Приложение №3

к приказу от 01.07.2021 г. №31-од
МБДОУ №83 «Винни-Пух»

ИНСТРУКЦИЯ
администратора информационной безопасности объекта информатизации «Информационная система персональных данных»

Настоящая инструкция определяет права и обязанности администратора информационной безопасности (ИБ) на объекте информатизации «Информационная система персональных данных» (далее - ИСПДн).

1. Общие положения:

Администратор ИБ ИСПДн организует выполнение мероприятий по защите информации в ИСПДн, осуществляет контроль за выполнением пользователями ИСПДн требований нормативных документов по защите информации, обеспечивает контроль за сохранностью защищаемой информации, настройку СЗИ от НСД в соответствии с разрешительной системой и матрицей доступа, при автоматизированной обработке защищаемой информации;

Администратор ИБ ИСПДн назначается приказом директора ГБУ РК «ЦСО Белогорского района» из числа штатных сотрудников, имеющих оформленное разрешение на доступ к защищаемой информации и обладающий достаточным уровнем квалификации в области администрирования автоматизированных систем обработки данных;

В практической деятельности Администратор ИБ ИСПДн руководствуется:

- Федеральным законом «Об информации, информационных технологиях и о защите информации» от 08.06.2006 г. № 149-ФЗ;
- Федеральным законом «О безопасности» от 5.03.1992 г. № 2446-I;
- Федеральным законом «О персональных данных» от 27 июля 2006 г. №152-ФЗ;
- Положением о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам», введенное в действие постановлением Правительства Российской Федерации от 15.09.1993 г. № 912-51.
- Положением по аттестации объектов информатизации по требованиям безопасности информации», Гостехкомиссия России, 1994 г;

– Положением о сертификации продукции по требованиям безопасности информации», Гостехкомиссия России, 1994 г;
– Специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР-К)», Гостехкомиссия России, 2002 г;
– ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью;
– Международным стандартом ИСО/МЭК 27001-2005 Информационные технологии. Методы защиты. Системы менеджмента защиты информации. Требования;
– ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы воздействующие на информацию. Общие положения;
– ГОСТ Р 51583-2000 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения;
– ГОСТ Р 50922-2006 Защита информации. Основные термины и определения;
– ГОСТ Р ИСО/МЭК 13335 Информационная технология. Методы и средства обеспечения безопасности;
– ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации;
– Основными мероприятиями по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационной системе персональных данных, утверждены заместителем директором ФСТЭК России 15 февраля 2008 г;
– Базовой моделью угроз безопасности персональных данных при их обработке в информационной системе персональных данных, утверждена заместителем директора ФСТЭК России 15 февраля 2008 г;
– Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационной системе персональных данных, утверждена заместителем директора ФСТЭК России 14 февраля 2008 г;
– Рекомендации по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных, утверждены заместителем директора ФСТЭК России 15 февраля 2008 г;
– РД Гостехкомиссии РФ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации, Гостехкомиссия России, 1992 г;
– РД Гостехкомиссии РФ. Защита от несанкционированного доступа к информации. Термины и определения. 1992 г;
– РД Гостехкомиссии РФ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. 1997 г;

- РД Гостехкомиссии РФ. Защита от несанкционированного доступа к информации Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей, Гостехкомиссия России, Москва, 1999 г;
- РД Гостехкомиссии РФ. «Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации» 1992 г;
- РД Гостехкомиссии РФ. «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» 1992 г;
- Инструкцией об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну. Введена в действие приказом от 13 июня 2001 года №152 (ФАПСИ);
- Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), введено приказом ФСБ РФ от 9 февраля 2005 г. № 66;
- Требованиями к средствам криптографической защиты конфиденциальной информации, ФСБ РФ, Москва;
- Методическими рекомендациями по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационной системе персональных данных с использованием средств автоматизации, утвержденные руководством 8 Центра ФСБ России 21 февраля 2008 г., №149/54-144;
- Типовыми требованиями по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационной системе персональных данных, ФСБ России, №149/5/6-622.
- другими нормативными документами ФСБ России, ФСТЭК (Гостехкомиссии) России по защите информации;
- приказами и распоряжениями директора ГБУ РК «ЦСО Белогорского района» ;

Настоящая инструкция корректируется и дополняется установленным порядком.

2. Функции администратора ИБ ИСПДН

Основными функциями Администратора ИБ ИСПДн являются:

Организация работ по предотвращению несанкционированного, непреднамеренного и неправомерного доступа лиц к защищаемой

информации;

Выявление возможных каналов утечки защищаемой информации в процессе деятельности директора ГБУ РК «ЦСО Белогорского района» и функционирования ИСПДн, внесение предложений по их закрытию;

Обеспечение режима конфиденциальности при автоматизированной обработке защищаемой информации в ИСПДн;

Установка, настройка, диагностика и поддержание в исправном состоянии технических и программных средств ИСПДн;

Регистрация пользователей в системе с присвоением каждому из них полномочий по доступу к ресурсам ИСПДн, изменение полномочий в случае необходимости для выполнения ими своих функциональных обязанностей;

Анализ содержимого системного журнала и журнала СЗИ, контроль соответствия действий пользователей с заданиями на работы и утвержденной технологией, контроль правильности ведения журналов пользователями;

Резервное копирование системной и пользовательской информации ИСПДн, ведение двух копий программного средства СЗИ от НСД, их периодическое тестирование и контроль работоспособности;

Обновление общесистемного и прикладного программного обеспечения ИСПДн, проверка целостности данных;

Периодическая (в соответствии с заданием ответственного за защиту информации) проверка системы на отсутствие вирусов.

3. Обязанности администратора ИБ ИСПДН

Администратор ИБ ИСПДн обязан:

Четко знать и выполнять требования действующих нормативных и руководящих документов ФСТЭК (Гостехкомиссии) России, а также внутренних инструкций, руководств по защите информации (ЗИ) и распоряжений, регламентирующих порядок действий по ЗИ;

Совместно с ответственным за ЗИ в ИСПДн организовывать разработку и обеспечивать проведение мероприятий по ЗИ при ее обработке в ИСПДн;

Обеспечивать сохранность эталонных вариантов общесистемного, прикладного и специального ПО ИСПДн;

В случаях неисправности или нарушения целостности СЗИ от НСД, выявления попыток НСД к защищаемой информации, либо обнаружения следов вскрытия ТС входящих в ИСПДн - действовать в соответствии с «Инструкцией по действиям персонала в нештатных ситуациях на объекте информатизации»;

В случае выявления каких-либо неквалифицированных действий пользователей, не несущих в себе угроз для безопасности информации, поставить в известность ответственного за ЗИ в ИСПДн, временно заблокировать возможность работы этого пользователя и организовать с ними дополнительные занятия;

Регулярно выполнять работу по администрированию СЗИ от НСД

ИСПДн, проверять данные в системном журнале СЗИ от НСД, в случае необходимости распечатывать системные журналы СЗИ от НСД. В случае выявления попыток НСД к защищаемой информации, представлять данный журнал ответственному за ЗИ в ИСПДн;

Производить настройку СЗИ от НСД (систем управления доступом, системы регистрации запуска программ, предназначенных для обработки защищаемой информации, систему регистрации попыток доступа программных средств к защищаемым файлам, систему регистрации попыток доступа к другим защищаемым объектам доступа (внешним устройствам ПЭВМ, каталогам, файлам и т.п.) в соответствии с разрешительной системой и матрицей доступа в ИСПДн;

Производить настройку полномочий пользователей ИСПДн в соответствии с заявками на наделение правами доступа и матрицей доступа;

Присваивать учетной записи пользователя средствами СЗИ от НСД первоначальный пароль. Сообщать его пользователю под роспись при первичном доступе к ИСПДн;

Регулярно, не реже 1 раза в квартал ознакамливать с результатами администрирования ответственного за ЗИ в ИСПДн;

Настраивать систему контроля регулярной смены паролей и систему контроля длины используемого пароля в соответствии с «Инструкцией по организации парольной защиты на объекте информатизации»;

Регулярно производить смену личного пароля доступа (не реже 1 раза в 6 месяцев) в соответствии с «Инструкцией по организации парольной защиты на объекте информатизации» с записью факта смены пароля (дата и время изменения пароля) в журнале учета профилактических работ. Запрещается сообщать кому - либо свой пароль доступа к ИСПДн, за исключением случая передачи обязанностей Администратора ИБ ИСПДн, в том числе и экстренное (отпуск, командировка, болезнь и т.д.), другому лицу в соответствии с приказом директора ГБУ РК «ЦСО Белогорского района» ;

При увольнении или переводе пользователей в другие подразделения оперативно изменять учетные реквизиты защиты пользователей: пароли, логины;

При изменении программной среды или персонала ИСПДн производить тестирование всех функций СЗИ от НСД с помощью сертифицированных ФСТЭК (Гостехкомиссией) России программных средств тестирования;

Не реже одного раза в квартал проводить обязательное плановое тестирование всех функций СЗИ от НСД с помощью сертифицированных ФСТЭК (Гостехкомиссией) России программных средств тестирования;

В случае необходимости обновлять эксплуатируемое, либо устанавливать новое ПО в соответствии с «Инструкцией по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств на объекте информатизации»;

Проверять все новые данные на отсутствие вирусов и регулярно

обновлять базы данных антивирусных средств в соответствии с «Инструкцией по организации антивирусной защиты на объекте информатизации»;

Иметь в наличии резервные копии программных средств СЗИ от НСД в соответствии с положениями эксплуатационной документации и лицензионных условий производителя СЗИ от НСД. Оригинал программного средства СЗИ от НСД (дистрибутив) хранить в опечатанном сейфе, текущую работу с СЗИ от НСД производить с использованием копии;

Проводить работу по повышению квалификации пользователей ИСПДн и обучению правилам и порядку работы со средствами защиты информации, в том числе на основе специально разрабатываемых для этой цели инструкций, памяток, и других документов;

Организовывать и проводить разъяснительную и профилактическую работу в подразделениях по изучению требований нормативных и руководящих документов по ЗИ, по порядку проведения работ в ИСПДн и ответственности за сохранение защищаемой информации;

Осуществлять контроль за выполнением руководящих документов по ЗИ при автоматизированной обработке защищаемой информации и соблюдением этих требований исполнителями работ;

В случае возникновения каких-либо нештатных ситуаций действовать в соответствии с «Инструкцией по действиям персонала в нештатных ситуациях на объекте информатизации».

4. Порядок действий Администратора ИБ ИСПДН при работе:

4.1. Общие положения:

4.1.1 Обработка защищаемой информации при выполнении функций по администрированию СЗИ от НСД Администратору ИБ ИСПДн строго запрещается;

4.1.2 Обработка защищаемой информации должна осуществляться с использованием отдельных учетных реквизитов (персонального идентификатора, персональной учетной записи и индивидуального пароля с пользовательскими привилегиями);

4.1.3 Работа с СЗИ от НСД осуществляется в соответствии с «Руководством администратора» комплекта документации на СЗИ от НСД;

4.1.4 При компрометации учетных данных (утеря персонального

4.1.5 Идентификатора, логина и пароля) Администратора ИБ ИСПДн, любая работа в ИСПДн должна быть НЕМЕДЛЕННО прекращена, а ответственный за ЗИ в ИСПДн должен быть поставлен об этом в известность.

4.2. Общий порядок работы:

4.2.1. Получить начальный персональный идентификатор, логин и пароль под роспись в журнале учета работ, в случае первого входа в ИСПДн;

4.2.2. Выполнить другие предусмотренные организационные мероприятия по ЗИ;

4.2.3. Убедиться в целостности и сохранности маркировок (наклеек) и/или печатей на корпусе системного блока ТС ИСПДн (системный

блок должен быть опечатан Администратором ИБ ИСПДн или Ответственным за ЗИ в ИСПДн);

4.2.4. Включить ТС ИСПДн, убедиться в исправности и нормальном функционировании. При появлении приглашения к идентификации пользователя ввести имя административной учетной записи и пароль доступа и нажать клавишу <Enter>;

4.2.5. Выполнить работу согласно заданию;

4.2.6. В случае необходимости, сделать записи в журналах учета нештатных ситуаций и учета выполнения профилактических работ, фактов вскрытия и опечатывания ПЭВМ, установки и модификации аппаратных и программных средств защищенных ПЭВМ информационной системы;

4.2.7. Выключить ТС ИСПДн.

4.3. Порядок администрирования работы ИСПДн:

4.3.1. Выполнить действия согласно п.п. 4.2.1. – 4.2.4;

4.3.2. Загрузить оболочку администратора СЗИ от НСД;

4.3.3. Произвести анализ неизменности списка пользователей ИСПДн;

4.3.4. Тщательно проанализировать записи системных журналов о попытках НСД.

4.3.5. При обнаружении любых фактов (попыток) НСД к информации, действовать в соответствии с п.п. 3.4;

4.3.6. Тщательно проанализировать настройки систем разграничения доступа к объектам доступа ИСПДн;

4.3.7. Выполнить контроль целостности программного обеспечения СЗИ от НСД и ПО ИСПДн;

4.3.8. Тщательно проанализировать и убедится в неизменности программной среды ИСПДн. В ИСПДн должны отсутствовать средства разработки и отладки программ, а также средства отладки объектного кода программ;

4.3.9. В случае необходимости произвести тестирование всех функций СЗИ от НСД с помощью сертифицированных ФСТЭК

4.3.10. (Гостехкомиссией) России программных средств тестирования;

4.3.11. При необходимости произвести очистку системных журналов;

4.3.12. Выполнить действия согласно п.п. 4.2.6 – 4.2.7.

4.4. Порядок модификации или установки нового ПО:

4.4.1 Установка (переустановка), изменение ПО ИСПДн выполняется с соответствии с п. 1.3 настоящей инструкции, а также согласно «Инструкции по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств на объекте информатизации»;

4.4.2 Выполнить действия согласно п.п. 4.2.1 – 4.2.4;

4.4.3 Произвести установку (обновление, изменение) программного обеспечения в соответствии с документацией на

нее;

4.4.4 Провести тестирование всех функций СЗИ от НСД с помощью сертифицированных ФСТЭК (Гостехкомиссией) России программных средств тестирования.

4.4.5 Выполнить действия согласно п.п. 4.2.6 – 4.2.7.

4.5. Действия в случае утери учетных данных (идентификатор, логин, пароль) пользователя:

4.5.1 НЕМЕДЛЕННО остановить любые работы в ИСПДн, поставить в известность ответственного за ЗИ в ИСПДн;

4.5.2 Выполнить администрирование ИСПДн в соответствии с п. 4.3;

4.5.3 Удалить запись о пользователе, соответствующую утерянным учетным данным;

4.5.4 Создать нового пользователя с использованием других учетных данным. Установить полномочия пользователя в соответствии с разрешительной системой и матрицей доступа. Настроить системы разграничения доступа пользователя к объектам доступа ИСПДн;

4.5.5 Провести тестирование всех функций СЗИ от НСД с помощью сертифицированных ФСТЭК (Гостехкомиссией) России программных средств тестирования;

4.5.6 Выполнить действия согласно п.п. 4.2.6 – 4.2.7.

4.6. Удаление защищаемой информации:

4.6.1 Отбор и удаление документированной защищаемой информации на учтенных машинных носителях информации производится комиссионно в составе: Администратор ИБ ИСПДн, ответственный за ЗИ в ИСПДн и пользователь/оператор, отвечающий за обновление (обработку) данной информации;

4.6.2 Выполнить действия согласно п.п. 4.2.1 – 4.2.4;

4.6.3 Определить информацию, подлежащую стиранию;

4.6.4 Удалить эту информацию;

4.6.5 Составить акт об уничтожении конфиденциальной информации (комиссионно).

4.6.6 Выполнить действия согласно п.п. 4.2.6 – 4.2.7.

4.7. Порядок регистрации нового пользователя и настройки полномочий пользователей ИСПДн:

4.7.1. Допуск (регистрация) нового пользователя ИСПДн осуществляется согласно «Инструкции по внесению изменений в списки пользователей и наделению их полномочиями доступа к ресурсам ИСПДн, а также с п.п. 3.7 и 3.8 настоящей инструкции;

4.7.2. Выполнить действия согласно п.п. 4.2.1 – 4.2.4;

4.7.3. Создать нового пользователя (зарегистрировать);

4.7.4. Установить полномочия пользователя в соответствии с разрешительной системой и матрицей доступа. Настроить системы разграничения доступа пользователя к объектам доступа ИСПДн;

4.7.5. В случае необходимости (изменения программной среды или персонала ИСПДн) провести тестирование всех функций СЗИ от НСД с помощью сертифицированных ФСТЭК (Гостехкомиссией) России программных средств тестирования;

4.7.6. Выдать пользователю его идентификатор (присвоить логин), первоначальный пароль под роспись с указанием даты выдачи;

4.7.7. Выполнить действия согласно п.п. 4.2.6 – 4.2.7.

5. Администратору ИБ ЗАПРЕЩАЕТСЯ:

Передавать (сообщать каким-либо образом) кому-либо свой персональный идентификатор, логин и пароль доступа (за исключением случая приема - передачи обязанностей Администратора ИБ ИСПДн другому лицу, на основании приказа директора ГБУ РК «ЦСО Белогорского района» ;

Оставлять работающие ТС ИСПДн, без блокировки консоли;

Передавать работающие ТС ИСПДн другому пользователю без перезагрузки.