Приложение 4
к приказу ГБУК г. Москвы «Государственный
выставочный зал истории войны в Афганистане»
от 27.09.2023г. № ВЗА-1-03-24

ПОЛОЖЕНИЕ
об обеспечении безопасности персональных данных в ГБУК г. Москвы «Государственный выставочный зал истории войны в Афганистане» при их обработке в информационных системах персональных данных

1. Понятия и сокращения

1.1. В Положении используются следующие понятия, определения и сокращения:

Учреждение – ГБУК г. Москвы «Государственный выставочный зал истории войны в Афганистане».

ПДн (персональные данные) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Обработка ПДн – любое действие с персональными данными, совершаемое с использованием средств автоматизации или без использования таких средств.

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

Пользователь ИСПДн (также – пользователь) – сотрудник Учреждения, допущенный к обработке ПДн.

АРМ – автоматизированное рабочее место пользователя ИСПДн.

Автоматизированная обработка ПДн – обработка ПДн с помощью средств вычислительной техники.

Обработка ПДн без использования средств автоматизации – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных осуществляются при непосредственном участии человека.

Актуальные угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Система защиты персональных данных (СЗПДн) – организационные и технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

СВТ – средства вычислительной техники.

НСД – несанкционированный доступ к данным, защищаемым СВТ.

БД – базы данных ПДн.

СЗИ – средства защиты информации.

2. Общие положения

2.1. Настоящее Положение об обеспечении безопасности персональных данных при их автоматизированной обработке в информационных системах персональных данных устанавливает состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных на протяжении всего цикла их эксплуатации.

2.2. Меры по обеспечению безопасности персональных данных принимаются для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

2.3. Меры по обеспечению безопасности персональных данных реализуются в рамках системы их защиты, создаваемой Учреждением в соответствии с требованиями к защите персональных данных при их обработке в информационных системах, утвержденными постановлением

Правительства Российской Федерации от 1 ноября 2012 г. № 1119, приказом 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 должны быть направлены на нейтрализацию актуальных угроз безопасности персональных данных.

2.4. Положение определяет

- порядок работы работников Учреждения с ИСПДн в части обеспечения безопасности ПДн при их обработке,
- порядок разбирательства и составления заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации,
- разработку и принятие мер по предотвращению возможных опасных последствий таких нарушений,
- порядок приостановки предоставления ПДн в случае обнаружения нарушений порядка их предоставления,
- порядок обучения работников практике работы в ИСПДн,
- порядок проверки электронного журнала обращений к ИСПДн,
- порядок контроля соблюдения условий использования средств защиты информации, предусмотренные эксплуатационной и технической документацией,
- правила обновления общесистемного и прикладного программного обеспечения,
- правила организации антивирусной защиты и парольной защиты ИСПДн,
- порядок охраны и допуска посторонних лиц в защищаемые помещения.

2.5. Настоящее Положение вступает в силу с момента его утверждения директором Учреждения и действует бессрочно, до замены его новым Положением.

2.6. Настоящее Положение подлежит корректировке при изменении законодательных и нормативно-правовых актов, по рекомендациям надзорных органов, по результатам проверок в рамках государственного контроля, а также в целях совершенствования технологий обработки ПДн.

2.8. Все сотрудники Учреждения, допущенные к обработке персональных данных, должны быть ознакомлены под подпись с Положением и изменениями к нему.

2.9. Настоящее Положение является обязательным для исполнения всеми сотрудниками Учреждения, имеющими доступ к персональным данным.

2.10. Ответственность за актуализацию настоящего Положения и

текущий контроль над выполнением норм Положения возлагается на назначаемого приказом Учреждения работника, ответственного за обеспечение информационной безопасности и защиты персональных данных.

2.11. Настоящее Положение разработано на основании следующих основных нормативных правовых актов и документов в области обеспечения безопасности ПДн:

- Федеральный закон от 27 июля 2006 г. № 152-ФЗ "О персональных данных";
- постановление Правительства Российской Федераций от 1 ноября 2012 г. № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";
- приказ Федеральной службы по техническому и экспортному контролю 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".

2.12. Положение разработано с учетом требований Положения об обработке и защите персональных данных в ГБУК г. Москвы «Государственный выставочный зал истории войны в Афганистане».

2.13. Учреждение учитывает требования настоящего Положения при разработке и утверждении внутренних локальных актов и иных документов Учреждения, связанных с обработкой ПДн.

3. Порядок работы пользователей ИСПДн по обеспечению безопасности ПДн

3.1. Настоящий порядок определяет действия пользователей ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн.

3.2. Допуск пользователей для работы на АРМ осуществляется на основании приказа и в соответствии со списком лиц, допущенных к работе в ИСПДн. В целях обеспечения ответственности за ведение, нормальное функционирование и контроль работы средств защиты информации в ИСПДн директором назначается администратор ИСПДн.

3.3. Администратор ИСПДн должен иметь профильное либо дополнительное образование в области защиты информации. Рекомендуется прохождение администратором специализированных курсов по защите информации в ИСПДн.

3.4. Администратор осуществляет свои полномочия совместно с лицом, назначенным в Учреждении ответственным за обработку и защиту персональных данных.

3.5. Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн. При этом для хранения информации, содержащей ПДн, разрешается использовать только машинные носители информации, учтенные в журнале учета машинных носителей.

3.6. Пользователь несет ответственность за правильность включения и выключения средств вычислительной техники, входа в систему и за все действия при работе в ИСПДн.

3.7. Вход пользователя в ИСПДн должен осуществляться по выдаваемому ему персональному паролю.

3.8. Запись информации, содержащей ПДн, может осуществляться пользователем на съемные машинные носители информации, соответствующим образом учтенные в журнале учета машинных носителей.

3.9. При работе со съемными машинными носителями информации пользователь каждый раз перед началом работы обязан проверить их на отсутствие вирусов с использованием штатных антивирусных программ, установленных на АРМ ИСПДн. В случае обнаружения вирусов пользователь обязан немедленно прекратить использование съемных носителей и действовать в соответствии с требованиями Положения.

3.10. Каждый работник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и *обязан:*

3.10.1. строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн;

3.10.2. знать и строго выполнять правила работы со средствами защиты информации, установленными на АРМ ИСПДн;

3.10.3. хранить в тайне свой пароль (пароли). В соответствии требованиями Положения с установленной периодичностью менять свой пароль (пароли);

3.10.4. хранить в установленном порядке свое индивидуальное устройство идентификации;

3.10.5. выполнять требования Положения по организации антивирусной защиты в полном объеме;

3.10.6. немедленно извещать администратора ИСПДн в случае:

компрометации личных паролей;

выявления фактов совершения в отсутствие пользователя попыток несанкционированного доступа к данным защищаемым АРМ;

несанкционированных изменений в конфигурации программных или аппаратных средств ИСПДн;

отклонений в нормальной работе системных и прикладных программных средств, выхода из строя или неустойчивого функционирования периферийных устройств (сканера, принтера и т.п.), а также перебоев в системе электроснабжения;

некорректного функционирования установленных на АРМ технических средств защиты.

3.11. Пользователю категорически запрещается:

3.11.1. использовать компоненты программного и аппаратного обеспечения АРМ в неслужебных целях;

3.11.2. самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства;

3.11.3. осуществлять обработку ПДн в присутствии посторонних (не допущенных к данной информации) лиц;

3.11.4. записывать и хранить конфиденциальную информацию (содержащую сведения ограниченного распространения) на неучтенных машинных носителях информации;

3.11.5. оставлять включенным без присмотра компьютер;

3.11.6. оставлять без личного присмотра на рабочем месте (или где бы то ни было) машинные носители и распечатки, содержащие ПДн либо другую служебную защищаемую информацию;

3.11.7. умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации;

3.11.8. размещать средства ИСПДн так, чтобы с них существовала возможность визуального считывания информации.

3.12. Администратор ИСПДн обязан:

3.12.1. знать состав основных и вспомогательных технических систем и средств, установленных и смонтированных в ИСПДн, перечень используемого программного обеспечения в ИСПДн;

3.12.2. контролировать целостность печатей (пломб, защитных наклеек) на периферийном оборудовании, защищенных АРМ и других устройствах;

3.12.3. производить необходимые настройки подсистемы управления доступом АРМ к ИСПДн, при этом:

3.12.4. реализовывать полномочия доступа (чтение, запись) для каждого пользователя к элементам защищаемых информационных ресурсов (файлам, каталогам, принтеру и т.д.);

3.12.5. вводить описания пользователей ИСПДн в информационную базу СЗИ от НСД;

3.12.6. своевременно удалять описания пользователей из базы данных СЗИ при изменении списка допущенных к работе лиц;

3.12.7. контролировать доступ лиц в помещение в соответствии со списком сотрудников, допущенных к работе в ИСПДн;

3.12.8. проводить инструктаж пользователей ИСПДн по правилам работы с используемыми техническими средствами и системами защиты информации;

3.12.9. контролировать своевременное (не реже чем один раз в полгода) проведение смены паролей для доступа пользователей к АРМ и ресурсам ИСПДн;

3.12.10. обеспечивать постоянный контроль выполнения работниками установленного комплекса мероприятий по обеспечению безопасности информации в ИСПДн;

3.12.11. осуществлять контроль порядка создания, учета, хранения и использования резервных и архивных копий массивов данных;

3.12.12. настраивать и сопровождать подсистемы регистрации и учета действий пользователей при работе в ИСПДн;

3.12.13. вводить в базу данных СЗИ от несанкционированного доступа описания событий, подлежащих регистрации в системном журнале;

3.12.14. проводить анализ системного журнала для выявления попыток несанкционированного доступа к защищаемым ресурсам не реже одного раза в 10 дней;

3.12.15. организовывать печать файлов пользователей на принтере и осуществлять контроль соблюдения установленных правил и параметров регистрации, а также учета бумажных носителей информации;

3.12.16. сопровождать подсистемы обеспечения целостности информации в ИСПДн;

3.120.17. периодически тестировать функции СЗИ от НСД, особенно при изменении программной среды и полномочий исполнителей;

3.12.18. восстанавливать программную среду, программные средства и настройки СЗИ при сбоях;

3.12.19. вести две копии программных средств СЗИ от НСД и контролировать их работоспособность;

3.12.20. контролировать отсутствие на магнитных носителях остаточной информации по окончании работы пользователей;

3.12.21. периодически обновлять антивирусные средства (базы данных), контролировать соблюдение пользователями порядок и правила проведения антивирусного тестирования;

3.12.22. проводить работу по выявлению возможных каналов вмешательства в процесс функционирования ИСПДн и осуществления несанкционированного доступа к информации и техническим средствам вычислительной техники;

3.12.23. сопровождать подсистему защиты информации от утечки за счет побочных электромагнитных излучений и наводок, контролировать соблюдение требований по размещению и использованию технических средств ИСПДн;

3.12.24. контролировать соответствие документально утвержденного состава аппаратной и программной части ИСПДн реальным конфигурациям ИСПДн, вести учет изменений аппаратно-программной конфигурации;

3.12.25. обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации технического обслуживания ИСПДн и отправке его в ремонт (контролировать затирание конфиденциальной информации на магнитных носителях с составлением соответствующего акта);

3.12.26. присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию ИСПДн;

3.12.27. вести Журнал учета нештатных ситуаций, фактов вскрытия и опечатывания СВТ, выполнения профилактических работ, установки и модификации аппаратных и программных средств СВТ;

3.12.28. поддерживать установленный порядок проведения антивирусного контроля в соответствии с требованиями настоящего Положения, в случае отказа средств и систем защиты информации принимать меры по их восстановлению;

3.12.29. докладывать руководителям о неправомерных действиях пользователей, приводящих к нарушению требований по защите информации;

3.12.30. вести документацию на ИСПДн в соответствии с требованиями нормативных документов.

3.12.31. определять необходимый уровень защищённости ПДн при их обработке в каждой из ИСПДн;

3.12.32. определять и осуществлять организационные и технические мероприятия, которые должны выполняться Оператором ИСПДн для нейтрализации угроз ПДн, признанных актуальными;

3.13. Администратор ИСПДн должен обеспечивать выполнение следующих основных мероприятий:

3.13.1. организация режима обеспечения безопасности помещений, в которых размещены ИСПДн, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

3.13.2. обеспечение сохранности носителей персональных данных;

3.13.3. использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз, при этом сертификаты на средства защиты информации должны быть действительными;

3.13.4. ограничения доступа к содержанию электронного журнала сообщений: доступ должен быть возможен исключительно для работников, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения трудовых обязанностей (для ИСПДн, для которой установлена необходимость обеспечения 3 уровня защищённости);

3.13.5. автоматическая регистрация в электронном журнале безопасности изменения полномочий работника по доступу к персональным данным, содержащимся в ИСПДн;

3.13.6. организация (при получении информации о факте нарушения действующих законодательных норм по обеспечению безопасности персональных данных в ИСПДн), служебного расследования для выявления лиц, в результате действий или бездействия которых произошло нарушение законодательных норм по обеспечению безопасности персональных данных.

3.14. Администратор ИСПДн имеет право:

3.14.1. требовать от пользователей ИСПДн соблюдения установленной технологии обработки информации и выполнения инструкций по обеспечению безопасности и защите информации в ИСПДн;

3.14.2. инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, модификации, порчи защищаемой информации и технических компонентов ИСПДн;

3.14.3. требовать прекращения обработки информации в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации;

3.14.4. участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа.

4. Требования по организации разрешительной системы доступа

к ИСПДн

4.1. Разрешительная система доступа к обрабатываемой в ИСПДн информации предусматривает установление единого порядка обращения со сведениями, содержащими ПДн, и их носителями, определяет степень ограничения на доступ к данной информации и степень ответственности за сохранность предоставленной информации.

4.2. Организация разрешительной системы доступа относится к основным вопросам управления обеспечением безопасности ПДн и включает:

- распределение функций управления доступом к данным и их обработкой между должностными лицами;
- определение порядка изменения правил доступа к защищаемой информации;
- определение порядка изменения правил доступа к резервируемым информационным и аппаратным ресурсам;
- контроль функционирования разрешительной системы доступа и расследование фактов неправомерного доступа лиц к защищаемой информации, в случае выявления таковых;
- оценку эффективности мер по исключению утечки информации;
- организацию деятельности должностных лиц, ответственных за подготовку предложений о внесении изменений в должностные обязанности и иные документы, определяющие задачи и функции пользователей ИСПДн;
- разработку внутренних организационно-распорядительных документов, определяющих порядок реализации и функционирования разрешительной системы доступа.

4.3. Основные условия правомерного доступа работников к обрабатываемой в ИСПДн информации включают в себя:

- подписание обязательства о неразглашении конфиденциальной информации;
- наличие у работника права допуска к ПДн, обрабатываемым в ИСПДн;
- наличие утвержденных в соответствии с трудовым законодательством Российской Федерации должностных инструкций работника, определяющих круг его задач и объем необходимой для их решения информации.

4.4. Лица, доступ которых к ПДн, обрабатываемым в ИСПДн, необходим для выполнения трудовых обязанностей, допускаются к соответствующим ПДн на основании списка, утвержденного приказом

Учреждения. Права доступа работников к защищаемой информации определяются в Матрице доступа.

4.5. Для обеспечения персональной ответственности за свои действия каждому пользователю ИСПДн присваивается уникальное имя (учетная запись пользователя), под которым он регистрируется и осуществляет работу в системе.

4.6. При регистрации и назначении прав доступа пользователей ИСПДн выполняются следующие требования:

- каждому пользователю присваивается уникальный идентификатор пользователя, по которому его можно однозначно идентифицировать;
- учетные записи всех пользователей привязываются к конкретным автоматизированным рабочим местам, за исключением учетных записей технического персонала, обслуживающего компоненты ИСПДн;
- при регистрации пользователей проводится проверка соответствия уровня доступа возложенным на пользователя задачам;
- назначенные пользователю права доступа документируются;
- пользователь знакомится под роспись с предоставленными ему правами доступа и порядком его осуществления;
- в ИСПДн предусматривается разрешение доступа только аутентифицированным пользователям;
- при внесении нового пользователя разрабатывается и обновляется формальный список всех пользователей, зарегистрированных для работы в ИСПДн;
- при изменении должностных обязанностей или увольнении пользователя проводится немедленное исправление или аннулирование прав его доступа;
- администраторами ИСПДн проводится удаление всех неиспользуемых учетных записей. Предусмотренные в системе запасные идентификаторы недоступны другим пользователям.

4.7. Контроль выполнения требований разрешительной системы доступа к ПДн возлагается на администратора ИСПДн и ответственного за обработку и защиту ПДн.

5. Порядок резервирования и восстановления СВТ, ПО, БД и СЗИ

5.1. Настоящий порядок определяет организацию резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации.

5.2. К использованию (для создания резервной копии в ИСПДн) допускаются только зарегистрированные в журнале учета носители.

5.3. Администратор ИСПДн обязан осуществлять периодическое резервное копирование конфиденциальной информации.

5.4. Еженедельно по окончанию работы с конфиденциальными документами, содержащими персональные данные, пользователь АРМ (при отсутствии администратора ИСПДн) обязан создавать резервную копию конфиденциальных документов на зарегистрированный носитель, создавая тем самым резервный электронный архив конфиденциальных документов.

5.5. Носители информации, предназначенные для создания резервной копии и хранения конфиденциальной информации, выдаются в установленном порядке руководителем или администратором ИСПДн. По окончании процедуры резервного копирования электронные носители конфиденциальной информации сдаются на хранение или администратору ИСПДн, или руководителю, или ответственному обработку и защиту ПДн.

5.6. Перед резервным копированием пользователь или администратор ИСПДн обязан проверить электронный носитель на отсутствие вирусов.

5.7. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

5.8. Запрещается запись посторонней информации на электронные носители резервной копии.

5.9. Хранение электронного носителя с резервной копией защищаемой информации осуществляется в специальном металлическом хранилище.

5.10. При восстановлении работоспособности программного обеспечения сначала осуществляется резервное копирование защищаемой информации, затем производится полная деинсталляция некорректно работающего программного обеспечения.

5.11. Восстановление программного обеспечения производится путем его инсталляции с использованием эталонных дистрибутивов, хранение которых осуществляется администратором ИСПДн в специальном хранилище.

5.12. При необходимости ремонта технических средств с них удаляются опечатывающие пломбы, после чего (по согласованию с администратором, ответственным за защиту информации, и представителем организации, проводившей аттестацию) оборудование передается в сервисный центр производителя.

5.13. Ремонт носителей защищаемой информации не допускается. Неисправные носители с защищаемой информацией подлежат уничтожению.

5.14. Восстановление средств защиты информации производится с использованием эталонных сертифицированных дистрибутивов, которые

хранятся в хранилище. После успешной настройки средств защиты информации необходимо выполнить резервное копирование настроек данных средств при помощи встроенных в них функций на зарегистрированный носитель.

5.15. Ответственность за осуществление резервного копирования в ИСПДн, за проведение мероприятий по восстановлению работоспособности технических средств и программного обеспечения баз, а также восстановление средств защиты информации возлагается администратора ИСПДн.

6. Порядок контроля защиты персональных данных в ИСПДн

6.1. Контроль защиты информации в ИСПДн – комплекс организационных и технических мероприятий, которые организуются и осуществляются в целях предупреждения и пресечения возможности получения посторонними лицами охраняемых сведений, выявления и предотвращения утечки информации по техническим каналам, исключения или существенного затруднения несанкционированного доступа к информации, хищения технических средств и носителей информации, предотвращения специальных программно-технических воздействий, вызывающих нарушение характеристик безопасности информации или работоспособности систем информатизации.

6.2. Основными задачами контроля являются:

— проверка выполнения плановых мероприятий по защите информации в структурных подразделениях, учета требований по защите ПДн в разрабатываемых плановых и распорядительных документах;
— уточнение зон перехвата обрабатываемой информации, возможных каналов утечки информации, несанкционированного доступа к ней и программно-технических воздействий на информацию (перечень каналов утечки устанавливается в соответствии с разработанной моделью угроз);
— проверка выполнения установленных норм и требований по защите информации от компрометации, оценка достаточности и эффективности мероприятий по защите информации;
— проверка выполнения требований по защите ИСПДн от несанкционированного доступа;
— проверка выполнения требований по антивирусной защите ИСПДн и АРМ;

— проверка знаний работников по вопросам защиты информации и их соответствия требованиям уровня подготовки для конкретного рабочего места;
— оперативное принятие мер по пресечению нарушений требований защиты информации в ИСПДн;
разработка предложений по устранению недостатков в обработке ПДн.

6.3. В ходе контроля проверяются:

- соответствие принятых мер по обеспечению безопасности персональных данных требованиям Федерального закона от 27 июля 2006 г. № 152-ФЗ "О персональных данных", постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" и иным нормативным актам, принятым на их основе;
- своевременность и полнота выполнения требований законодательства в сфере обработки ПДн и настоящего Положения;
- полнота выявления каналов утечки информации, несанкционированного доступа к ней и программно-технических воздействий на информацию;
- эффективность применяемых организационных и технических мероприятий по защите информации;
- устранение ранее выявленных недостатков.

Кроме того, приглашенными специалистами организации, имеющей соответствующие лицензии ФСТЭК России, могут проводиться необходимые измерения и расчеты.

6.4. Основными видами технического контроля являются визуально-оптический контроль, контроль эффективности защиты информации от утечки по техническим каналам, контроль несанкционированного доступа к информации и программно-технических воздействий на информацию.

6.5. Результаты, полученные в ходе ведения контроля, обрабатываются и анализируются в целях определения достаточности и эффективности предписанных мер защиты информации и выявления нарушений.

6.6. При обнаружении нарушений норм и требований по защите информации администратор ИСПДн докладывает директору Учреждения для принятия решения о прекращении обработки ПДн и проведения соответствующих организационных и технических мер по устранению нарушения. Результаты контроля защиты информации оформляются актами либо в соответствующих журналах учета результатов контроля.

6.7. Ведение контроля защиты информации осуществляется путем проведения периодических, плановых и внезапных проверок объектов

защиты, которые проводятся, как правило, силами администратора ИСПДн, ответственного за обработку и защиту ПДн, комиссии по ПДн в соответствии с утвержденным планом или по согласованию с директором.

6.8. Одной из форм контроля защиты информации является обследование объектов ИСПДн. Оно проводится не реже одного раза в год рабочей группой в составе администратора ИСПДн, ответственного за обработку и защиту ПДн. Для обследования ИСПДн может привлекаться организация, имеющая лицензию ФСТЭК России на деятельность по технической защите информации.

6.9. Обследование ИСПДн проводится с целью определения соответствия помещений, технических и программных средств требованиям по защите и безопасности персональных данных.

6.10. В ходе обследования проверяется:

— соответствие текущих условий функционирования обследуемой ИСПДн условиям, сложившимся на момент проверки;
— соблюдение организационно-технических требований к помещениям, в которых располагается ИСПДн;
— сохранность печатей, пломб на технических средствах передачи и обработки информации, а также на устройствах их защиты, отсутствие повреждений экранов корпусов аппаратуры, оболочек кабелей и их соединений с шинами заземления;
— соответствие выполняемых на ИСПДн мероприятий по защите информации данным, изложенным в настоящем Положении;
— выполнение требований по защите информационных систем от несанкционированного доступа;
— выполнение требований по антивирусной защите.

6.11. Право проверки соблюдения условий использования средств защиты информации имеют директор Учреждения, ответственный за обработку и защиту информации, администратор ИСПДн.

6.12. Пользователю ИСПДн категорически запрещается обрабатывать конфиденциальную информацию с отключенными СЗИ, менять настройки СЗИ.

7. Правила защиты ИСПДн от вредоносного ПО

7.1. При использовании в ИСПДн средств антивирусной защиты и защиты от вредоносных программ выполняются следующие организационные меры:

– использование съемных носителей ПДн пользователя ИСПДн на других компьютерах только с механической защитой от записи;

- запрет на использование посторонних съемных носителей ПДн при работе в ИСПДн;
- запрет на передачу съемных носителей ПДн посторонним лицам;
- запрет на запуск программ с внешних съемных носителей информации при работе в ИСПДн;
- запрет на несанкционированное использование отчуждаемых носителей информации;
- использование в ИСПДн только дистрибутивов программных продуктов, приобретенных у официальных дилеров фирм-разработчиков этих продуктов;
- обязательная проверка всех программных продуктов;
- проверка всех программных файлов и файлов документов, полученных по электронной почте, специальными антивирусными средствами;
- систематическая проверка содержимого дисков файловых хранилищ обновленными версиями антивирусных программ;
- контроль и обновление списка разрешенных ссылок на веб-ресурсы сети Интернет.

7.2. Ответственность за эксплуатацию средств антивирусной защиты и защиты от вредоносных программ возлагается на администратора ИСПДн.

8. Требования по обеспечению безопасности при работе в сети Интернет

8.1. Доступ в сеть Интернет и другие глобальные сети пользователям предоставляется исключительно в целях повышения квалификации и выполнения ими своих трудовых обязанностей.

8.2. Пользователи ИСПДн могут использовать сети Интернет в качестве:

- транспортной среды при обмене информацией между несколькими территориально разнесенными элементами ИСПДн или другими информационными системами;
- средства предоставления открытой общедоступной информации внешнему абоненту;
- средства получения необходимой пользователям ИСПДн информации, содержащейся в сети Интернет или других корпоративных сетях.

8.3. Наименование структурного подразделения/должность может ограничивать доступ к ресурсам сети Интернет, содержание которых не имеет отношения к исполнению трудовых обязанностей, а также к ресурсам, содержание и направленность которых запрещены международным и российским законодательством, включая материалы, носящие вредоносную,

угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия, и т.д.

8.4. При работе с ресурсами в сети Интернет запрещается:

- разглашение конфиденциальной информации, ставшей известной работнику по трудовой необходимости либо иным путем;
- распространение защищаемых авторскими правами материалов, затрагивающих какой-либо патент, торговую марку, коммерческую тайну или прочие права собственности и/или авторские и смежные с ним права Учреждения и (или) третьей стороны;
- публикация, загрузка и распространение материалов, содержащих вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления НСД, а также размещение ссылок на вышеуказанную информацию;
- загрузка и запуск исполняемых либо иных файлов без предварительной проверки на наличие вирусов установленным антивирусным пакетом;
- использование анонимных прокси-серверов и серверов чужих виртуальных частных сетей (VPN);
- доступ к ресурсам сети Интернет, содержащим развлекательную (в том числе музыкальные, видео, графические и другие файлы, не связанные с производственной деятельностью), эротическую или порнографическую информацию.

8.5. Вся информация о ресурсах, посещаемых пользователем ИСПДн, протоколируется.

8.6. Администратор ИСПДн, ответственный за обработку и защиту ПДн обязаны проводить анализ использования ресурсов в сети Интернет и (в случае необходимости) представлять отчет об использовании Интернет-ресурсов пользователями ИСПДн руководителю структурного подразделения.

8.7. Использование личной почты в служебных целях запрещено.

9. Порядок обучения пользователей ИСПДн обеспечению безопасности ПДн

9.1. Перед началом работы в ИСПДн пользователи должны ознакомиться под личную роспись локальными нормативными актами, принятыми Учреждением в сфере обработки ПДн.

9.2. Систему внутреннего обучения сотрудников в области защиты ПДн составляет:

- самостоятельное изучение работниками необходимых для работы документов, средств и продуктов;
- обучение на курсах повышения квалификации в области защиты персональных данных.

9.3. В результате прохождения обучения работники получают необходимые знания и навыки в отношении:

- правил использования СЗИ;
- содержания основных нормативных правовых актов, руководящих и нормативно-методических документов в области обеспечения безопасности ПДн при их обработке в ИСПДн;
- основных мероприятий по организации и техническому обеспечению безопасности ПДн при их обработке в ИСПДн;
- планирования, организации и контроля выполнения мероприятий по обеспечению безопасности ПДн при их обработке в ИСПДн.

9.4. Пользователи должны продемонстрировать администратору ИСПДн или ответственному за обработку и защиту ПДн наличие необходимых знаний и умений для выполнения требований настоящего Положения.

9.5. Пользователи, демонстрирующие недостаточные знания и умения для обеспечения безопасности персональных данных в соответствии с требованиями настоящего Положения, к работе в ИСПДн не допускаются.

9.6. Ответственными за организацию обучения и оказание методической помощи являются администратор ИСПДн и ответственный за обработку и защиту ПДн.

9.7. При самостоятельном обучении работниками, осуществляющими обработку ПДн, самостоятельно изучаются (в части, их касающейся):

- руководящие и нормативно-методические документы в области обеспечения безопасности ПДн;
- правила и инструкции по использованию программных и аппаратных СЗИ;
- внутренние локальные нормативные акты, устанавливающие порядок обращения с ПДн и их защиты.

Время для самостоятельного изучения определяется начальниками соответствующих структурных подразделений.

10. Порядок проверки электронного журнала обращений к ИСПДн

10.1. Проверка электронного журнала обращений проводится с целью выявления несанкционированного доступа к защищаемой информации в ИСПДн.

10.2. Право проверки электронного журнала обращений имеют администратор ИСПДн, ответственный за обработку и защиту ПДн, директор Учреждения.

10.3. Проверка должна проводиться не реже, чем один раз в месяц с целью своевременного выявления фактов нарушения требований настоящего Положения.

10.4. Факты проверок электронных журналов отражаются в специальном журнале проверок. После каждой проверки администратор ИСПДн делает соответствующую отметку в журнале и ставит свою подпись.

11. Правила антивирусной защиты

11.1. К использованию на АРМ и в ИСПДн допускаются только лицензионные антивирусные средства, официально закупленные у поставщиков указанных средств.

11.2. Установка и начальная настройка средств антивирусного контроля осуществляется администратором ИСПДн.

11.3. Администратор ИСПДн осуществляет периодическое обновление антивирусных пакетов и контроль их работоспособности.

11.4. Ярлык для запуска антивирусной программы должен быть доступен всем пользователям ИСПДн.

11.5. Еженедельно в начале работы (после загрузки компьютера в автоматическом режиме) должен проводиться антивирусный контроль всех дисков и файлов компьютеров.

11.6. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях (магнитных дисках, лентах, CD-ROM и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

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

11.8. Устанавливаемое ПО должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки ПО администратором ИСПДн должна быть выполнена антивирусная проверка ИСПДн.

11.9. На АРМ запрещается установка ПО, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.

11.10. При возникновении подозрения на наличие компьютерного вируса пользователь самостоятельно или вместе с администратором ИСПДн должен провести внеочередной антивирусный контроль АРМ.

11.11. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

— приостановить обработку данных в ИСПДн;
— немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора ИСПДн, а также смежные подразделения, использующие эти файлы в работе;
— провести лечение или уничтожение зараженных файлов.

11.12. Ответственность за проведение мероприятий антивирусной защиты в конкретной ИСПДн и соблюдение требований настоящего Положения возлагается на администратора ИСПДн и всех пользователей ИСПДн.

12. Правила парольной защиты

12.1. Организационное и техническое обеспечение смены, прекращения действия паролей в ИСПДн, процессов генерации и использования возлагается в пределах их полномочий на работников ГБУК г. Москвы «Государственный выставочный зал истории войны в Афганистане» и администратора ИСПДн, сопровождающего механизмы идентификации и аутентификации (подтверждения подлинности) пользователей по значениям паролей.

12.2. При использовании паролей в ИСПДн выполняются следующие правила:

- пароли должны меняться с установленной периодичностью в соответствии с требованиями организационно-распорядительного документа Учреждения;
- пароль имеет не менее 8 символов и как содержит буквенные (заглавные и строчные), так и цифровые символы;
- обязательно применение индивидуальных паролей, применение групповых паролей не допускается;
- при создании пароля пользователя администратором

предусматривается возможность его автоматическое изменение самим пользователем после первого входа в ИСПДн;

- для предотвращения повторного использования паролей ведется их учет за предыдущие 12 месяцев;
- при вводе пароль не выдается на монитор компьютера в явном виде;
- рекомендуется использование возможностей операционной системы по контролю за периодичностью смены (не реже 1 раза в 3 месяца), составу символов и недопущению повторений паролей.

12.3. Контроль за действиями пользователей ИСПДн при работе с паролями возлагается на администратора ИСПДн и ответственного за обработку и защиту ПДн в пределах их полномочий.

12.4. При использовании паролей запрещается:

- использовать в качестве пароля свои имя, фамилию, дату рождения, имена родственников, кличку собаки и т. п., равно как и обычные слова;
- использовать в качестве пароля русское слово, введенное при нахождении клавиатуры в латинском регистре;
- использовать в качестве пароля легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ), а также общепринятые сокращения;
- использовать в качестве пароля "пустой" пароль - имя входа в систему, а также выбирать пароли, которые уже использовались ранее;
- использовать один и тот же пароль при загрузке АРМ и при работе в ИСПДн;
- записывать пароль на неучтённых бумажных носителях информации;
- разглашать кому бы то ни было свои персональные пароли доступа.

12.5. Владельцы паролей знакомятся с перечисленными требованиями организации парольной защиты с проставлением собственноручно подписи в листе ознакомления с соответствующей документированной процедурой и предупреждаются об ответственности за использование паролей, не соответствующих установленным требованиям, а также за разглашение парольной информации.

13. Правила обновления ИСПДн и АРМ

13.1. Настоящие правила регламентируют обеспечение безопасности информации при проведении обновления, модификации общесистемного и прикладного программного обеспечения, технического обслуживания и при возникновении нештатных ситуаций в работе ИСПДн.

13.2. Право внесения изменений в конфигурацию аппаратно-программных, системных и прикладных программных средств защищенных ИСПДн предоставляется по согласованию с директором: администратору ИСПДн и системному администратору.

13.3. Изменение конфигурации аппаратно-программных средств ИСПДн кем-либо, кроме вышеперечисленных уполномоченных сотрудников, запрещено.

13.4. Процедура внесения изменений в конфигурацию аппаратно-программных, системных и прикладных программных средств ИСПДн регламентируется соответствующими локальными нормативными актами.

13.5. Установка и обновление ПО (системного, тестового и т.п.) производится только с оригинальных лицензионных дистрибутивных носителей, полученных установленным порядком.

13.6. Все добавляемые программные и аппаратные компоненты должны быть предварительно установленным порядком проверены на работоспособность, а также отсутствие опасных функций.

13.7. С целью соблюдения принципа персональной ответственности за свои действия каждому пользователю ИСПДн должно быть сопоставлено персональное уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать на данном АРМ.

13.8. Использование несколькими пользователями ИСПДн одного и того же имени пользователя ("группового имени") запрещено.

14. Порядок уничтожения защищенной информации и ее носителей

14.1. Уничтожению в обязательном порядке подлежат поврежденные, выводимые из эксплуатации носители, содержащие защищаемую информацию, использование которых не предполагается в дальнейшем.

14.2. Уничтожению подлежат носители, содержащие защищаемую информацию, которые выводятся из эксплуатации в составе ИСПДн.

Не допускается уничтожение неисправных носителей и передача их в сервисный центр для ремонта. Такие носители должны уничтожаться в соответствии с настоящим порядком.

14.3. Уничтожение должно производиться по технологии, предусмотренной для данного типа носителя, с применением сертифицированных средств гарантированного уничтожения информации.

14.4. Уничтожение носителей производится путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления информации. Непосредственные

действия по уничтожению конкретного типа носителя должны быть достаточны для исключения возможности восстановления информации.

14.5. Бумажные и прочие сгораемые носители уничтожают с помощью любых бумагорезательных машин.

14.6. По факту уничтожения или стирания носителей составляется акт, в журналах учета делаются соответствующие записи.

14.7. Процедуры стирания и уничтожения осуществляются постоянно действующей Комиссией по ПДн.

15. Заключительные положения

15.1. Требования настоящего Положения обязательны для всех работников, допущенных к обработке ПДн.

15.2. Нарушение требований настоящего Положения влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

_____