПДн;
- рассматривать заявки пользователей на доступ к информационным ресурсам ИСПДн пользователей;
- осуществлять контроль технологических процессов обработки защищаемой информации;
- разрабатывать предложения по изменению нормативных документов, регламентирующих процессы обработки и обеспечения безопасности персональных данных;
- осуществлять совместно с Ответственным за обеспечение ИБ периодические проверки состояния защиты персональных данных (в соответствии с утвержденным «Планом внутренних проверок состояния защиты персональных данных» и «Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных»);
- участвовать в качестве члена комиссиях по:
 - а) проведению классификации информационных систем персональных данных;
 - б) установлению уровней защищенности информационных систем персональных данных;
 - в) уничтожению персональных данных;
 - г) контролю защищенности персональных данных;
- вести учет всех средств защиты информации и технической документации к ним, используемых в ОАУСО «Холмский КЦ» в «Журнале поэкземплярного учета средств защиты персональных данных, эксплуатационной и технической документации к ним»;
- оказывать помощь в разработке Администратору ИСПДн и согласовывать перечень информационных ресурсов ИСПДн, подлежащих резервному копированию, а также осуществлять контроль выполнения резервного копирования информационных ресурсов Администратором ИСПДн;
- осуществлять надежное хранение резервных копий;
- осуществлять контроль действий пользователей ИСПДн с паролями;
- оказывать помощь Ответственному за обеспечение безопасности и обработку персональных данных в других вопросах, касающихся обеспечения безопасности и обработки персональных данных ОАУСО «Холмский КЦ».

3. ПРАВА АДМИНИСТРАТОРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИСПДн

Администратор информационной безопасности ИСПДн имеет право:

- отключать любые элементы СЗПДн при изменении конфигурации, регламентном техническом обслуживании или устранении неисправностей в установленном порядке;
- в установленном порядке изменять конфигурацию элементов ИСПДн и СЗПДн;
- требовать от сотрудников ОАУСО «Холмский КЦ» соблюдения правил работы в ИСПДн, определенных в «Инструкции пользователя ИСПДн»;

- требовать от пользователей безусловного соблюдения установленной технологии обработки защищаемой информации и выполнения требований внутренних документов ОАУСО «Холмский КЦ», регламентирующих вопросы обеспечения безопасности и защиты информации;
- обращаться к ответственному за обеспечение безопасности и обработки ПДн с требованием о прекращении обработки информации в случаях нарушения установленной технологии обработки защищаемой информации или нарушения функционирования средств и систем защиты информации;
- просить свои предложения по совершенствованию функционирования ИСПДн;
- инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения ИБ в ИСПДн.

4. ОТВЕТСТВЕННОСТЬ АДМИНИСТРАТОРА ИБ ИСПДн

Администратор информационной безопасности ИСПДн несет ответственность:

- за ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей инструкцией, другими инструктивными документами в соответствии с действующим законодательством Российской Федерации, трудовым законодательством Российской Федерации, за полноту и качество проводимых им работ по обеспечению защиты информации;
- за правонарушения, совершенные в процессе своей деятельности в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации;
- за разглашение сведений конфиденциального характера и другой защищаемой информации ОАУСО «Холмский КЦ» в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации;
- на АИБ ИСПДн возлагается персональная ответственность за работоспособность средств защиты ПДн

5. ПОРЯДОК ПЕРЕСМОТРА ИНСТРУКЦИИ

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

Инструкция подлежит частичному пересмотру в остальных случаях. Частичный пересмотр проводится ответственным за обеспечение безопасности и обработки ПДн ОАУСО «Холмский КЦ».

Полный пересмотр данного документа проводится ответственным за обеспечение безопасности и обработки ПДн ОАУСО «Холмский КЦ» с целью проверки соответствия положений данного документа реальным условиям применения их в ИСПДн.

Все изменения вносятся в лист регистрации изменений в Инструкции, форма которого представлена в Приложении № 1 к данной инструкции.

Вносимые изменения не должны противоречить другим положениям Инструкции.

6. ОТВЕТСТВЕННЫЕ ЗА КОНТРОЛЬ ВЫПОЛНЕНИЯ ИНСТРУКЦИИ

Ответственным за контроль выполнения требований данной Инструкции является ответственный за обеспечение безопасности и обработки ПДн.

