

Муниципальное образовательное учреждение
Чебаковская средняя общеобразовательная школа

П Р И К А З

11.05.2010

№ 45/ 01-12

ПРИКАЗ

**Об утверждении эксплуатационной
документации ИСПДн**

В целях исполнения Федерального закона №152-ФЗ от 27 июля 2006 года «О персональных данных» приказываю:

ПРИКАЗЫВАЮ:

Утвердить прилагаемые эксплуатационные документы ИСПДн МОУ Чебаковская СОШ

1. Журнал учета мероприятий по контролю над соблюдением режима защиты персональных данных (Приложение 1);
2. План внутренних проверок режима защиты персональных данных (Приложение 2);
3. Журнал учета обращений субъектов персональных данных о соблюдении их законных прав, при обработке персональных данных в ИСПДн (Приложение 3);
4. Инструкция администратора ИСПДн (Приложение 4);
5. Инструкция пользователя ИСПДн (Приложение 5);
6. Инструкция администратора безопасности ИСПДн (Приложение 6);
7. Положение о Порядке резервирования и восстановления работоспособности ТС и ПО, баз данных и СЗИ (Приложение 7).

Директор школы _____ Родина О.В.



Журнал учета мероприятий по контролю над соблюдением режима защиты персональных данных

Мероприятие	Дата	Исполнитель	Результат

Журнал учета мероприятий по контролю над соблюдением режима защиты персональных данных, содержит перечень периодически проводимых мероприятий.

В Журнале отмечаются мероприятия, в соответствии с Планом мероприятий по обеспечению защиты персональных данных, носящих периодический характер.

В журнал заносится следующая информация:

1. Название проведенного мероприятия.
2. Дата проведенного мероприятия.
3. Исполнитель мероприятия.

Результат (отчет, действия) мероприятия, если есть.

План внутренних проверок режима защиты персональных данных

Мероприятие	Периодичность	Исполнитель
Контроль над соблюдением режима обработки ПДн	Еженедельно	
Контроль над соблюдением режима защиты	Ежедневно	
Контроль над выполнением антивирусной защиты	Еженедельно	
Контроль над соблюдением режима защиты при подключении к сетям общего пользования и (или) международного обмена	Еженедельно	
Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн	Ежегодно	
Контроль за обновлениями программного обеспечения и единообразия применяемого ПО на всех элементах ИСПДн	Еженедельно	
Контроль за обеспечением резервного копирования	Ежемесячно	
Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а так же предсказание появления новых, еще неизвестных, угроз	Ежегодно	
Поддержание в актуальном состоянии нормативно-организационных документов	Ежемесячно	
Контроль за разработкой и внесением изменений в программное обеспечение собственной разработки или штатное ПО специально дорабатываемое собственными разработчиками или сторонними организациями.	Ежемесячно	

План внутренних проверок режима защиты персональных данных, содержит перечень внутренних проверок.

План составляется для мероприятий, в соответствии с Планом мероприятий по обеспечению защиты персональных данных, и определяет периодичность проведения проверок.

В План внутренних проверок содержится следующую информацию:

1. Название проведенного мероприятия.
2. Периодичность проведения проверки.

3. Исполнитель мероприятия.
План внутренних проверок распространяется на все информационные системы персональных данных Учреждения.

Приложение 3

Журнал учета обращений субъектов персональных данных о соблюдении их законных прав, при обработке персональных данных в ИСПДн АСИОУ

№	ФИО	Дата	Цель

Приложение 4

Инструкция Администратора ИСПДн

1. Администратор обязан:

1.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

1.2. Обеспечивать установку, настройку и своевременное обновление элементов ИСПДн: программного обеспечения АРМ и серверов (операционные системы, прикладное и специальное ПО); аппаратных средств; аппаратных и программных средств защиты.

1.3. Обеспечивать работоспособность элементов ИСПДн и локальной вычислительной сети.

1.4. Осуществлять контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов.

1.5. Обеспечивать функционирование и поддерживать работоспособность средств защиты в рамках возложенных на него функций.

1.6. В случае отказа технических средств и/или потери работоспособности программного обеспечения элементов ИСПДн, в том числе средств защиты информации, принимать меры по своевременному восстановлению и выявлению причин, приведших к этому.

1.7. Проводить периодический контроль принятых мер по защите, в пределах возложенных на него функций.

1.8. Хранить, осуществлять прием и выдачу персональных паролей пользователей, осуществлять контроль за правильностью использования персонального пароля Оператором ИСПДн.

1.9. Обеспечивать постоянный контроль за выполнением пользователями установленного комплекса мероприятий по обеспечению безопасности информации.

1.10. Информировать ответственного за обеспечение защиты персональных данных о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИСПДн.

1.11. Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств и отправке их в ремонт. Техническое обслуживание и ремонт средств вычислительной техники, предназначенных для обработки персональных данных, проводятся организациями, имеющими соответствующие лицензии. При проведении технического обслуживания и ремонта запрещается передавать ремонтным организациям узлы и блоки с элементами накопления и хранения информации. Вышедшие из строя элементы и блоки средств вычислительной

техники заменяются на элементы и блоки, прошедшие специальные исследования и специальную проверку.

1.12. Присутствовать при выполнении технического обслуживания элементов ИСПДн, сторонними физическими людьми и организациями.

1.13. Принимать меры по реагированию, в случае возникновения внештатных и аварийных ситуаций.

2. Администратор имеет право:

2.1. Требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн или средств защиты.

2.2. Знакомиться с документами, определяющими его права и обязанности по занимаемой должности, критерии оценки качества исполнения должностных обязанностей.

2.3. Вносить на рассмотрение руководства предложения по совершенствованию работы, связанной с предусмотренными настоящей должностной инструкцией обязанностями.

2.4. Требовать от руководства обеспечения организационно - технических условий, необходимых для исполнения должностных обязанностей.

3. Ответственность администратора ИСПДн

3.1. Системный администратор несет ответственность за:

3.1.1. Нарушение функционирования ИСПДн вследствие ненадлежащего исполнения своих должностных обязанностей.

3.1.2. Несвоевременную регистрацию пользователей ИСПДн.

3.1.3. Несвоевременное уведомление руководства о случаях нарушения правил пользования ИСПДн.

3.2. Системный администратор привлекается к ответственности:

3.2.1. За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей должностной инструкцией - в пределах, установленных действующим трудовым законодательством Российской Федерации.

3.2.2. За правонарушения, совершенные в процессе своей деятельности - в пределах, установленных действующим административным, уголовным и гражданским законодательством Российской Федерации.

3.2.3. За причинение материального ущерба ОГВ - в пределах, установленных действующим законодательством Российской Федерации.

Приложение 5

Инструкция пользователя ИСПДн

Пользователями ИСПДн (далее – Пользователь) являются сотрудники, ответственные за обработку персональных данных в ИСПДн МОУ Чебаковская СОШ, а также сотрудники, участвующие в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации в ИСПДн, имеющие доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты ИСПДн. Пользователь в своей работе руководствуется настоящей инструкцией, Федеральным законом №152-ФЗ от 27 июля 2006 года «О персональных данных», Концепцией и Политикой информационной безопасности, руководящими и нормативными документами ФСТЭК.

Методическое руководство работой пользователя осуществляется ответственным за обеспечение защиты персональных.

1. Обязанности пользователя

1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

2. Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности ПДн, а также руководящих и организационно-распорядительных документов.
3. Соблюдать требования парольной политики.
4. Соблюдать правила работы в сетях общего доступа и (или) международного обмена – Интернет и других (п.3 данного приложения).
5. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).
6. Обо всех выявленных нарушениях, связанных с информационной безопасностью МОУ Чебаковская СОШ, а так же для получения консультаций по вопросам информационной безопасности, необходимо обратиться в _____ по электронной почте: _____ или по внутреннему телефону _____.
7. Для получения консультаций по вопросам работы и настройке элементов ИСПДн необходимо обращаться к Администратору ИСПДн по внутреннему телефону _____.
8. Пользователям запрещается:
 1. Разглашать защищаемую информацию третьим лицам.
 2. Копировать защищаемую информацию на внешние носители без разрешения своего руководителя.
 3. Самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств.
 4. Несанкционированно открывать общий доступ к папкам на своей рабочей станции.
 5. Подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства.
 6. Отключать (блокировать) средства защиты информации.
 7. Обращаться на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИСПДн.
 8. Сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн.
 9. Привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за обеспечение защиты персональных данных.
9. При отсутствии визуального контроля за рабочей станцией: доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl>+<Alt>+ и выбрать опцию <Блокировка> (либо комбинацию <Windows>+<L>).
10. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий, в рамках возложенных на него функций.

2. Организация парольной защиты

1. Личные пароли доступа к элементам ИСПДн выдаются пользователям Администратором информационной безопасности, Администратором ИСПДн или создаются самостоятельно.
2. Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 3 месяца.
3. Правила формирования пароля:
 - Пароль не может содержать имя учетной записи пользователя или какую-либо его часть.
 - Пароль должен состоять не менее чем из 8 символов.
 - В пароле должны присутствовать символы трех категорий из числа следующих четырех:

- a. прописные буквы английского алфавита от А до Z;
 - b. строчные буквы английского алфавита от а до z;
 - c. десятичные цифры (от 0 до 9);
 - d. символы, не принадлежащие алфавитно-цифровому набору (например, !, \$, #, %).
- Запрещается использовать в качестве пароля имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а так же имена и даты рождения свои или родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе.
 - Запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;
 - Запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);
 - Запрещается выбирать пароли, которые уже использовались ранее.
4. Правила ввода пароля:
- Ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан.
 - Во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).
5. Правила хранения пароля:
- Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах.
 - Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.
 - Запрещается регистрироваться в системе под чужой учетной записью.
6. Лица, использующие пароли доступа к элементам ИСПДн, обязаны:
- четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по паролированию.
 - своевременно сообщать Администратору информационной безопасности об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

3. Правила работы в сетях общего доступа и (или) международного обмена

1. Работа в сетях общего доступа и (или) международного обмена (сети Интернет и других) (далее – Сеть) на элементах ИСПДн, должна проводиться при служебной необходимости.
2. При работе в Сети запрещается:
- Осуществлять работу при отключенных средствах защиты (антивирус и других).
 - Передавать по Сети защищаемую информацию без использования средств шифрования.
 - Скачивать из Сети программное обеспечение и другие файлы.
 - Посещать сайты сомнительной репутации (сайты эротического содержания, сайты содержащие нелегально распространяемое ПО, медиаконтент и другие).
 - Использовать подключение к Сети во внеслужебных целях.

Приложение 6

Инструкция администратора безопасности ИСПДн

1. Администратор безопасности обязан:

- 1.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.
- 1.2. Осуществлять установку, настройку и сопровождение технических средств защиты.

- 1.3. Участвовать в контрольных и тестовых испытаниях и проверках элементов ИСПДн.
- 1.4. Участвовать в приемке новых программных средств.
- 1.5. Обеспечивать доступ к защищаемой информации пользователям ИСПДн согласно их правам доступа при получении оформленного соответствующим образом разрешения.
- 1.6. Уточнять в установленном порядке обязанности пользователей ИСПДн по обработке объектов защиты.
- 1.7. Вести контроль над процессом осуществления резервного копирования объектов защиты.
- 1.8. Осуществлять контроль над выполнением Плана мероприятий по защите персональных данных.
- 1.9. Анализировать состояние защиты ИСПДн и ее отдельных подсистем.
- 1.10. Контролировать неизменность состояния средств защиты их параметров и режимов защиты.
- 1.11. Контролировать физическую сохранность средств и оборудования ИСПДн.
- 1.12. Контролировать исполнение пользователями ИСПДн введенного режима безопасности, а так же правильность работы с элементами ИСПДн и средствами защиты.
- 1.13. Контролировать исполнение пользователями парольной политики.
- 1.14. Контролировать работу пользователей в сетях общего пользования и (или) международного обмена.
- 1.15. Своевременно анализировать журнал учета событий, регистрируемых средствами защиты, с целью выявления возможных нарушений.
- 1.16. Не допускать установки, использования, хранения и размножения в ИСПДн программных средств, не связанных с выполнением функциональных задач.
- 1.17. Не допускать к работе на элементах ИСПДн посторонних лиц.
- 1.18. Осуществлять периодические контрольные проверки рабочих станций и тестирование правильности функционирования средств защиты ИСПДн.
- 1.19. Оказывать помощь пользователям ИСПДн в части применения средств защиты и консультировать по вопросам введенного режима защиты.
- 1.20. Периодически представлять руководству отчет о состоянии защиты ИСПДн, о нештатных ситуациях на объектах ИСПДн и допущенных пользователями нарушениях установленных требований по защите информации.
- 1.21. В случае отказа технических средств и/или потери работоспособности программного обеспечения элементов ИСПДн, в том числе средств защиты информации, принимать меры по своевременному восстановлению и выявлению причин, приведших к этому.
- 1.22. Принимать меры по реагированию, в случае возникновения нештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.

2. Администратор имеет право:

- 2.1. Знакомиться с проектами решений руководства, касающихся его деятельности.
- 2.2. Вносить на рассмотрение руководства предложения по совершенствованию работы, связанной с предусмотренными настоящей инструкцией обязанностями.
- 2.3. В пределах своей компетенции сообщать своему непосредственному руководителю о всех выявленных в процессе осуществления должностных обязанностей недостатках и вносить предложения по их устранению.
- 2.4. Запрашивать от специалистов подразделений информацию и документы, необходимые для выполнения его должностных обязанностей.
- 2.5. Привлекать специалистов всех структурных подразделений к решению задач, возложенных на него в части, их касающейся.
- 2.6. Требовать от руководства оказания содействия в исполнении им своих должностных обязанностей.

3. Ответственность администратора безопасности

Администратор безопасности ИСПДн несет ответственность:

- 3.1. За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей инструкцией - в пределах, определенных действующим трудовым законодательством Российской Федерации.

- 3.2. За правонарушения, совершенные в процессе осуществления своей деятельности - в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.
- 3.3. За причинение материального ущерба - в пределах, определенных действующим трудовым и гражданским законодательством Российской Федерации.

Приложение 7

Положение о Порядке резервирования и восстановления работоспособности ТС и ПО, баз данных и СЗИ

1. Назначение и область действия

Порядок резервирования и восстановления работоспособности ТС и ПО, баз данных и СЗИ определяет действия (далее – Инструкция), связанные с функционированием ИСПДн МОУ Чебаковская СОШ, меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн.

Целью настоящего документа является превентивная защита элементов ИСПДн от потери защищаемой информации.

Задачей данной Инструкции является:

- определение мер защиты от потери информации;
- определение действий восстановления в случае потери информации.

Действие настоящей Инструкции распространяется на всех пользователей МОУ Чебаковская СОШ, имеющих доступ к ресурсам ИСПДн, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

Пересмотр настоящего документа осуществляется по мере необходимости, но не реже раза в два года.

Ответственным сотрудником за реагирование на инциденты безопасности, приводящие к потере защищаемой информации, назначается Администратор ИСПДн Родина О.В.

Ответственным сотрудником за контроль обеспечения мероприятий по предотвращению инцидентов безопасности, приводящих к потере защищаемой информации, назначается Администратор безопасности Родина О.В.

2. Порядок реагирования на инцидент

В настоящем документе под Инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн, а так же потерей защищаемой информации.

Происшествие, вызывающее инцидент, может произойти:

- В результате непреднамеренных действий пользователей.
- В результате преднамеренных действий пользователей и третьих лиц.
- В результате нарушения правил эксплуатации технических средств ИСПДн.
- В результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

Все действия в процессе реагирования на Инцидент должны документироваться администратором безопасности Журнале по учету мероприятий по контролю.

В кратчайшие сроки, не превышающие одного рабочего дня Администратор безопасности и Администратор предпринимают меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством. По необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

3. Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов

Технические меры

К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения Инцидентов, такие как:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.
- Системы жизнеобеспечения ИСПДн включают:
- пожарные сигнализации и системы пожаротушения;
- системы вентиляции и кондиционирования;
- системы резервного питания.

Все критичные помещения МОУ Чебаковская СОШ (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ИСПДн в помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха.

Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

- локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;
- источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;

Системы обеспечения отказоустойчивости:

- кластеризация;
- технология RAID.

Для обеспечения отказоустойчивости критичных компонентов ИСПДн при сбое в работе оборудования и их автоматической замены без простоев должны использоваться методы кластеризации. Могут использоваться следующие методы кластеризации: для наиболее критичных компонентов ИСПДн должны использоваться территориально удаленные системы кластеров.

Для защиты от отказов отдельных дисков серверов, осуществляющих обработку и хранение защищаемой информации, должны использоваться технологии RAID, которые (кроме RAID-0) применяют дублирование данных, хранимых на дисках.

Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на твердый носитель (ленту, жесткий диск и т.п.).

Организационные меры

Резервное копирование и хранение данных должно осуществляться на периодической основе:

- для обрабатываемых персональных данных – не реже раза в неделю;
- для технологической информации – не реже раза в месяц;
- резервные копии системы со средствами защиты и специальным программным обеспечением (образ), с которых после инцидента осуществляется их установка на элементы ИСПДн – не реже раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

Данные о проведении процедуры резервного копирования, должны отражаться в специально созданном журнале учета.

Носители, на которые произведено резервное копирование, должны быть пронумерованы: номером носителя, датой проведения резервного копирования.

Носители должны храниться в негорючем шкафу или помещении оборудованном системой пожаротушения отдельно от установленных элементов ИСПДн (в разных помещениях).

Носители должны храниться не менее года, для возможности восстановления данных.