МИНИСТЕРСТВО ОБРАЗОВАНИЯ НОВОСИБИРСКОЙ ОБЛАСТИ

ПРИКАЗ

15 ИЮН 2022 № 1184

г. Новосибирск

О внесении изменений в приказ министерства образования Новосибирской области от 07.05.2018 № 1098

П р и к а з ы в а ю:

Внести в приказ министерства образования Новосибирской области от 07.05.2018 № 1098 «Об утверждении правил по проведению работ по защите информации в министерстве образования Новосибирской области» следующие изменения:

1. В пункте 1:

1) подпункты 2, 3, 4, 5 признать утратившими силу;

2) дополнить подпунктами 7, 8 следующего содержания:

«7) Положение по управлению конфигурацией информационных систем министерства образования Новосибирской области;

8) Правила обеспечения целостности и доступности информационных систем и информации в министерстве образования Новосибирской области.».

2. Дополнить:

1) Положением по управлению конфигурацией информационных систем министерства образования Новосибирской области согласно приложению № 1 к настоящему приказу;

2) Правилами обеспечения целостности и доступности информационных систем и информации в министерстве образования Новосибирской области согласно приложению № 2 к настоящему приказу.

Министра С.В. Федорчук

ПРИЛОЖЕНИЕ № 1
к приказу Минобразования
Новосибирской области
от 15 ИЮН 2022 № 1184

«УТВЕРЖДЕНО
приказом Минобразования
Новосибирской области
от 07.05.2018 № 1098

ПОЛОЖЕНИЕ
по управлению конфигурацией информационных систем министерства образования Новосибирской области
(далее – Положение)

I. Общие положения

1. Настоящее Положение определяет порядок управления конфигурацией информационных систем (далее – ИС) министерства образования Новосибирской области (далее – Министерство) и их системы защиты информации.

II. Порядок управления конфигурацией информационных систем и системы защиты информации

2. Действия по внесению изменений в конфигурацию ИС Министерства и их системы защиты информации разрешены уполномоченным сотрудникам государственного автономного учреждения дополнительного профессионального образования Новосибирской области «Новосибирский институт повышения квалификации и переподготовки работников образования», государственного бюджетного учреждения Новосибирской области «Центр защиты информации Новосибирской области» и государственного бюджетного учреждения Новосибирской области «Центр информационных технологий Новосибирской области» в пределах их полномочий, а также представителям сторонним организаций, оказывающим услуги гарантийного и (или) технического обслуживания программных и программно-аппаратных средств, включая средства защиты информации, ИС Министерства в пределах полномочий согласно заключенным договорам, соглашениям, контрактам.

3. Управление конфигурацией ИС Министерства осуществляется на основе согласованных решений уполномоченных лиц, указанных в пункте 2 настоящего Положения, и включает:

1) разработку параметров настройки, обеспечивающих защиту информации;

2) анализ потенциального воздействия планируемых изменений на обеспечение защиты информации (возникновение дополнительных угроз безопасности информации и работоспособность ИС);

3) санкционирование внесения изменений в ИС Министерства и их системы защиты информации;

4) документирование действий по внесению изменений в ИС Министерства и их системы защиты информации и сохранение данных об изменениях конфигурации.

4. Объектами управления конфигурацией (компонентами ИС Министерства и их системы защиты информации, подлежащих изменению в рамках управления конфигурацией) определены программно-аппаратные, программные средства, включая средства защиты информации, их настройки и программный код, эксплуатационная документация, интерфейсы, файлы и иные компоненты, подлежащие изменению и контролю.

5. Внесение изменений в ИС Министерства и их системы защиты информации в отношении объектов управления конфигурацией может осуществляться в рамках гарантийного и (или) технического обслуживания (в том числе дистанционно (удаленно)), программных и программно-аппаратных средств, включая средства защиты информации, ИС Министерства.

6. Документирование (внесение информации (данных)) об изменениях в конфигурации ИС Министерства и их систем защиты информации (структуры системы защиты информации ИС, состава, мест установки и параметров настройки средств защиты информации, программного обеспечения и технических средств) в эксплуатационную документацию на систему защиты информации ИС осуществляет администратор информационной безопасности в Министерстве.».

ПРИЛОЖЕНИЕ № 2
к приказу Минобразования
Новосибирской области
от 15 ИЮН 2022 № 1184

«УТВЕРЖДЕНЫ
приказом Минобразования
Новосибирской области
от 07.05.2018 № 1098

ПРАВИЛА
обеспечения целостности и доступности информационных систем и информации в министерстве образования Новосибирской области (далее – Правила)

I. Общие положения

1. Правила разработаны в целях реализации мер по обеспечению целостности и доступности информационных систем (далее – ИС) и информации в министерстве образования Новосибирской области (далее – Министерство, оператор).

2. Меры по обеспечению целостности ИС и информации должны обеспечивать обнаружение фактов несанкционированного нарушения целостности ИС и содержащейся в ней информации, а также возможность восстановления ИС и содержащейся в ней информации.

3. Меры по обеспечению доступности информации должны обеспечивать авторизованный доступ пользователей, имеющих права по такому доступу, к информации, содержащейся в ИС, в штатном режиме функционирования ИС.

4. Защита резервируемой информации в ИС Министерства обеспечивается применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования, определенных в проектной и организационно-распорядительной документации по защите информации в Министерстве.

II. Обеспечение возможности восстановления программного обеспечения (в том числе средств защиты информации) при возникновении нештатных ситуаций

5. Возможность восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций предусматривает:

1) восстановление программного обеспечения, включая программное обеспечение средств защиты информации, из резервных копий (дистрибутивов) программного обеспечения;

2) восстановление и проверку работоспособности системы защиты информации, обеспечивающей необходимый уровень защищенности информации;

3) возврат ИС Министерства в начальное состояние (до возникновения нештатной ситуации), обеспечивающее их штатное функционирование, или восстановление отдельных функциональных возможностей ИС Министерства, позволяющих решать задачи по обработке информации.

6. В ИС Министерства должны применяться компенсирующие меры защиты информации в случаях, когда восстановление работоспособности системы защиты информации невозможно.

III. Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование

7. В ИС Министерства осуществляется контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование.

8. Контроль безотказного функционирования проводится в отношении серверного и телекоммуникационного оборудования, каналов связи, средств обеспечения функционирования ИС путем периодической проверки работоспособности в соответствии с эксплуатационной документацией (в том числе путем посылки тестовых сообщений и принятия «ответов», визуального контроля, контроля трафика, контроля «поведения» системы или иными методами).

9. При обнаружении отказов функционирования осуществляется их локализация и принятие мер по восстановлению отказавших средств в соответствии с настоящим Положением, их тестирование в соответствии с эксплуатационной документацией, а также регистрация событий, связанных с отказами функционирования.

IV. Периодическое резервное копирование информации на резервные машинные носители информации

10. В Министерстве обеспечивается периодическое резервное копирование информации (баз данных и иной информации, содержащейся в ИС Министерства, и (или) необходимой для функционирования ИС Министерства, и размещенной на технических средствах Министерства) на резервные машинные носители информации, предусматривающее:

1) резервное копирование информации на резервные машинные носители информации с установленной периодичностью;

2) разработку перечня информации (типов информации), подлежащей периодическому резервному копированию на резервные машинные носители информации;

3) регистрацию событий, связанных с резервным копированием информации на резервные машинные носители информации;

4) принятие мер для защиты резервируемой информации, обеспечивающих ее конфиденциальность, целостность и доступность.

11. Резервное копирование и хранение данных должно осуществлять на периодической основе. Перечень резервируемой информации и периодичность создания резервных копий указана в таблице 1.

Таблица 1 – Перечень резервируемой информации и периодичность создания резервных копий

№ п/п	Наименование резервируемого ресурса	Периодичность резервного копирования
1.	Защищаемая информация, содержащаяся в базах данных, хранящихся на технических средствах Министерства	Не реже раза в квартал (локально на АРМ пользователей)
2.	Эталонные копии программного обеспечения (системное программное обеспечение, программное обеспечение общего назначения, специализированное программное обеспечение и программные средства защиты информации)	При необходимости при обновлении программного обеспечения

12. Хранение (размещение) резервных копий информации должно осуществляться на отдельных (размещенных вне информационной системы) средствах хранения резервных копий и в условиях, которые исключают воздействие внешних факторов на хранимую информацию.

13. Резервные копии должны храниться в течение установленного срока с целью обеспечения возможности восстановления данных.

14. Ответственным за защиту информации, не содержащей сведения, составляющие государственную тайну, содержащейся в ИС Министерства, лицами, ответственными за управление (администрирование) системой защиты информации ИС Министерства, и лицами с полномочиями системных администраторов ИС Министерства, обеспечивающими функционирование ИС Министерства, в пределах своей компетенции определяются методы резервного копирования, порядок хранения и восстановления резервируемой информации и осуществляется периодическая проверка работоспособности средств резервного копирования, средств хранения резервных копий и средств восстановления информации из резервных копий.

V. Восстановление информации с резервных машинных носителей информации (резервных копий)

15. Восстановление информации из резервных копий обеспечивается лицами, ответственными за управление (администрирование) системой защиты информации ИС Министерства, лицами с полномочиями системных администраторов ИС Министерства, обеспечивающими функционирование ИС Министерства, в пределах их компетенции.

16. Восстановление программного обеспечения (системного программного обеспечения, программного обеспечения общего назначения, специализированного программного обеспечения и программных средств защиты информации) производится с дистрибутивных носителей или их резервных копий в соответствии с инструкциями производителя по установке или восстановлению данного программного обеспечения.

17. Восстановление информации с резервных машинных носителей информации (резервных копий) предусматривает определение времени, в течение

которого должно быть обеспечено восстановление информации и обеспечивающего требуемые условия непрерывности функционирования ИС Министерства и доступности информации:

1) для защищаемой информации (баз данных) и иной информации, содержащейся в ИС Министерства и необходимой для функционирования ИС Министерства – не более 8 часов;

2) для эталонных копий программного обеспечения (системное программное обеспечение, программное обеспечение общего назначения, специализированное программное обеспечение и программные средства защиты информации) – не более 24 часов.

18. Основанием для инициирования процедуры восстановления служит полная или частичная утрата резервируемой информации вследствие сбоев оборудования, программного обеспечения, в результате иных нештатных ситуаций.

19. Восстановление утраченных данных производится из резервной копии, обеспечивающей минимальную потерю данных, содержащихся в информационном ресурсе.

20. В зависимости от характера и уровня повреждения информационных ресурсов, восстановлению из резервной копии подлежит либо весь архив копии данных, либо отдельные утраченные (поврежденные) фрагменты данных из соответствующих хранилищ.».