



МИНИСТЕРСТВО ОБРАЗОВАНИЯ НОВОСИБИРСКОЙ ОБЛАСТИ

ПРИКАЗ

№ _____

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» следующее изменение:

1. Пункт 1 дополнить подпунктами 9-12 следующего содержания:

«9) План проведения внутреннего контроля соответствия обработки защищаемой информации, не содержащей сведения, составляющие государственную тайну, в министерстве образования Новосибирской области установленным требованиям».

10) Контроль выполнения мероприятий по обеспечению безопасности защищаемой информации (в том числе персональных данных), не содержащей сведения, составляющие государственную тайну, обрабатываемой в министерстве образования Новосибирской области.

11) Форма отчета о результатах контроля соответствия условий обработки персональных данных в министерстве образования Новосибирской области установленным требованиям.

12) Форма протокола контроля за выполнением требований по обеспечению безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну, в министерстве образования Новосибирской области установленным требованиям.».

2. Дополнить:

1) Планом проведения внутреннего контроля соответствия обработки защищаемой информации, не содержащей сведения, составляющие государственную тайну, в министерстве образования Новосибирской области установленным требованиям».

10) Контролем выполнения мероприятий по обеспечению безопасности защищаемой информации (в том числе персональных данных), не содержащей

сведения, составляющие государственную тайну, обрабатываемой в министерстве образования Новосибирской области.

11) Formой отчета о результатах контроля соответствия условий обработки персональных данных в министерстве образования Новосибирской области установленным требованиям.

12) Formой протокола контроля за выполнением требований по обеспечению безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну, в министерстве образования Новосибирской области установленным требованиям.».

И.о. министра

Ю.И. Савостьянов

начальник отдела организации
управления и кадровой работы
организационно-правового управления
министерства образования
Новосибирской области

Силакова Е.Е.

начальник организационно-правового
управления министерства
образования Новосибирской области

Тарасик Т.М.

Рассылка: структурные подразделения министерства образования
Новосибирской области

Для размещения на сайте Минобразования Новосибирской области и в ГИС
НСО «Электронная демократия»

На контроль

Для размещения на сайте Минобразования Новосибирской области и в ГИС
НСО «Электронная демократия»

с «__» _____ по «__» _____ 20__ года *даты начала и окончания приема
заключений независимой антикоррупционной экспертизы
размещения НПА (не менее 7 дней).*

для НПА: 1) Прокуратура Новосибирской области – 1экз.;
2) Главное Управление Министерства юстиции Российской
Федерации по Новосибирской области – 1экз.;
3) Законодательное Собрание Новосибирской области – 1экз.;
4) Министерство юстиции Новосибирской области – 1 экз.;
5) Размещается на сайте Минобразования Новосибирской области;
6) На официальное опубликование на www.nsopravo.ru

для НПА на официальное размещение (опубликование) www.pravo.gov.ru».

УТВЕРЖДЕН
приказом Минобразования
Новосибирской области
от «__» _____ 20__ г. № ____

План проведения внутреннего контроля соответствия обработки защищаемой информации, не содержащей сведения, составляющие государственную тайну, в министерстве образования Новосибирской области установленным требованиям

1. Контроль условий обработки персональных данных в министерстве образования новосибирской области

Перечень мероприятий, проводимых в рамках внутреннего контроля соответствия условий обработки персональных данных (далее – ПДн) в министерстве образования Новосибирской области (далее – министерство, оператор) установленным требованиям, их периодичность и ответственные исполнители приведены в Таблице 1.

Таблица 1 – Перечень мероприятий, проводимых в рамках внутреннего контроля соответствия условий обработки ПДн

№ п/п	Периодичность	Мероприятие	Ответственный исполнитель
1.	Не реже одного раза в год	Контроль актуальности положений Политики в отношении обработки ПДн, соблюдения прав субъектов ПДн, чьи ПДн обрабатываются в ИС министерства, и обязанностей оператора, предусмотренных действующим законодательством в области ПДн	Ответственный за организацию обработки ПДн в министерстве
2.	Не реже одного раза в год	Контроль изменений правил обработки и защиты ПДн (принципов, целей обработки ПДн, состава и количества субъектов ПДн и состава ПДн, обрабатываемых в министерства, способов обработки ПДн и актуальности ранее установленного уровня защищенности ПДн пр.)	Ответственный за организацию обработки ПДн в министерстве
3.	Не реже одного раза в год	Контроль состава и соответствия содержания локальных актов министерства в области обработки и защиты ПДн действующему законодательству Российской Федерации	Ответственный за организацию обработки ПДн в министерстве

№ п/п	Периодичность	Мероприятие	Ответственный исполнитель
4.	Не реже одного раза в год	Контроль выполнения сотрудниками министерства требований и правил обработки ПДн (правильности осуществления сбора, систематизации, записи, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), блокирования, удаления, уничтожения ПДн)	Ответственный за организацию обработки ПДн в министерстве
5.	Не реже одного раза в год	Контроль актуальности перечня лиц, уполномоченных на обработку ПДн и имеющих доступ к ПДн	Ответственный за организацию обработки ПДн в министерстве
6.	Не реже одного раза в год	Контроль санкционирования и учета физического доступа в помещения и сооружения, в которых размещены информационные системы министерства и ведется обработка ПДн (контроль актуальности Перечня лиц, имеющих доступ в помещения, в которых размещены информационные системы министерства и ведется обработка информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну; контроль выдачи и наличия ключей от помещений; контроль соблюдения порядка доступа в помещения, в которых, в которых размещены информационные системы министерства и ведется обработка информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну)	Начальники управлений министерства/ Ответственный за организацию обработки ПДн в министерстве
7.	Не реже одного раза в год	Контроль соблюдения порядка взаимодействия с субъектами ПДн (в том числе соблюдения сроков, предусмотренных действующим законодательством в области ПДн, соблюдения требований по уведомлениям, порядка разъяснения	Начальники управлений министерства/ Ответственный за организацию обработки ПДн в министерстве

№ п/п	Периодичность	Мероприятие	Ответственный исполнитель
		субъектам ПДн необходимой информации, порядка реагирования на обращения (запросы) субъектов ПДн, порядка действий при достижении целей обработки ПДн и отзыве согласий субъектами ПДн)	
8.	Не реже одного раза в год	Контроль наличия необходимых согласий субъектов, чьи ПДн обрабатываются в министерстве	Начальники управлений министерства
9.	В случае изменения сведений, указанных в уведомлении об обработке ПДн, а также в случае прекращения обработки ПДн в течение десяти рабочих дней с даты возникновения таких изменений или с даты прекращения обработки ПДн	Контроль актуальности сведений, содержащихся в уведомлении об обработке ПДн	Ответственный за организацию обработки ПДн в министерстве
10.	Не реже одного раза в год	Контроль подписания сотрудниками министерства обязательств о соблюдении конфиденциальности информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, и обязательств о прекращении обработки персональных данных в случае расторжения с ними служебного контракта (трудового договора)	Сотрудник отдела организации управления и кадровой работы
11.	Не реже одного раза в год	Проверка ознакомления сотрудников, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн и локальными актами	Ответственный за организацию обработки ПДн в министерства

№ п/п	Периодичность	Мероприятие	Ответственный исполнитель
		министерства по вопросам обработки ПДн, а также знания и соблюдения ими требований и положений вышеуказанных документов	
12.	Не реже одного раза в год	Контроль за уничтожением ПДн, а также электронных (бумажных) носителей ПДн	Начальники управлений министерства/ Ответственный за организацию обработки ПДн в министерстве
13.	Не реже одного раза в год	Контроль соответствия оценки соотношения вреда, который может быть причинен субъектам ПДн в случае нарушения требований по обработке и обеспечению безопасности ПДн, и принимаемых мер по обработке и обеспечению безопасности ПДн в министерстве	постоянно действующая экспертная комиссия по проведению мероприятий по защите персональных данных

УТВЕРЖДЕН
приказом Минобразования
Новосибирской области
от «__» _____ 20__ г. № ____

Контроль выполнения мероприятий по обеспечению безопасности защищаемой информации (в том числе персональных данных), не содержащей сведения, составляющие государственную тайну, обрабатываемой в министерстве образования Новосибирской области

Перечень проверок, осуществляемых в рамках контроля выполнения мероприятий по обеспечению безопасности защищаемой информации (в том числе персональных данных), не содержащей сведения, составляющие государственную тайну, обрабатываемой в министерстве образования Новосибирской области, их периодичность и ответственные исполнители, приведены в Таблице 2.

Таблица 2 – Перечень проверок, осуществляемых в рамках контроля выполнения мероприятий по обеспечению безопасности защищаемой информации

№ п/п	Периодичность	Мероприятие	Ответственный исполнитель
1.	Контроль за проведением анализа угроз безопасности информации		
1.1.	Не реже одного раза в 2 года	Контроль проведения периодического выявления, анализа и устранения уязвимостей ИС	Ответственный за защиту информации, не содержащей сведения, составляющие государственную тайну, содержащейся в информационных системах (далее – ИС) министерства (далее – ответственный за защиту информации)
1.2.	Не реже одного раза в 2 года	Контроль проведения периодического анализа изменения угроз безопасности информации в ИС, возникающих в ходе их эксплуатации, и принятие мер защиты информации в случае возникновения новых угроз безопасности информации	Ответственный за защиту информации

№ п/п	Периодичность	Мероприятие	Ответственный исполнитель
2.	Контроль за обеспечением управления (администрирования) системой защиты информации		
2.1.	Не реже одного раза в 2 года	<p>Контроль закрепления в организационно-распорядительных документах (далее – ОРД по защите информации) порядка осуществления следующих мероприятий в рамках управления (администрирования) системой защиты информации:</p> <ul style="list-style-type: none"> – управления учетными записями пользователей и правилами разграничения доступа в ИС; – управления средствами защиты информации ИС; – управления обновлениями программных и программно-аппаратных средств, в том числе средств защиты информации; – порядка мониторинга и анализа зарегистрированных событий в ИС, связанных с обеспечением безопасности 	Ответственный за защиту информации
2.2.	Не реже одного раза в 2 года	Контроль ведения и актуализации эксплуатационной документации (технических паспортов ИС министерства и ОРД по защите информации)	Ответственный за защиту информации
3	Контроль за обеспечением управления конфигурацией ИС и их системами защиты информации		
3.1	Не реже одного раза в 2 года	Контроль определения в ОРД по защите информации объектов управления конфигурацией и процедур управления изменениями ИС и их систем защиты	Ответственный за защиту информации
3.2	Не реже одного раза в 2 года	Контроль документирования изменений в конфигурации ИС министерства и их систем защиты информации: состава, мест установки	Ответственный за защиту информации

№ п/п	Периодичность	Мероприятие	Ответственный исполнитель
		и параметров настройки программно-аппаратных, программных средств, включая средства защиты информации (контроль внесения информации (данных) в технические паспорта ИС, протоколы настройки средств защиты информации, перечень разрешенного к использованию программного обеспечения и пр.)	
4	Контроль за реализацией процедур реагирования на инциденты безопасности		
4.1	Не реже одного раза в 2 года	Контроль закрепления в ОРД по защите информации порядка обнаружения инцидентов и информирования ответственных лиц о возникновении инцидентов безопасности, а также порядка реагирования на инциденты безопасности	Ответственный за защиту информации
5	Контроль за проведением информирования и обучения персонала ИС по вопросам защиты информации		
5.1	Не реже одного раза в год	Контроль информирования персонала о появлении актуальных угроз безопасности информации, о правилах безопасной эксплуатации ИС	Ответственный за защиту информации
5.2	Не реже одного раза в год	Контроль доведения до персонала ИС требований по защите информации, а также положений ОРД по защите информации	Ответственный за защиту информации
5.3	Не реже одного раза в год	Контроль обучения персонала ИС правилам эксплуатации отдельных средств защиты информации	Ответственный за защиту информации
5.4	Не реже одного раза в год	Проверка проведения контроля осведомленности персонала ИС об угрозах безопасности информации и уровня знаний персонала по вопросам обеспечения защиты информации	Ответственный за защиту информации
6	Контроль за обеспечением уровня защищенности информации, содержащейся в ИС		
6	Контроль (анализ) защищенности информации ИС		
6.1	Не реже одного раза в	Контроль установки обновлений программного обеспечения	Ответственный за защиту информации

№ п/п	Периодичность	Мероприятие	Ответственный исполнитель
	2 года	(общесистемного, прикладного, программных средств защиты информации), в том числе проверка обновлений баз применяемых в ИС средств защиты информации (для средств антивирусной защиты и средств анализа защищенности)	(с привлечением лиц, осуществляющих функции администратора информационной безопасности ¹ , и
6.2	Не реже одного раза в 2 года	Проверка проведения контроля работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации	лиц, осуществляющих функции системных администраторов ²)
6.3	Не реже одного раза в 2 года	Проверка проведения контроля состава технических средств, программного обеспечения и средств защиты информации	
6.4	Не реже одного раза в год	Контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации	Ответственный за защиту информации
6.5	Не реже одного раза в 2 года	Контроль реализации мер защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, при ее передаче по каналам связи, имеющим выход за пределы контролируемой зоны	Ответственный за защиту информации (с привлечением лиц, осуществляющих функции администратора информационной безопасности)
6.6	Не реже одного раза в 2 года	Контроль соблюдения правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей	Ответственный за защиту информации (с привлечением лиц, осуществляющих функции

1 Администраторами информационной безопасности являются лица, осуществляющие администрирование (управление) системой защиты информации ИС министерства, назначенные из числа сотрудников министерства, и (или) являющиеся сотрудниками иных организаций, привлекаемых к выполнению работ по защите информации на договорной основе

2 Системными администраторами являются лица, обеспечивающие функционирование ИС министерства, назначенные из числа сотрудников министерства, и (или) являющиеся сотрудниками иных организаций

№ п/п	Периодичность	Мероприятие	Ответственный исполнитель
		ИС министерства	администратора информационной безопасности, и лиц, осуществляющих функции системных администраторов)
7	Анализ и оценка функционирования системы защиты информации ИС, включая выявление, анализ и устранение недостатков в функционировании системы защиты информации ИС		
7.1	Не реже одного раза в год	Контроль наличия технической и эксплуатационной документации на технические и программные средства, применяемые в ИС	Ответственный за защиту информации
7.2	Не реже одного раза в год	Контроль проведения процедур уничтожения (стирания) защищаемой информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации	Ответственный за защиту информации
7.3	Не реже одного раза в год	Контроль поэкземплярного учета средств защиты информации, эксплуатационной и технической документации к ним	Ответственный за защиту информации
7.4	Не реже одного раза в год	Контроль учёта машинных носителей информации	Ответственный за защиту информации
7.5	Не реже одного раза в 2 года	Проверка проведения контроля безотказного функционирования технических средств, обнаружение и локализацию отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование	Ответственный за защиту информации (с привлечением лиц, осуществляющих функции администратора информационной безопасности, и лиц, осуществляющих функции

№ п/п	Периодичность	Мероприятие	Ответственный исполнитель
			системных администраторов)
7.6	Не реже одного раза в 2 года	Проверка проведения контроля работоспособности средств резервного копирования, средств хранения резервных копий и средств восстановления информации из резервных копий	Ответственный за защиту информации (с привлечением лиц, осуществляющих функции системных администраторов, лиц, осуществляющих процедуру резервного копирования)
7.7	В режиме мониторинга в ходе эксплуатации ИС	Контроль проведения периодических проверок компонентов ИС на наличие вредоносных компьютерных программ (вирусов)	Ответственный за защиту информации
7.8	Не реже одного раза в 2 года	Пересмотр перечня событий безопасности, подлежащих регистрации в ИС	Ответственный за защиту информации
7.9	Не реже одного раза в год	Проверка расположения средств отображения информации	Ответственный за защиту информации
7.10	В случае вывода из эксплуатации ИС или после принятия решения об окончании обработки информации	Контроль за обеспечением защиты информации при выводе из эксплуатации аттестованной ИС или после принятия решения об окончании обработки информации	Ответственный за защиту информации

Форма

Отчет о результатах контроля соответствия условий обработки персональных данных в министерстве образования Новосибирской области установленным требованиям

1. Характеристика объекта контроля

1.1. Наименование объекта контроля³:

1.2. Адрес размещения объекта контроля:

1.3. Категория персональных данных, обрабатываемых на объекте контроля:

1.4. Уровень защищенности персональных данных при их обработке на объекте контроля: _____

1.5. Метод проведения контроля⁴:

2. В ходе проверки были проведены следующие мероприятия⁵:

3. Результаты проведения проверки:

4. Меры по устранению выявленных нарушений (при их наличии):

В проведении контроля участвовали:

должность

подпись

фамилия, инициалы

подпись

фамилия, инициалы

³ Указывается наименование структурного подразделения и (или) наименование информационной системы

⁴ Экспертно-документальный/инструментальный

⁵ Перечисляются мероприятия, проводимые в рамках внутреннего контроля соответствия условий обработки персональных данных, в соответствии с Планом проведения внутреннего контроля соответствия обработки защищаемой информации, не содержащей сведения, составляющие государственную тайну, в министерстве установленным требованиям

_____	_____	_____
ДОЛЖНОСТЬ		
_____	_____	_____
_____	_____	_____
ДОЛЖНОСТЬ	ПОДПИСЬ	ФАМИЛИЯ, ИНИЦИАЛЫ

Дата проведения контроля: _____
(число, месяц, год)

УТВЕРЖДЕН
приказом Минобразования
Новосибирской области
от « » 20 г. №

Форма

Протокол контроля за выполнением требований по обеспечению безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну, в министерстве

1. Характеристика объекта контроля

1.1. Наименование информационных(ой) систем(ы):

1.2. Адрес размещения объекта контроля:

1.3. Класс защищенности информационных(ой) систем(ы):

2. Метод проведения контроля⁶:

3. Контроль проводился на соответствие требованиям по защите информации, установленным:

– постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

4. Сведения о проводимых в ходе контроля мероприятиях и результатах проверок:

№ п/п	Мероприятия по контролю ⁷	Результаты проведения проверки

5. Меры по устранению выявленных нарушений (при их наличии):

⁶ Экспертно-документальный/инструментальный

⁷ Перечисляются мероприятия, проводимые в рамках контроля за выполнением мероприятий по обеспечению безопасности защищаемой информации в соответствии с Планом проведения внутреннего контроля соответствия обработки защищаемой информации, не содержащей сведения, составляющие государственную тайну, в министерства установленным требованиям

В проведении контроля участвовали:

должность

подпись

фамилия, инициалы

должность

подпись

фамилия, инициалы

Дата проведения контроля: _____

(число, месяц, год)