МИНИСТЕРСТВО ОБРАЗОВАНИЯ НОВОСИБИРСКОЙ ОБЛАСТИ
(МИНОБРАЗОВАНИЯ НОВОСИБИРСКОЙ ОБЛАСТИ)

ПРИКАЗ

18.02.2019 №336

г. Новосибирск

Об утверждении Положения об управлении доступом субъектов доступа к объектам доступа в информационной системе персональных данных министерства образования Новосибирской области

В связи с осуществлением обработки персональных данных в информационной системе персональных данных министерства образования Новосибирской области (далее – ИСПДн министерства), в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», приказом Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке и информационных системах персональных данных», Приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 № 152 «Об утверждении Инструкции 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», руководящим документом «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», утвержденным решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30.03.1992, **п р и к а з ы в а ю**:

1. Утвердить прилагаемые:

1) Положение об управлении доступом субъектов доступа к объектам доступа в ИСПДн министерства;

2) Правила идентификации и аутентификации субъектов доступа и объектов доступа в ИСПДн министерства;

3) Правила регистрации событий безопасности в ИСПДн министерства;

4) Перечень событий безопасности в событий безопасности в информационных системах министерства образования Новосибирской области;

5) Описание технологического процесса обработки информации ограниченного доступа в информационных системах министерства образования Новосибирской области;

6) Инструкцию по контролю защищенности информации в информационных системах министерства образования Новосибирской области;

7) Матрицу доступа субъектов доступа по отношению к защищаемым информационным ресурсам в информационных системах министерства образования Новосибирской области;

8) форму журнала хранилищ (сейфов) для хранения средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов.

2. Признать утратившими силу приказ министерства образования, науки и инновационной политики Новосибирской области от 27.02.2017 № 408 «Об утверждении Положения об управлении доступом субъектов доступа к объектам доступа в информационной системе персональных данных министерства образования Новосибирской области».

3. Контроль за исполнением требований настоящего оставляю за собой.

Министр С.В. Федорчук

УТВЕРЖДЕНО
приказом Минобразования
Новосибирской области
от 18.02.19 № 336

ПОЛОЖЕНИЕ
об управлении доступом субъектов доступа к объектам доступа в информационной системе персональных данных министерства образования Новосибирской области

I. Общие положения

1. Настоящее Положение определяет права и привилегии субъектов доступа, описывает разграничение доступа субъектов доступа к объектам доступа на основе совокупности правил разграничения доступа, установленных в информационных системах персональных данных министерства образования Новосибирской области (далее – министерство), а также контроль соблюдения этих правил.

2. Разграничение прав осуществляется на основании «Модели угроз безопасности персональных данных при их обработке в ИСПДн Минобразования Новосибирской области», а также исходя из характера и режима обработки персональных данных в ИСПДн министерства.

3. Уровень прав доступа представлен в Таблице 1.

Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование ИСПДн, осуществляется в соответствии с их должностными обязанностями. Доступ к объектам доступа с учетом разделения полномочий (ролей) обеспечивается в соответствии с матрицей субъектов доступа по отношению к защищаемым информационным ресурсам в информационных системах министерства образования Новосибирской области (далее – матрица доступа).

Таблица 1

№ п/п	Группа	Уровень доступа к ПДн, ТС, прикладному ПО и СЗИ	Разрешенные действия
1	Администратор ИСПДн	Доступ на правах администратора к ПДн, ТС и прикладному ПО. Без доступа к СЗИ	1) модернизация, настройка и мониторинг работоспособности комплекса ТС (серверов, рабочих станций); 2) установка, модернизация, настройка и мониторинг работоспособности системного и базового ПО;

№ п/п	Группа	Уровень доступа к ПДн, ТС, прикладному ПО и СЗИ	Разрешенные действия
			3) установка, настройка и мониторинг прикладного ПО; 4) соблюдение правил, оговоренных в инструкции администратора.
2	Администратор ИБ ИСПДн	Доступ на правах администратора к СЗИ. Без доступа на изменение к ПДн, ТС и прикладному ПО	1) разработка, управление и реализация эффективной политики информационной безопасности системы; 2) управление (администрирование) системой защиты информации ИСПДн; 3) выявление инцидентов и реагирование на них; управление конфигурацией ИСПДн и ее системы защиты; 4) контроль (мониторинг) за обеспечением уровня защищенности информации, содержащейся в ИСПДн; управление правами доступа пользователей к функциям системы; 5) проверка состояния используемых СЗИ от НСД, проверка правильности их настройки; 6) обеспечение функционирования и поддержание работоспособности СЗИ; проведение инструктажа эксплуатационного персонала и пользователей СВТ по правилам работы с используемыми СЗИ; 7) контроль и предотвращение несанкционированного изменения целостности ресурсов; 8) контроль аппаратной конфигурации защищаемых компьютеров и предотвращение попытки ее несанкционированного изменения.
3	Администратор ВИ	Доступ на правах администратора к прикладному ПО. Без доступа на изменение ПДн, ТС и СЗИ	1) установка, модернизация, настройка и мониторинг работоспособности ВИ; 2) доступ к операциям создания, запуска, останова, создания копий, удаления виртуальных машин; 3) доступ к конфигурации

№ п/п	Группа	Уровень доступа к ПДн, ТС, прикладному ПО и СЗИ	Разрешенные действия
			виртуальных машин.
4	Администратор резервного копирования	Доступ на правах администратора к прикладному ПО. Без доступа на изменение ПДн, ТС и СЗИ	1) настройка и контроль работы процедуры резервного копирования; 2) изготовление резервных копий информации; 3) анализ объемов данных резервного копирования; 4) контроль состояния оборудования системы резервного копирования; 5) замена неработоспособных или выработавших свой ресурс носителей резервной информации или оборудования системы резервного копирования; 6) восстановление программ и данных из резервных копий в случае порчи или утери данных.
5	Ответственный за эксплуатацию СКЗИ	Доступ на правах администратора к сертифицированным СКЗИ. Без доступа на изменение к ПДн, ТС, прикладному ПО, СЗИ	1) поэкземплярный учет используемых криптосредств, эксплуатационной и технической документации к ним; 2) контроль за соблюдением условий использования криптосредств, установленных эксплуатационной и технической документацией на СКЗИ и настоящей инструкцией; 3) учет Пользователей криптосредств; 4) надежное хранение эксплуатационной и технической документации к криптосредствам, ключевых документов, носителей дистрибутивов криптосредств, бумажных и машинных носителей ПДн; 5) расследования и составление заключений по фактам нарушения условий использования СКЗИ, которые могут привести к снижению требуемого уровня безопасности информации; 6) разработка и принятие мер по предотвращению возможных

№ п/п	Группа	Уровень доступа к ПДн, ТС, прикладному ПО и СЗИ	Разрешенные действия
			негативных последствий нарушений.
6	Пользователь	Доступ на правах пользователя к ПДн, ТС, прикладному ПО и СЗИ. Без доступа на изменение ПО, СЗИ и ТС	Сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, предоставление записей, содержащих ПДн.

4. Доступ в помещения, в которых расположены технические средства ИСПДн министерства (далее – Помещения), осуществляется в соответствии с перечнем лиц, утверждаемым приказом министерства.

II. Правила разграничения доступа

5. В ИСПДн министерства реализуется:

1) управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей, возлагается на администратора ИБ, а также внутри виртуальных машин на администратора ВИ, путем следующих функций:

а) определение типа учетной записи (внутреннего пользователя, внешнего пользователя; системная, приложения; гостевая (анонимная), временная и (или) иные типы записей);

б) объединение учетных записей в группы (при необходимости);

в) верификация пользователя (проверка личности пользователя, его должностных (функциональных) обязанностей) при заведении учетной записи пользователя;

г) заведение, активация, блокирование и уничтожение учетных записей пользователей (при необходимости);

д) пересмотр и, при необходимости, корректировка учетных записей не реже одного раза в три месяца;

е) уничтожение временных учетных записей пользователей, предоставленных для однократного (ограниченного по времени) выполнения задач в информационной системе;

ж) предоставление пользователям прав доступа к объектам доступа ИСПДн, основываясь на задачах, решаемых пользователями в ИСПДн и взаимодействующими с ней ИСПДн.

Временная учетная запись может быть заведена для пользователя на ограниченный срок для выполнения задач, требующих расширенных полномочий, или для проведения настройки, тестирования информационной системы, для организации гостевого доступа (посетителям, сотрудникам

сторонних организаций, стажерам и иным пользователям с временным доступом к информационной системе).

Заведение временных учетных записей осуществляется на основании подписанного администратором ИБ и ответственным за обработку и защиту персональных данных, соответствующего Акта, содержащего цель, место, наименование и сроки;

2) дискреционный метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе идентификационной информации субъекта и для каждого объекта доступа – списка, содержащего набор субъектов доступа (групп субъектов) и ассоциированных с ними типов доступа. Типы доступа должны включать операции по чтению, записи, удалению, выполнению и иные операции, разрешенные к выполнению пользователем (группе пользователей).

Правила разграничения доступа реализуются на основе матрицы доступа и обеспечивают управление доступом пользователей (групп пользователей) и запускаемых от их имени процессов при входе в систему, доступе к ТС, устройствам (в том числе внешним), объектам файловой системы, запускаемым и исполняемым модулям, объектам СУБД, параметрам настройки СЗИ, в том числе внутри виртуальных машин, информации о конфигурации системы защиты информации и иной информации о функционировании системы защиты информации.

В ИСПДн министерства правила разграничения доступа должны обеспечивать:

а) управление доступом субъектов при входе в ИСПДн;

б) управление доступом субъектов к ТС, устройствам, внешним устройствам;

в) управление доступом субъектов к объектам, создаваемым общесистемным (общим) ПО;

г) управление доступом субъектов внутри виртуальной инфраструктуры;

3) в ИСПДн министерства осуществляется управление информационными потоками при передаче информации между устройствами, сегментами в рамках информационной системы, включающее:

а) фильтрацию информационных потоков в соответствии с установленными правилами управления потоками;

б) разрешение передачи информации в ИСПДн министерства только по установленному маршруту;

в) изменение (перенаправление) маршрута передачи информации в случаях необходимости, по согласованию с администратором информационной безопасности;

4) права и привилегии, назначаемые пользователям и запускаемым от их имени процессам, администраторам и лицам, обеспечивающим функционирование ИСПДн министерства, являются минимально необходимыми для выполнения ими своих должностных обязанностей (функций);

5) ограничение неуспешных попыток входа в ИСПДн (доступа к ИСПДн), равное 5 (пяти), при этом обеспечивается блокирование устройства, с которого предпринимаются попытки доступа, и (или) учетной записи пользователя при

превышении пользователем ограничения количества неуспешных попыток входа в ИСПДн (доступа к ИСПДн) не менее чем на 5 (пять) минут;

6) блокирование сеанса доступа в ИСПДн министерства, после 15 минут времени бездействия (неактивности) пользователя или по его запросу.

Блокирование сеанса доступа пользователя в ИСПДн обеспечивает временное приостановление работы пользователя со СВТ или с виртуальной машиной, с которого осуществляется доступ к ИСПДн министерства (без выхода из ИСПДн).

Для заблокированного сеанса осуществляется блокирование любых действий по доступу к информации и устройствам отображения, кроме необходимых для разблокирования сеанса.

Блокирование сеанса доступа пользователя в ИСПДн сохраняется до прохождения им повторной идентификации и аутентификации;

7) запрет всех действий пользователей до прохождения процедур идентификации и аутентификации в ИСПДн (кроме необходимых для прохождения процедур идентификации и аутентификации).

Администратору ИБ разрешаются действия в обход установленных процедур идентификации и аутентификации, необходимые только для восстановления функционирования ИСПДн в случае сбоев в работе или выходе из строя отдельных ТС (устройств).

Применяемые термины и сокращения:

Аутентификационная информация (информация аутентификации)	–	информация, используемая для установления подлинности (верификации) субъекта доступа в информационной системе
Аутентификация	–	проверка принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности субъекта доступа в информационной системе)
Идентификатор	–	представление (строка символов), однозначно идентифицирующее субъект и (или) объект доступа в информационной системе
Идентификация	–	присвоение субъектам доступа, объектам доступа идентификаторов (уникальных имен) и (или) сравнение предъявленного идентификатора с перечнем присвоенных идентификаторов
Локальный доступ	–	доступ субъектов доступа к объектам доступа, осуществляемый непосредственно через подключение (доступ) к компоненту информационной системы или через локальную вычислительную сеть (без использования информационно-телекоммуникационной сети)

Многофакторная аутентификация	–	аутентификация с использованием двух (двухфакторная) или более различных факторов аутентификации
Непривилегированная учетная запись	–	учетная запись пользователя (процесса, выполняемого от его имени) информационной системы
Объект доступа	–	единица информационного ресурса информационной системы (файл, техническое средство, узел сети, линия (канал) связи, мобильное устройство, программа, том, каталог, запись, поле записей и иные объекты), доступ к которой регламентируется правилами разграничения доступа и по отношению к которой субъекты доступа выполняют операции
Пользователь	–	лицо, которому разрешено выполнять некоторые действия (операции) по обработке информации в информационной системе или использующее результаты ее функционирования
Привилегированная учетная запись	–	учетная запись администратора информационной системы
Роль	–	предопределенная совокупность правил, устанавливающих допустимое взаимодействие между пользователем и информационной системой
Субъект доступа	–	пользователь, процесс, выполняющие операции (действия) над объектами доступа и действия которых регламентируются правилами разграничения доступа
Удаленный доступ	–	процесс получения доступа (через внешнюю сеть) к объектам доступа информационной системы из другой информационной системы (сети) или со средства вычислительной техники, не являющегося постоянно (непосредственно) соединенным физически или логически с информационной системой, к которой он получает доступ
Управление доступом	–	ограничение и контроль доступа субъектов доступа к объектам доступа в информационной системе в соответствии с установленными правилами разграничения доступа
ВИ	–	виртуальная инфраструктура
ИБ	–	информационная безопасность
ИСПДн	–	информационная система персональных

		данных
НСД	–	несанкционированный доступ
ПО	–	программное обеспечение
СВТ	–	средство вычислительной техники
СЗИ	–	средство защиты информации
СКЗИ	–	средство криптографической защиты информации
СУБД	–	система управления базой данных
ТС	–	техническое средство

УТВЕРЖДЕНЫ
приказом Минобразования
Новосибирской области
от «18» 02.2019 г. №336

ПРАВИЛА
идентификации и аутентификации субъектов доступа и объектов доступа в информационной системе персональных данных министерства образования Новосибирской области

I. Общие положения

1. Настоящие Правила регламентируют порядок и процедуры присвоения субъектам и объектам доступа уникального признака (идентификатора), сравнения предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверки принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности), а также организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационной системе персональных данных (далее – ИСПДн) министерства образования Новосибирской области (далее – Минобразования Новосибирской области) и контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

II. Идентификация и аутентификация пользователей, являющихся внутренними пользователями

2. При доступе в информационную систему персональных данных (далее – ИСПДн) осуществляется идентификация и аутентификация пользователей, являющихся сотрудниками Минобразования Новосибирской области (внутренних пользователей), и процессов, запускаемых от имени этих пользователей, а также процессов, запускаемых от имени системных учетных записей. К внутренним пользователям относятся следующие должностные лица Минобразования Новосибирской области:

1) администратор ИСПДн;

2) администратор информационной безопасности (далее – ИБ) ИСПДн;

3) администратор резервного копирования;

4) ответственные сотрудники, выполняющие при эксплуатации ИСПДн свои должностные обязанности (функции) в соответствии с должностными регламентами (инструкциями), утвержденными в министерстве и которым в ИСПДн присвоены учетные записи;

5) администратор виртуальной инфраструктуры (ВИ).

В качестве внутренних пользователей дополнительно рассматриваются должностные лица обладателя информации, заказчика, уполномоченного лица и (или) оператора иной информационной системы, а также лица, привлекаемые на договорной основе для обеспечения функционирования ИСПДн (ремонт, гарантийное обслуживание, регламентные и иные работы) в соответствии с организационно-распорядительными документами. Для каждого внутреннего пользователя в ИСПДн должны быть заведены учетные записи.

3. Пользователи ИСПДн однозначно идентифицируются и аутентифицируются для всех видов доступа, кроме тех видов доступа, которые определяются как действия, разрешенные до идентификации и аутентификации в соответствии с Положением об управлении доступом субъектов доступа к объектам доступа в ИСПДн Минобразования Новосибирской области.

4. Аутентификация пользователя в ИСПДн осуществляется с использованием паролей. Также на усмотрение администратора ИБ ИСПДн могут применяться аппаратные средства в случае многофакторной (двухфакторной) аутентификации.

5. В ИСПДн обеспечивается возможность однозначного сопоставления идентификатора пользователя с запускаемыми от его имени процессами.

III. Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов

6. В ИСПДн устанавливаются и реализуются следующие функции управления идентификаторами пользователей и устройств:

1) формирование идентификатора, который однозначно идентифицирует пользователя и (или) устройство;

2) присвоение идентификатора пользователю и (или) устройству;

3) предотвращение повторного использования идентификатора пользователя и (или) устройства в течение одного года;

4) блокирование идентификатора пользователя после 90 дней неиспользования;

5) В качестве ответственного за создание, присвоение и уничтожение идентификаторов пользователей и устройств определен Администратор ИБ ИСПДн.

IV. Управление средствами аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации

7. В ИСПДн устанавливаются и реализуются следующие функции управления средствами аутентификации (аутентификационной информацией) пользователей:

1) изменение аутентификационной информации (средств аутентификации), заданных их производителями и (или) используемых при внедрении системы защиты ИСПДн;

2) выдача средств аутентификации пользователям;

3) генерация и выдача начальной аутентификационной информации (начальных значений средств аутентификации);

4) установление характеристик пароля: длина пароля не менее шести символов, алфавит пароля не менее 6 символов, максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки 5 попыток, блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 15 минут, смена паролей не более чем через 120 дней;

5) блокирование (прекращение действия) и замена утерянных, скомпрометированных или поврежденных средств аутентификации;

6) назначение необходимых характеристик средств аутентификации (в том числе механизма пароля);

7) обновление аутентификационной информации (замена средств аутентификации) с периодичностью не более, чем через 120 дней;

8) защита аутентификационной информации от неправомерных доступа к ней и модифицирования.

8. В случае компрометации личного пароля пользователя ИСПДн должны быть немедленно предприняты меры в зависимости от полномочий владельца скомпрометированного пароля:

1) внеплановая смена личного пароля или удаление учетной записи пользователя ИСПДн в случае прекращения его полномочий (увольнение, переход на другую работу внутри организации и т.п.) должна производиться Администратором ИБ ИСПДн немедленно после окончания последнего сеанса работы данного пользователя с системой;

2) внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри организации и другие обстоятельства) Администратора ИБ ИСПДн и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой ИСПДн.

9. В качестве ответственного за хранение, выдачу, инициализацию, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации устройств определен Администратор ИБ ИСПДн.

V. Защита обратной связи при вводе аутентификационной информации

10. В ИСПДн осуществляется защита аутентификационной информации в процессе ее ввода для аутентификации от возможного использования лицами, не имеющими на это полномочий.

11. Защита обратной связи «система – субъект доступа» в процессе аутентификации обеспечивается исключением отображения для пользователя действительного значения аутентификационной информации и (или) количества вводимых пользователем символов аутентификационной информации. Вводимые символы пароля могут отображаться условными знаками«*»,«•» или иными знаками.

VI. Ответственность при организации идентификации и аутентификации

12. Ответственность за реализацию правил идентификации и аутентификации субъектов доступа и объектов доступа в соответствии с требованиями настоящих Правил возлагается на Администратора ИБ ИСПДн.

13. Ответственность за поддержание установленного порядка и соблюдение требований настоящих Правил возлагается на Администратора ИБ ИСПДн и пользователей ИСПДн.

14. Периодический контроль за выполнением всех требований настоящих Правил осуществляется комиссией по проведению мероприятий по защите персональных данных.

Утверждены
приказом Минобразования
Новосибирской области
от 18.02.2019 г. № 336

ПРАВИЛА
регистрации событий безопасности в информационной системе персональных данных министерства образования Новосибирской области

I. Общие положения

1. Настоящие Правила регламентируют состав и содержание информации о событиях безопасности, подлежащих регистрации, правила и процедуры сбора, записи, хранения и защиты информации о событиях безопасности в информационной системе персональных данных (далее – ИСПДн) министерства образования Новосибирской области (далее –Минобразования Новосибирской области).

II. Определение событий безопасности, подлежащих регистрации, и сроков их хранения

2. В ИСПДн подлежат регистрации в текущий момент времени следующие события безопасности:

№ п/п	События безопасности, подлежащие регистрации	Состав и содержание информации о событиях безопасности
1	Вход (выход), а также попытки входа субъектов доступа в информационную систему и загрузки (останова) операционной системы	Дата и время входа (выхода) в систему (из системы) или загрузки (останова) операционной системы, результат попытки входа (успешная или неуспешная), результат попытки загрузки (останова) операционной системы (успешная или неуспешная), идентификатор, предъявленный при попытке доступа.
2	Подключение машинных носителей информации и вывод информации на носители информации	Дата и время подключения машинных носителей информации и вывода информации на носители информации, логическое имя (номер) подключаемого машинного носителя информации,

		идентификатор субъекта доступа, осуществляющего вывод информации на носитель информации.
3	Запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации	Дата и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный).
4	Попытки доступа программных средств к защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей)	Дата и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого файла (логическое имя, тип).
5	Попытки удаленного доступа	Дата и время попытки удаленного доступа с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), используемый протокол доступа, используемый интерфейс доступа и (или) иную информацию о попытках удаленного доступа к информационной системе.
6	Доступ субъектов доступа к компонентам виртуальной инфраструктуры	Дата и время доступа субъектов доступа к гипервизору и виртуальной машине, к хостовой операционной системе, результат попытки доступа субъектов доступа к указанным компонентам виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке доступа субъектов доступа к компонентам виртуальной инфраструктуры.
7	Изменения в составе и конфигурации компонентов виртуальной инфраструктуры во время их запуска, функционирования и аппаратного отключения	Дата и время изменения в составе и конфигурации виртуальных машин, виртуального аппаратного обеспечения, виртуализированного программного обеспечения, виртуального аппаратного обеспечения в гипервизоре и в виртуальных машинах, в хостовой операционной системе, виртуальном сетевом оборудовании, результат

		попытки изменения в составе и конфигурации указанных компонентов виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке изменения в составе и конфигурации компонентов виртуальной инфраструктуры.
8	Изменения правил разграничения доступа к компонентам виртуальной инфраструктуры	Дата и время изменения правил разграничения доступа к виртуальному и физическому аппаратному обеспечению, к файлам-образам виртуализированного программного обеспечения и виртуальных машин, к файлам-образам, используемым для обеспечения работы виртуальных файловых систем, к виртуальному сетевому оборудованию, к защищаемой информации, хранимой и обрабатываемой в гипервизоре и виртуальных машинах, в хостовой операционной системе, результат попытки изменения правил разграничения доступа к указанным компонентам виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке изменения правил разграничения доступа к компонентам виртуальной инфраструктуры.

3. Сроки хранения соответствующих записей регистрационных журналов должны обеспечивать возможность обнаружения, идентификации и анализа инцидентов, возникших в ИСПДн, в течение 3-х месяцев.

III. Определение состава и содержания информации о событиях безопасности, подлежащих регистрации

4. Состав и содержание информации о событиях безопасности, включаемой в записи регистрации о событиях безопасности, должны, как минимум, обеспечить возможность идентификации типа события безопасности, даты и времени события безопасности, идентификационной информации источника события безопасности, результат события безопасности (успешно или неуспешно), субъект доступа (пользователь и (или) процесс), связанный с данным событием безопасности.

5. Состав и содержание информации о событиях безопасности, включаемой в записи регистрации о событиях безопасности, приведены в пункте 2 настоящих Правил.

IV. Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения

6. Процедуры сбора, записи и хранения информации о событиях безопасности в течение установленного времени хранения предусматривают:

1) возможность выбора администратором информационной безопасности событий безопасности, подлежащих регистрации в текущий момент времени из перечня событий безопасности, определенных в пункте 2 настоящих Правил;

2) генерацию (сбор, запись) записей регистрации (аудита) для событий безопасности, подлежащих регистрации (аудиту) в соответствии с пунктом 2 настоящих Правил, с составом и содержанием информации, установленными для соответствующего типа события;

3) хранение информации о событиях безопасности в течение времени, установленного в соответствии с пунктом 3 настоящих Правил.

7. Объем памяти для хранения информации о событиях безопасности рассчитывается и выделяется администратором информационной безопасности ИСПДн Фонда с учетом типов событий безопасности, подлежащих регистрации в соответствии с в пункте 2 настоящих Правил, составом и содержанием информации о событиях безопасности, подлежащих регистрации, прогнозируемой частоты возникновения подлежащих регистрации событий безопасности, срока хранения информации о зарегистрированных событиях безопасности.

V. Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них

8. Мониторинг (просмотр и анализ) записей регистрации (аудита) должен проводиться администратором информационной безопасности не реже двух раз в месяц для всех событий, подлежащих регистрации, и обеспечивать своевременное выявление признаков инцидентов безопасности в ИСПДн.

9. В случае выявления признаков инцидентов безопасности в ИСПДн администратор информационной безопасности осуществляет планирование и проведение мероприятий по реагированию на выявленные инциденты безопасности.

VI. Защита информации о событиях безопасности

10. Защита информации о событиях безопасности (записях регистрации (аудита)) в ИСПДн должна обеспечиваться применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования, определенных в проектной и организационно-распорядительной документации по защите информации, и в том числе включает защиту средств ведения регистрации (аудита) и настроек механизмов регистрации событий.

11. Доступ к записям аудита и функциям управления механизмами регистрации (аудита) предоставляется только администратору информационной безопасности и администратору виртуальной инфраструктуры.

Утвержден
приказом Минобразования
Новосибирской области
от «18»02.2019г. № 336

ПЕРЕЧЕНЬ
событий безопасности в информационных системах министерства образования Новосибирской области

№ п/п	Событие безопасности, подлежащие регистрации	Состав и содержание регистрационных записей
1	Вход (выход), а также попытки входа субъектов доступа в информационную систему и загрузки (останова) операционной системы	Дата и время входа (выхода) в систему (из системы) или загрузки (останова) операционной системы, результат попытки входа (успешная или неуспешная), результат попытки загрузки (останова) операционной системы (успешная или неуспешная), идентификатор, предъявленный при попытке доступа
2	Подключение машинных носителей информации и вывод информации на носители информации	Дата и время подключения машинных носителей информации и вывода информации на носители информации, логическое имя (номер) подключаемого машинного носителя информации, идентификатор субъекта доступа, осуществляющего вывод информации на носитель информации
3	Запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации	Дата и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный)
4	Попытки доступа программных средств к защищаемым объектам доступа	Дата и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого файла (логическое имя, тип)
5	Попытки удаленного доступа	Дата и время попытки удаленного доступа с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), используемый протокол доступа, используемый интерфейс доступа и (или) иную информацию о попытках удаленного доступа к информационной системе

№ п/п	Событие безопасности, подлежащие регистрации	Состав и содержание регистрационных записей
6	Запуск (завершение) работы компонентов виртуальной инфраструктуры	Дата и время запуска (завершения) работы гипервизора и виртуальных машин, хостовой операционной системы, программ и процессов в виртуальных машинах, результат запуска (завершения) работы указанных компонентов виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке запуска (завершения) работы компонентов виртуальной инфраструктуры
7	Доступ субъектов доступа к компонентам виртуальной инфраструктуры	Дата и время доступа субъектов доступа к гипервизору и виртуальной машине, к хостовой операционной системе, результат попытки доступа субъектов доступа к указанным компонентам виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке доступа субъектов доступа к компонентам виртуальной инфраструктуры
8	Изменения в составе и конфигурации компонентов виртуальной инфраструктуры во время их запуска, функционирования и аппаратного отключения	Дата и время изменения в составе и конфигурации виртуальных машин, виртуального аппаратного обеспечения, виртуализированного программного обеспечения, виртуального аппаратного обеспечения в гипервизоре и в виртуальных машинах, в хостовой операционной системе, виртуальном сетевом оборудовании, результат попытки изменения в составе и конфигурации указанных компонентов виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке изменения в составе и конфигурации компонентов виртуальной инфраструктуры
9	Изменения правил разграничения доступа к компонентам виртуальной инфраструктуры	Дата и время изменения правил разграничения доступа к виртуальному и физическому аппаратному обеспечению, к файлам-образам виртуализированного программного обеспечения и виртуальных машин, к файлам-образам, используемым для обеспечения работы виртуальных файловых систем, к виртуальному сетевому оборудованию, к защищаемой информации, хранимой и обрабатываемой в гипервизоре и виртуальных машинах, в хостовой операционной системе, результат попытки изменения правил разграничения доступа к указанным компонентам виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке изменения правил разграничения доступа к компонентам виртуальной инфраструктуры

Лист регистрации изменений

Изм.	Номера пунктов				Всего пунктов в докум.	№ докум.	Вх. № докум. и дата	Подп.	Дата
	изменен-ных	заменен-ных	новых	аннулиро-ванных					

Утверждено
приказом Минобазования
Новосибирской области
от 18.02.2019 № 336

ОПИСАНИЕ
технологического процесса обработки информации ограниченного доступа в информационных системах министерства образования Новосибирской области

Перечень условных обозначений и сокращений

АРМ	–	Автоматизированное рабочее место
ВТСС	–	Вспомогательные технические средства и системы
ИБ	–	Информационная безопасность
ИС	–	Информационная система
КЗ	–	Контролируемая зона
ЛВС	–	Локально-вычислительная сеть
НСД	–	Несанкционированный доступ
ОС	–	Операционная система
ОТСС	–	Основные технические средства и системы
ПДн	–	Персональные данные
ПО	–	Программное обеспечение
ППО	–	Прикладное программное обеспечение
СВТ	–	Средства вычислительной техники
СЗИ	–	Средства защиты информации
ТС	–	Техническое средство

1 Описание объекта информатизации

1.1 Общие сведения

Описание информационных систем министерства образования Новосибирской области (далее – ИС Минобразования Новосибирской области) и состав информации ограниченного доступа (в том числе ПДн), не содержащей сведения, составляющие государственную тайну (далее – Информация), приведены в таблице 1.

Основные элементы ИС, объекты и субъекты доступа, источники информации, состав программного обеспечения, участвующего в технологическом процессе обработки информации, а также класс защищенности автоматизированной системы приведены в п. 1.3-1.8 настоящего документа.

Адреса местонахождения ИС Минобразования Новосибирской области: 630007, г. Новосибирск, Красный проспект, 18; 630099, г. Новосибирск, ул. Чаплыгина, 29; 630073, г. Новосибирск, ул. Блюхера, 40; 630091, г. Новосибирск, ул. Мичурина, 19.

1.2 Назначение и решаемые задачи

ИС Минобразования Новосибирской области созданы в связи с реализацией трудовых отношений, для оказания государственных услуг и исполнения государственных функций в целях, указанных в таблице 1 настоящего документа.

1.3 Состав ИС

Основными элементами ИС являются:

- Информация;
- технические средства ИС, осуществляющие обработку Информации (СВТ, компоненты ЛВС, средства и системы передачи, приема и обработки Информации);
- программные средства (ОС, общесистемное и прикладное ПО);
- СЗИ;
- ВТСС, их коммуникации, средства и системы передачи данных, средства и системы охранной и пожарной сигнализации, средства и системы оповещения и сигнализации, не предназначенные для обработки Информации, но размещенные в помещениях, в которых расположены технические средства ИС;
- информационные технологии.

1.4 Объекты доступа

Объектами доступа являются:

- ИС в целом;
- технические средства отображения информации;
- материальные носители информации;
- оперативная память АРМ;
- файлы подкачки – [C:\pagefile.sys].

1.5 Субъекты доступа

Субъектами доступа в ИС являются:

- пользователи ИС Минобразования Новосибирской области, указанные в п. 2.1.1 настоящего документа, и их учетные записи;
- программы (процессы), используемые для обработки информации и администрирования ИС Минобразования Новосибирской области.

1.6 Источники информации

Информация поступает непосредственно от субъекта ПДн.

1.7 Состав технических средств и программного обеспечения, участвующего в технологическом процессе обработки информации

Перечень и состав ОТСС приведен в Техническом паспорте объекта информатизации министерства образования Новосибирской области (далее – Технический паспорт ОИ Минобразования Новосибирской области). Обработка Информации на АРМ производится с использованием ПО, приведенного в Перечне программного обеспечения, разрешенного к использованию в информационных системах министерства образования Новосибирской области.

1.8 Класс защищенности автоматизированной системы

В соответствии с Актом определения УЗ ПДн в ИС Минобразования Новосибирской области и Актом классификации ИС Минобразования Новосибирской области, составленных постоянно действующей экспертной комиссией по проведению мероприятий по защите персональных данных, контролю за соблюдением порядка обращения с документами, содержащими персональные данные, назначенной приказом «О проведении мероприятий по защите персональных данных» (далее – Приказ «О проведении мероприятий»), для ИС Минобразования Новосибирской области признано необходимым обеспечение 4-го уровня защищенности ПДн и третьего класса защищенности (К3) ИС Минобразования Новосибирской области.

2. Организация работы с Информацией

2.1 Доступ пользователя к работе на автоматизированной системе

2.1.1.Пользователи информационной системы

Пользователями ИС Минобразования Новосибирской области (далее – Пользователи) являются:

– ответственный за обработку и защиту Информации согласно Приказу «Об ответственном за организацию обработки персональных данных в министерстве образования Новосибирской области»;

– администратор информационной системы персональных данных согласно Приказу «Об обеспечении технической защиты персональных данных» (далее – Приказ «Об обеспечении технической защиты»);

– администратор информационной безопасности (далее – администратор ИБ) согласно Приказу «Об обеспечении технической защиты»;

– администратор резервного копирования согласно Приказу «**О** назначении ответственного по резервному копированию данных»;

– ответственный пользователь за эксплуатацию СКЗИ согласно Приказу «О назначении ответственного за эксплуатацию СКЗИ в министерстве образования Новосибирской области»;

– работники Минобразования Новосибирской области в соответствии с Перечнем лиц, имеющих право доступа в помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой и парольной информации СКЗИ информационных систем министерства образования Новосибирской.

2.1.2. Правила доступа к техническим средствам и информационным ресурсам ИС

Контролируемая зона (КЗ) ИС Минобразования Новосибирской области определена в приказе «О проведении мероприятий».

Регистрация пользователей, не являющихся работниками оператора, не предусмотрена.

Перед началом сеанса работы Пользователь включает АРМ и проходит процедуру аутентификации при входе в ОС семейства Windows. По окончании загрузки АРМ Пользователь получает установленные администратором ИБ права доступа к устройствам, программам, каталогам и файлам АРМ.

После завершения работы в ИС Пользователь (за исключением внешних пользователей) выполняет одно из следующих действий:

– выключает компьютер в случае, если не планируется дальнейшая обработка информации;

– при временном оставлении рабочего места производит блокировку АРМ путем нажатия комбинации клавиш <Ctrl-Alt-Del> и выбора в диалоговом окне кнопки «Блокировать» либо путем нажатия комбинации клавиш <Win-L>. Разблокирование АРМ производится путем ввода пароля Пользователя.

Разграничение прав доступа к техническим средствам ИС и установление полномочий реализуется на основе принятых ролевых моделей, принципов разделения обязанностей и минимизации полномочий с использованием средств аутентификации и авторизации в соответствии с Матрицей доступа субъектов доступа по отношению к защищаемым информационным ресурсам в информационных системах министерства образования Новосибирской области (далее – Матрица доступа) и Положением об управлении доступом субъектов доступа к объектам доступа в информационных системах министерства образования Новосибирской области, утвержденными в Минобразования Новосибирской области.

Разграничение прав доступа к информационным ресурсам ИС (защищаемой информации) осуществляется по группам пользователей, указанных в п. 2.1.1, по принципу минимизации прав и привилегий, необходимых для выполнения ими своих должностных обязанностей (функций) в соответствии с должностными инструкциями.

Разграничение прав доступа к защищаемой информации для конкретных пользователей осуществляется средством защиты информации от несанкционированного доступа (далее – СЗИ от НСД) Dallas Lock 8.0-К. Настройки СЗИ от НСД в соответствии с Матрицей доступа приведены в Протоколе настроек системы защиты информации на объекте информатизации министерства образования Новосибирской области.

2.2. Обработка Информации в ИС Минобразования Новосибирской области

ИС Минобразования Новосибирской области являются информационными системами с подключением к внешним информационным системам, в том числе сетям общего пользования.

ИС Минобразования Новосибирской области строятся на базе локальной вычислительной сети Минобразования Новосибирской области с использованием технологии Ethernet, динамической адресацией, топология – «звезда». Доступ в сеть международного информационного обмена предоставляется провайдером ООО «Новотелеком».

В ИС Минобразования Новосибирской области используются технологии виртуализации, мобильного кода и не используются технологии беспроводных соединений и облачные технологии.

В ИС Минобразования Новосибирской области не применяется удаленный доступ.

Передача Информации осуществляется по защищенному каналу связи, с использованием сертифицированного программного комплекса ViPNet Client, установленного на каждой рабочей станции.

Обобщенная схема технологического процесса обработки информации приведена на рисунке 1.

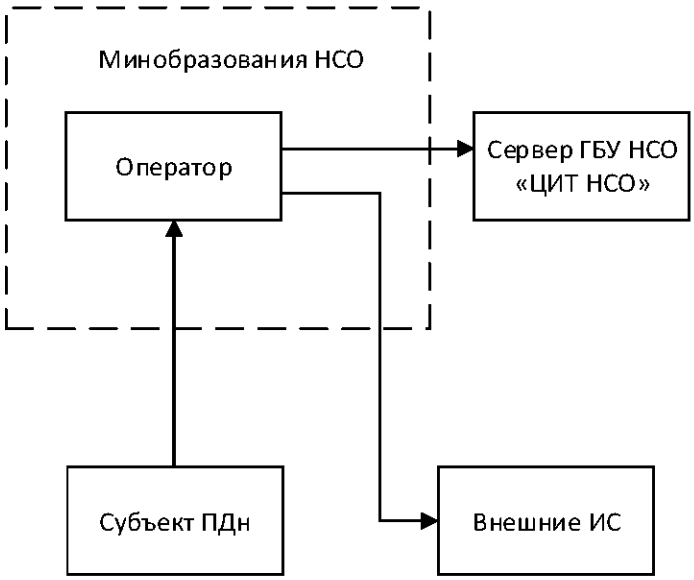

Рисунок 1 – Схема технологического процесса

2.3. Хранение Информации

Технология обработки Информации в ИС предусматривает хранение Информации на бумажных носителях, на виртуальном сервере ИС Минобразования Новосибирской области.

В ИС Минобразования Новосибирской области для обработки Информации не используются мобильные технические средства.

Перечень мест хранения материальных носителей (съемных машинных и бумажных носителей) Информации (в том числе ПДн) приведен в Перечне хранилищ материальных носителей информации ограниченного доступа в информационных системах министерства образования Новосибирской области.

2.4. Печать, сканирование и копирование с бумажных носителей

Разрешения по доступу к принтеру и другим устройствам ввода-вывода информации на «твердую» копию для различных категорий пользователей ИС Минобразования НСО установлены в соответствии с Матрицей доступа.

Размещение ТС в ИС Минобразования Новосибирской области исключает возможность несанкционированного просмотра защищаемой информации с распечаток принтеров и с других устройств ввода-вывода информации лицами, не имеющими права доступа к обрабатываемой информации.

2.5. Удаление электронных документов, содержащих Информацию с жестких дисков

Удаление электронных документов, содержащих Информацию с жестких дисков, в том числе уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для

ремонта или утилизации, а также контроль уничтожения (стирания) осуществляется в соответствии с Правилами обращения с машинными носителями информации в информационных системах министерства образования Новосибирской области (далее – Правила обращения с МНИ).

2.6. Уничтожение съемных носителей

В ИС Минобразования Новосибирской области не используются съемные машинные носители информации.

3. Обеспечение информационной безопасности

Состав средств защиты информации ИС Минобразования Новосибирской области приведен в Техническом паспорте ОИ ИС Минобразования Новосибирской области.

СЗ ИС Минобразования Новосибирской области реализует набор мер в соответствии с Техническим заданием на создание системы защиты информации при ее обработке в информационных системах министерства образования Новосибирской области и возможность адекватно блокировать (нейтрализовать) все угрозы безопасности информации, включенные в Модель угроз и нарушителя безопасности информации при её обработке в информационных системах министерства образования Новосибирской области, либо снизить вероятность их реализации. Состав и содержание мер и усилений по обеспечению безопасности Информации, а также перечень технических средств защиты информации и организационных мер, необходимых для обеспечения безопасности Информации, представлены в Приложении А Пояснительной записки к техническому проекту «Система защиты информации при ее обработке в информационных системах министерства образования Новосибирской области».

УТВЕРЖДЕНА
приказом Минобразования
Новосибирской области
от 18.02.2019 г.№336

ИНСТРУКЦИЯ
по контролю защищенности информации в информационных системах министерства образования Новосибирской области

1. Общие положения

1.1. Настоящая инструкция регламентирует контроль уровня защищенности информации, обрабатываемой в информационных системах министерства образования Новосибирской области (далее – ИС Минобразования Новосибирской области), путем проведения систематических мероприятий по анализу защищенности информационной системы и тестированию работоспособности системы защиты информации.

2. Выявление, анализ и устранение уязвимостей информационной системы

2.1. В ИС Минобразования Новосибирской области при выявлении (поиске), анализе и устранении уязвимостей проводятся:

- выявление (поиск) уязвимостей, связанных с ошибками кода в программном (микропрограммном) обеспечении (общесистемном, прикладном, специальном), а также программном обеспечении средств защиты информации, правильностью установки и настройки средств защиты информации, технических средств и программного обеспечения, а также корректностью работы средств защиты информации при их взаимодействии с техническими средствами и программным обеспечением;
- разработка по результатам выявления (поиска) уязвимостей отчетов с описанием выявленных уязвимостей и планом мероприятий по их устранению;
- анализ отчетов с результатами поиска уязвимостей и оценки достаточности реализованных мер защиты информации;
- устранение выявленных уязвимостей, в том числе путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств;
- информирование должностных лиц Минобразования Новосибирской области (пользователей, администраторов) о результатах поиска уязвимостей и оценки достаточности реализованных мер защиты информации.

2.2. В качестве источников информации об уязвимостях используются опубликованные данные разработчиков средств защиты информации, общесистемного, прикладного и специального программного обеспечения, технических средств, а также другие базы данных уязвимостей.

2.3. Выявление (поиск), анализ и устранение уязвимостей проводится на этапах создания и эксплуатации информационной системы. На этапе

эксплуатации поиск и анализ уязвимостей проводится администраторами не реже одного раза в месяц. При этом в обязательном порядке для критических уязвимостей проводится поиск и анализ уязвимостей в случае опубликования в общедоступных источниках информации о новых уязвимостях в средствах защиты информации, технических средствах и программном обеспечении, применяемом в ИС Минобразования Новосибирской области.

2.4. В случае невозможности устранения выявленных уязвимостей путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств необходимо предпринять действия (корректировка настроек средств защиты информации, изменение режима и порядка использования ИС Минобразования Новосибирской области), направленные на устранение возможности использования выявленных уязвимостей.

2.5. В ИС Минобразования Новосибирской области используются для выявления (поиска) уязвимостей средства анализа (контроля) защищенности (сканеры безопасности), имеющие стандартизованные (унифицированные) в соответствии с национальными стандартами описание и перечни программно-аппаратных платформ, уязвимостей программного обеспечения, ошибочных конфигураций, правил описания уязвимостей, проверочных списков, процедур тестирования и языка тестирования информационной системы на наличие уязвимостей, оценки последствий уязвимостей, имеющие возможность оперативного обновления базы данных выявляемых уязвимостей.

2.6. В ИС Минобразования Новосибирской области осуществляется получение из доверенных источников и установка обновлений базы признаков уязвимостей (для системы анализа защищенности).

2.7. Доступ к функциям выявления (поиска) уязвимостей предоставляется только администратору информационной безопасности и администратору виртуальной инфраструктуры. Администратор информационной безопасности проводит анализ журналов регистрации событий безопасности (журнала аудита) в целях определения, были ли выявленные уязвимости ранее использованы в ИС Минобразования Новосибирской области для нарушения безопасности информации.

3. Контроль установки обновлений программного обеспечения, включая программное обеспечение средств защиты информации

3.1. В ИС Минобразования Новосибирской области администраторами в рамках своих полномочий осуществляется контроль установки обновлений программного обеспечения, включая программное обеспечение средств защиты информации и программное обеспечение базовой системы ввода-вывода.

3.2. В ИС Минобразования Новосибирской области администраторами в рамках своих полномочий осуществляется получение из доверенных источников и установка обновлений программного обеспечения, включая программное обеспечение средств защиты информации и программное обеспечение базовой системы ввода-вывода.

3.3. При контроле установки обновлений осуществляются проверки соответствия версий общесистемного, прикладного и специального программного (микропрограммного) обеспечения, включая программное обеспечение средств защиты информации, установленного в ИС Минобразования Новосибирской области и выпущенного разработчиком, а также наличие отметок в эксплуатационной документации (формуляр или паспорт) об установке (применении) обновлений.

3.4. Контроль установки обновлений проводится не реже одного раза в месяц.

3.5. При контроле установки обновлений осуществляются проверки установки обновлений баз данных признаков вредоносных компьютерных программ (вирусов) средств антивирусной защиты в соответствии с Инструкцией по антивирусной защите в информационных системах министерства образования Новосибирской области, баз признаков уязвимостей средств анализа защищенности и иных баз данных, необходимых для реализации функций безопасности средств защиты информации.

4. Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации

4.1. При контроле работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации, осуществляется:

- контроль работоспособности (неотключения) программного обеспечения и средств защиты информации;
- проверка правильности функционирования (тестирование на тестовых данных, приводящих к известному результату) программного обеспечения и средств защиты информации;
- контроль соответствия настроек программного обеспечения и средств защиты информации параметрам настройки, приведенным в эксплуатационной документации на систему защиты информации и средства защиты информации;
- восстановление работоспособности (правильности функционирования) и параметров настройки программного обеспечения и средств защиты информации (при необходимости), в том числе с использованием резервных копий и (или) дистрибутивов.

4.2. Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации проводится администраторами в рамках своих полномочий не реже одного раза в три месяца.

5. Контроль состава технических средств, программного обеспечения и средств защиты информации

5.1. При контроле состава технических средств, программного обеспечения и средств защиты информации (инвентаризации) осуществляется:

- контроль соответствия состава технических средств, программного обеспечения и средств защиты информации приведенному в эксплуатационной документации с целью поддержания актуальной (установленной в соответствии с эксплуатационной документацией) конфигурации ИС Минобразования Новосибирской области и принятие мер, направленных на устранение выявленных недостатков;
- контроль состава технических средств, программного обеспечения и средств защиты информации на соответствие сведениям действующей (актуализированной) эксплуатационной документации и принятие мер, направленных на устранение выявленных недостатков;
- контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации и принятие мер, направленных на устранение выявленных недостатков;
- исключение (восстановление) из состава ИС Минобразования Новосибирской области несанкционированно установленных (удаленных) технических средств, программного обеспечения и средств защиты информации.

5.2. Контроль состава технических средств, программного обеспечения и средств защиты информации проводится администраторами в рамках своих полномочий не реже одного раза в месяц.

6. Контроль правил генерации и смены паролей пользователей, заведения и удаления учётных записей, реализации правил разграничения доступом, полномочий пользователей в информационной системе

6.1. При контроле правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в ИС Минобразования Новосибирской области осуществляется:
- контроль правил генерации и смены паролей пользователей в соответствии с Правилами идентификации и аутентификации пользователей в информационных системах министерства образования Новосибирской области;
- контроль заведения и удаления учетных записей пользователей в соответствии с Положением об управлении доступом субъектов доступа к объектам доступа в информационных системах министерства образования Новосибирской области;
- контроль реализации правил разграничения доступом в соответствии с Положением об управлении доступом субъектов доступа к объектам доступа в информационных системах министерства образования Новосибирской области;
- контроль реализации полномочий пользователей в соответствии с Положением об управлении доступом субъектов доступа к объектам доступа в информационных системах министерства образования Новосибирской области;
- контроль наличия документов, подтверждающих разрешение изменений учетных записей пользователей, их параметров, правил разграничения доступом и полномочий пользователей, предусмотренных организационно-распорядительными документами по защите информации в Минобразования Новосибирской области;

– устранение нарушений, связанных с генерацией и сменой паролей пользователей, заведением и удалением учетных записей пользователей, реализацией правил разграничения доступом, установлением полномочий пользователей.

6.2. Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в ИС Минобразования Новосибирской области проводится администратором информационной безопасности не реже одного раза в три месяца.

УТВЕРЖДЕНА
приказом Минобразования
Новосибирской области
от 18.02.2019г. № 336

Форма

ЖУРНАЛ

хранилищ (сейфов) для хранения средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов

№ п/п	Наименование хранилища (сейф, металлический шкаф)	Инвентарный номер	Местонахождение (подразделение, номер комнаты)	Что находится (документы, изделия)	ФИО ответственного за хранилище (сейф, шкаф)	Количество комплектов ключей и их номера	Подпись ответственного за хранилище
1	2	3	4	7	8	9	10