Приложение 10
к приказу ГБОУ ОЦДиК
от 29.12.2017 г.№ 245

Инструкция
администратора безопасности информационных систем персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий документ разработан в соответствии с нормативными документами по безопасности информации и определяет порядок обеспечения безопасности информации при проведении работ администратором безопасности (далее – АБ) в информационных системах персональных данных (далее – ИСПДн) ГБОУ «Областной центр диагностики и консультирования» (далее – Учреждение).

1.2. Субъектами доступа к ресурсам ИСПДн являются пользователи, АБ и обслуживающий персонал (работники, осуществляющие техническое обслуживание, ремонт), в соответствии с утвержденным перечнем.

1.3. Обрабатываемая в ИСПДн информация относится к сведениям, составляющим персональные данные (далее – ПДн).

1.4. Машинные носители с защищаемой информацией имеют пометку «ПДн».

1.5. АБ назначается Приказом Директора Учреждения и получает неограниченные права на доступ к ресурсам ИСПДн.

1.6. АБ осуществляет общее руководство и контроль за обеспечением безопасности информации при работе пользователей ИСПДн и обслуживающего персонала.

1.7. Методическое руководство по информационной безопасности объектов информатизации осуществляет АБ.

1.8. АБ имеет право вносить предложения по изменению и дополнению данной Инструкции, а также «Инструкции пользователя…» и «Инструкции обслуживающего персонала…».

1.9. Изменения и дополнения к данной Инструкции утверждаются в установленном порядке.

1.10. Право толкования положений настоящей Инструкции возлагается на Директора Учреждения.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. Доступ к информации – возможность получения информации и ее использования.

2.2. Защита информации – деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на информацию, то есть процесс, направленный на достижение информационной безопасности.

2.3. Информация – сведения (сообщения, данные) независимо от формы их представления.

2.4. Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.5. Несанкционированный доступ – доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т. д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т. д. различных организаций путем изменения (повышения, фальсификации) своих прав доступа.

2.6. Носитель информации – любой материальный объект или среда, используемый для хранения или передачи информации.

2.7. Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

2.8. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу.

2.9. Средство защиты информации – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

2.10. Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

3. ТРЕБОВАНИЯ К АБ

3.1. АБ обязан знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций и распоряжений, регламентирующих порядок действий по защите информации.

3.2. АБ, не ознакомленный с данной Инструкцией, а также с изменениями и дополнениями к ней, к работе с ресурсами ИСПДн не допускается.

3.3. АБ осуществляет учет съемных машинных носителей информации, их уничтожение, либо контроль процедуры их уничтожения.

3.4. АБ обязан немедленно реагировать на сообщения пользователей о любых неисправностях в работе основных и вспомогательных средств и систем (далее – ОТСС и ВТСС), СЗИ, системного и прикладного программного обеспечения (далее – ПО) ИСПДн.

3.5. АБ обязан немедленно ставить в известность ответственного за обеспечение безопасности персональных данных Учреждения обо всех неисправностях аппаратно-программных средств ИСПДн.

3.6. АБ обязан ставить в известность ответственного за обеспечение безопасности персональных данных Учреждения о необходимости проведения работ по

администрированию СЗИ.

3.7. АБ имеет право проводить внеплановые проверки работоспособности СЗИ и соблюдения пользователями технологии обработки персональных данных.

3.8. АБ разрабатывает планы мероприятий по администрированию и техническому обслуживанию аппаратных и программных средств ИСПДн Учреждения.

3.9. АБ обязан в случае отказа технических средств или программного обеспечения элементов ИСПДн, в том числе СЗИ, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

3.10. АБ имеет право требовать прекращения обработки персональных данных, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн или средств защиты.

3.11. АБ присутствует при выполнении технического обслуживания элементов ИСПДн сторонними специалистами на территории Учреждения.

3.12. АБ осуществляет разбирательства и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с техническими и программными средствами ИСПДн, в том числе с СЗИ, или по другим нарушениям, которые могут привести к снижению уровня защищенности персональных данных.

3.13. В ходе управления (администрирования) системой защиты ИСПДн АБ обязан осуществлять:

3.13.1. заведение и удаление учетных записей пользователей, управление полномочиями пользователей ИСПДн и поддержание правил разграничения доступа в ИСПДн;

3.13.2. создание, присвоение и уничтожение идентификаторов пользователей и устройств, однозначно их идентифицирующих;

3.13.3. управление СЗИ в ИСПДн, в том числе параметрами настройки программного обеспечения, включая программное обеспечение СЗИ, управление учетными записями пользователей, восстановление работоспособности СЗИ, генерацию, смену и восстановление паролей;

3.13.4. изменение аутентификационной информации (средств аутентификации), заданной их производителями и (или) используемой при внедрении системы защиты информации ИСПДн;

3.13.5. установку обновлений программного обеспечения, включая программное обеспечение СЗИ, выпускаемых разработчиками (производителями) СЗИ или по их поручению;

3.13.6. централизованное управление системой защиты информации ИСПДн (при необходимости);

3.13.7. регистрацию и анализ событий в ИСПДн, связанных с защитой информации;

3.13.8. информирование пользователей об угрозах безопасности информации, о правилах эксплуатации системы защиты информации ИСПДн и отдельных СЗИ, а также

их обучение;

3.13.9. сопровождение функционирования системы защиты информации ИСПДн в ходе ее эксплуатации, включая корректировку эксплуатационной документации на нее и организационно-распорядительных документов по защите информации.

3.14. В ходе выявления инцидентов и реагирования на них АБ обязан осуществлять:

3.14.1. обнаружение и идентификацию инцидентов, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, программного обеспечения и СЗИ, нарушений правил разграничения доступа, неправомерных действий по сбору информации, внедрений вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

3.14.2. своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в ИСПДн;

3.14.3. анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;

3.14.4. планирование и принятие мер по устранению инцидентов, в том числе по восстановлению ИСПДн и ее сегментов в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

3.14.5. планирование и принятие мер по предотвращению повторного возникновения инцидентов.

3.15. В ходе контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в ИСПДн, АБ обязан осуществлять:

3.15.1. анализ и оценку функционирования системы защиты информации ИСПДн, включая выявление, анализ и устранение недостатков в функционировании системы защиты информации ИСПДн;

3.15.2. проверку работоспособности и параметров настройки программного обеспечения, аппаратных и программных СЗИ ИСПДн;

3.15.3. проверку состава технических средств, программного обеспечения и СЗИ;

3.15.4. контроль целостности печатей (пломб, наклеек) технических средств, используемых для обработки персональных данных;

3.15.5. еженедельное отслеживание появления новых видов уязвимостей ПО ИСПДн. По необходимости АБ производит устранение уязвимостей согласно рекомендациям разработчика, в том числе путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств. В качестве источников информации об уязвимостях должны использоваться опубликованные данные разработчиков средств защиты информации, общесистемного, прикладного и специального программного обеспечения, технических средств, а также другие базы данных уязвимостей;

3.15.6. периодический анализ изменения угроз безопасности информации в ИСПДн, возникающих в ходе ее эксплуатации, и принятие мер защиты информации в случае возникновения новых угроз безопасности информации;

3.15.7. контроль за событиями безопасности и действиями пользователей в ИСПДн. В частности, АБ обязан осуществлять постоянный контроль за выполнением пользователями установленного комплекса мероприятий по обеспечению безопасности информации;

3.15.8. контроль (анализ) защищенности информации, содержащейся в ИСПДн;

3.15.9. документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в ИСПДн;

3.15.10.принятие решения по результатам контроля (мониторинга) за обеспечением уровня защищенности информации о доработке (модернизации) системы защиты информации ИСПДн, повторной аттестации ИСПДн или проведении дополнительных аттестационных испытаний.

4. ДОСТУП К РЕСУРСАМ ИСПДН

4.1. Обязательными условиями получения доступа к ресурсам ИСПДн АБ являются:

- право доступа в помещение;
- наличие допуска к персональным данным;
- право доступа к ИСПДн;
- знание технологии обработки информации в ИСПДн с учетом требований информационной безопасности.

4.2. Идентификация АБ в ИСПДн осуществляется по уникальному имени и персональному идентификатору (при его наличии).

4.3. Длина пароля АБ и всех пользователей – не менее 6 буквенно-цифровых символов.

4.4. Уникальное имя, персональный идентификатор (при его наличии) и пароль АБ получает в установленном порядке. АБ обязан их помнить и не допускать раскрытия, не допускается запись на каких-либо носителях в целях напоминания. Во время ввода пароля на клавиатуре должна быть исключена возможность его просмотра другими лицами. Не допускается оставление без присмотра и передача другим лицам персонального идентификатора (при его наличии).

4.5. При утере или подозрении на утечку своего имени, пароля или персонального идентификатора АБ должен немедленно изменить свои идентификационные данные и проконтролировать возможные изменения в настройках СЗИ.

4.6. Регистрация пользователя осуществляется АБ в соответствии с «Инструкцией по организации парольной защиты» и состоит в определении имени регистрируемого пользователя, присвоении ему персонального идентификатора (при его наличии) и назначении пароля.

4.7. При заведении новой учетной записи, АБ должен проверить личность пользователя и его трудовые обязанности.

4.8. Пересмотр и, при необходимости, корректировка учетных записей пользователей производится АБ не реже одного раза в 6 месяцев и по мере необходимости.

4.9. Предоставление пользователям прав доступа к объектам доступа ИСПДн должно осуществляться на основании задач, решаемых пользователями.

4.10. АБ не имеет права требовать у пользователей раскрытия их паролей, а также передачи ему персональных идентификаторов (при их наличии), кроме случая изменения идентификационных данных.

4.11. АБ имеет право требовать у пользователя изменения его пароля, но не имеет права самостоятельно изменять его пароль.

5. ПОРЯДОК РАБОТЫ АБ С РЕСУРСАМИ ИСПДН

Ниже приводится перечень работ, производимых АБ с ресурсами ИСПДн.

5.1. Проверка работоспособности и настройка системы доступа к ресурсам ИСПДн

АБ присваивает пользователям идентификационные данные к ресурсам ИСПДн. При этом должны выполняться следующие требования:

- АБ определяет политику изменения учетных данных пользователей и периодически контролирует ее соблюдение;
- АБ сообщает пользователю его уникальное имя и предоставляет возможность задать пароль, далее кодирует персональный идентификатор (при его наличии) пользователя;
- изменение учетных данных пользователя производится АБ по требованию ответственного за обеспечение безопасности персональных данных Учреждения, а также периодически по утвержденному плану и в случае увольнения работника;
- АБ имеет право в целях тестирования уязвимости системы доступа (выявление простейших паролей) производить попытки взлома паролей пользователей, если попытка взлома была успешной, АБ обязан потребовать у пользователя изменение пароля.

5.2. Проверка работоспособности и настройка аппаратных и программных средств защиты информации (СЗИ)

АБ обязан перед началом работ включить и убедиться в работоспособности аппаратных СЗИ, в случае сбоя – работы прекратить.

В случае сбоя СЗИ, таких, как неправильная идентификация пользователей, АБ обязан приостановить обработку защищаемой информации до устранения неисправности. В случае производственной необходимости – отключить СЗИ и лично контролировать проведение работ пользователями.

5.3. Антивирусная защита ресурсов ИСПДн

АБ разрабатывает и контролирует реализацию антивирусной политики, а именно:

- настраивает параметры антивирусной программы;

- контролирует работоспособность антивирусной программы;
- немедленно реагирует на сообщения пользователей о подозрительном поведении ПО, а также о появлении любых сообщений антивирусной программы и принимает соответствующие меры;
- имеет право на проведение внеплановой проверки на наличие вирусов;
- периодически (один раз в неделю) контролирует корректность процесса обновления антивирусных баз, а также исполняемых модулей антивирусной программы.

5.4. Хранение дистрибутивов программного обеспечения СЗИ

АБ должен хранить дистрибутивы программного обеспечения СЗИ и прикладного программного обеспечения, установленного в ИСПДн Учреждения в месте, исключающем доступ посторонних лиц.

5.5. Проверка целостности системного и прикладного ПО

Контролю целостности подлежат файлы ПО ИСПДн с расширениями: *.exe, *.com, *.dll, *.sys, *.vxd, *.drv из каталогов: Windows, Program Files.

5.6. Резервное копирование и восстановление информации

Резервное копирование производится регулярно с заданной периодичностью, а также в случае производственной необходимости. При этом необходимо выполнять следующие требования:

- обязательное резервное копирование производится в случае обнаружения неисправностей в работе ПЭВМ или отчуждаемых машинных носителей (далее – МН);
- допускается обоснованное внеплановое резервное копирование информации как по инициативе пользователя, так и АБ, если это не нарушает технологию обработки информации;
- резервные копии пользовательской информации и информации операционной системы хранятся на учтенных внешних МН;
- ответственным лицом за хранение резервных копий является АБ.

По мере устранения неисправностей ПЭВМ АБ производит восстановление информации ограниченного доступа с резервных копий.

Восстановление работоспособности (правильности функционирования) и параметров настройки программного обеспечения и средств защиты информации (при необходимости), производится, в том числе с использованием резервных копий и (или) дистрибутивов.

АБ разрешаются действия в обход установленных процедур идентификации и аутентификации, необходимые только для восстановления функционирования информационной системы в случае сбоев в работе или выходе из строя отдельных технических средств (устройств).

5.7. Конфигурирование ИСПДн

Конфигурационной единицей являются услуги, оборудование, программное обеспечение, здания, люди, документы и пр.

Управление изменениями конфигурации осуществляет ответственный за обеспечение безопасности. Планирование реализации и непосредственно реализация необходимых изменений возлагается на АБ.

В ходе управления конфигурацией аттестованной информационной системы и ее системы защиты информации АБ обязан осуществлять:

– поддержание конфигурации ИСПДн и ее системы защиты информации (структуры системы защиты информации ИСПДн, состава, мест установки и параметров настройки СЗИ, программного обеспечения и технических средств) в соответствии с эксплуатационной документацией на систему защиты информации (поддержание базовой конфигурации ИСПДн и ее системы защиты информации);

– управление изменениями базовой конфигурации ИСПДн и ее системы защиты информации, в том числе определение типов возможных изменений базовой конфигурации ИСПДн и ее системы защиты информации, санкционирование внесения изменений в базовую конфигурацию ИСПДн и ее системы защиты информации, документирование действий по внесению изменений в базовую конфигурацию ИСПДн и ее системы защиты информации, сохранение данных об изменениях базовой конфигурации ИСПДн и ее системы защиты информации, контроль действий по внесению изменений в базовую конфигурацию ИСПДн и ее системы защиты информации;

– анализ потенциального воздействия планируемых изменений в базовой конфигурации ИСПДн и ее системы защиты информации на обеспечение защиты информации, возникновение дополнительных угроз безопасности информации и работоспособность ИСПДн;

– определение параметров настройки программного обеспечения, включая программное обеспечение СЗИ, состава и конфигурации технических средств и программного обеспечения до внесения изменений в базовую конфигурацию ИСПДн и ее системы защиты информации;

– внесение информации (данных) об изменениях в базовой конфигурации ИСПДн и ее системы защиты информации в документацию на систему защиты информации ИСПДн;

– принятие решения по результатам управления конфигурацией о повторной аттестации ИСПДн или проведении дополнительных аттестационных испытаний.

Обязанности по управлению изменениями в аппаратном и программном обеспечении и всех элементах документации, которые связаны с работой, поддержкой и сопровождением систем, находящихся в эксплуатации, возлагаются на АБ. При возникновении необходимости изменения конфигурации ИСПДн, аттестованной по требованиям безопасности информации, АБ согласовывает планируемые изменения с предприятием-лицензиатом, проводившим аттестационные испытания.

5.8. Вывод ресурсов ИСПДн из эксплуатации

При невозможности ремонта различных ресурсов ИСПДн АБ обязан:

- физически уничтожать любые МН, независимо от содержащейся на них

информации; картриджи принтера, иные комплектующие могут быть использованы за пределами ИСПДн;

- факт выхода из строя и замены оборудования должен быть отражен в Техническом паспорте на ИСПДн.

5.9. Реагирование на сбои при регистрации событий безопасности

Реагирование на сбои при регистрации событий безопасности осуществляется АБ путем изменения параметров сбора, записи и хранения информации о событиях безопасности в журналах СЗИ от НСД, в том числе отключение записи информации о событиях безопасности от части компонентов ИСПДн, запись поверх устаревших хранимых записей событий безопасности.

В случае выявления признаков инцидентов безопасности, АБ обязан:

- немедленно уведомить Директора о данном факте;
- по возможности в максимально сжатые сроки установить причину возникновения инцидента и исключить возможность его повторения;
- восстановить работоспособность ИСПДн;
- по окончании работ по восстановлению работоспособности ИСПДн произвести запись в соответствующих журналах.

6. ДЕЙСТВИЯ ПРИ ОБНАРУЖЕНИИ ПОПЫТОК НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

6.1. К попыткам несанкционированного доступа относятся:

- сеансы работы с ИСПДн незарегистрированных пользователей, пользователей, нарушивших установленную периодичность доступа, или срок действия полномочий которых истек, или превышающих свои полномочия по доступу к данным;
- действия постороннего лица, пытающегося получить доступ (или уже получившего доступ) к ИСПДн, при использовании учетной записи администратора или другого пользователя ИСПДн, методом подбора пароля, использования пароля, разглашенного владельцем учетной записи или любым другим методом.

6.2. При выявлении факта несанкционированного доступа АБ обязан:

- пресечь дальнейший несанкционированный доступ к ИСПДн;
- доложить ответственному за обеспечение безопасности персональных данных Учреждения служебной запиской о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях;
- известить руководителя структурного подразделения, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка несанкционированного доступа, о факте несанкционированного доступа.

7. ОТВЕТСТВЕННОСТЬ

7.1. АБ несет персональную ответственность за:

- сохранность носителей информации и содержащейся на них информации в

рабочее время;

- несоблюдение требований данной Инструкции и неправомерное использование ресурсов ИСПДн;
- средства защиты информации, применяемые в ИСПДн Учреждения;
- качество проводимых работ по обеспечению безопасности персональных данных и за все действия, совершенные от имени учетной записи АБ в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования учетной записи.

7.2. АБ при нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несет дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.