МИНИСТЕРСТВО ОБРАЗОВАНИЯ НОВОСИБИРСКОЙ ОБЛАСТИ (МИНОБРНАУКИ НОВОСИБИРСКОЙ ОБЛАСТИ)

ПРИКАЗ

12.12.18 №3223

г. Новосибирск

О внесении изменений в приказ министерства образования Новосибирской области от 07.05.2018 № 1097 и признании утратившими силу отдельных приказов министерства образования, науки и инновационной политики Новосибирской области

П р и к а з ы в а ю:

1. Внести в приказ министерства образования, науки и инновационной политики Новосибирской области от 07.05.2018 № 1097 «Об утверждении инструкций по проведению работ по защите информации в министерстве образования Новосибирской области» следующие изменения:

1) пункт 1 дополнить подпунктами 9, 10 следующего содержания:

«9) Инструкцию пользователя по обеспечению безопасности при возникновении нештатных ситуаций, в информационных системах министерства образования Новосибирской области;

10) Инструкцию по организации парольной защиты в информационных системах персональных данных министерства образования Новосибирской области.»;

2) абзац 31 раздела 3 Инструкции администратора информационной безопасности в министерстве образования Новосибирской области признать утратившим силу;

3) раздел 1 Инструкции оператора информационной системы персональных данных в министерстве образования Новосибирской области дополнить абзацами следующего содержания:

«**Автоматизированная система** – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций;

База данных – объективная форма представления и организации совокупности данных, систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны с помощью электронно-вычислительных машин (далее – ЭВМ);

Информация – сведения (сообщения, данные) независимо от формы их представления;

Персональные данные – любая информация, относящаяся к прямо или

косвенно определённому или определяемому физическому лицу (субъекту персональных данных);

Компрометация пароля – утрата доверия к тому, что используемый пароль обеспечивает безопасность персональных данных. К событиям, приводящим к компрометации пароля, относятся следующие события (включая, но не ограничиваясь):

несанкционированное сообщение пароля другому лицу;

утеря бумажного или машинного носителя информации, на котором был записан пароль;

запись пароля на бумажном, машинном, ином носителе информации, доступ к которому не контролируется;

утеря пароля – события, приводящие к невозможности восстановления пароля в памяти лица, владеющего данным паролем;

Конфиденциальность персональных данных – обязательное для соблюдения лицом, получившим доступ к персональным данным, требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания;

Несанкционированный доступ к персональным данным – доступ к персональным данным с нарушением установленных прав доступа, приводящий к нарушению конфиденциальности персональных данных, к утечке, искажению, подделке, уничтожению, блокированию доступа к персональным данным;

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

Распространение персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

Разглашение персональных данных – распространение персональных данных без согласия субъекта персональных данных или наличия иного законного основания;

Средство защиты информации (СЗИ) – программные, программно-аппаратные, аппаратные средства, предназначенные и используемые для защиты персональных данных в информационных системах персональных данных (далее – ИСПДн);

Электронная вычислительная машина ИСПДн (ЭВМ) – персональный компьютер, предназначенный для автоматизации деятельности пользователей и входящий в состав ИСПДн. В состав ЭВМ входят: системный блок, монитор, клавиатура, мышь, внешние устройства (локальный принтер, сканер и т.д.), программное обеспечение.».

4) в Инструкции о порядке обеспечения конфиденциальности при обработке персональных данных в министерстве образования Новосибирской области:

а) в разделе 1:

в абзаце первом слова «работников, обучающихся, участников единого государственного экзамена (за исключением обучающихся), граждан, привлекаемых к проведению государственной итоговой аттестации, членов предметных комиссий, общественных наблюдателей, слушателей и других лиц» заменить словами «субъектов персональных данных»;

абзац девятый изложить в следующей редакции:

«Список лиц, допущенных к обработке персональных данных в министерстве с использованием средств автоматизации и без использования таких средств, утверждается приказом министерства образования Новосибирской области. Обработка персональных данных лицами, не указанными в приказе, запрещается.»;

в абзаце десятом слово «Учреждение» заменить словом «министерство»;

б) в грифе приложения № 1 слова «по организации парольной защиты на объектах вычислительной техники» заменить словами «о порядке обеспечения конфиденциальности при обработке персональных данных»;

в) в грифе приложения № 2 слова «по организации парольной защиты на объектах вычислительной техники» заменить словами «о порядке обеспечения конфиденциальности при обработке персональных данных»;

г) в грифе приложения № 3 слова «по организации парольной защиты на объектах вычислительной техники» заменить словами «о порядке обеспечения конфиденциальности при обработке персональных данных»;

5) дополнить Инструкцией пользователя по обеспечению безопасности при возникновении нештатных ситуаций, в информационных системах министерства образования Новосибирской области, согласно приложению № 1 к настоящему приказу;

6) дополнить Инструкцией по организации парольной защиты в информационных системах персональных данных министерства образования Новосибирской области, согласно приложению № 2 к настоящему приказу.

2. Признать утратившими силу:

приказ министерства образования, науки и инновационной политики Новосибирской области от 17.04.2013 № 1069 «Об утверждении инструкций»;

приказ министерства образования, науки и инновационной политики Новосибирской области от 09.06.2017 № 1305 «О внесении изменения в приказ министерства образования, науки и инновационной политики Новосибирской области от 17.04.2013 № 1069»;

приказ министерства образования, науки и инновационной политики Новосибирской области от 18.12.2013 № 2867/3 «О внесении изменений в приказ министерства образования, науки и инновационной политики Новосибирской области от 17.04.2013 № 1069».

Министр С.В. Федорчук

ПРИЛОЖЕНИЕ № 1
к приказу Минобразования
Новосибирской области
от 12.12.18 №3223

«УТВЕРЖДЕНА
приказом Минобразования
Новосибирской области
от 07.05.2018 № 1097

ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ
по обеспечению безопасности при возникновении нештатных ситуаций, в информационных системах министерства образования Новосибирской области
(далее – Инструкция)

I. Общие положения

1. Настоящая Инструкция разработана в соответствии с требованиями:

Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

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

приказа ФСТЭК России 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».

2. Данная инструкция определяет порядок действий пользователя при возникновении нештатной ситуации при работе с персональными данными в информационной системе персональных данных (далее – ИС) министерства образования Новосибирской области (далее – министерство) и по реагированию на нештатные ситуации, связанные с работой в ИС.

3. Пользователем ИС (далее – Пользователь) является сотрудник министерства, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИС согласно приказу списка лиц, которым необходим доступ к персональным данным, обрабатываемым в ИС, для выполнения своих должностных обязанностей.

4. Пользователь в своей работе руководствуется, кроме должностных и технологических инструкций, действующими нормативными, организационно-распорядительными документами по вопросам информационной безопасности.

5. Положения инструкции обязательны для исполнения всеми пользователями и доводятся до сотрудников под роспись. Пользователь должен быть предупрежден о возможной ответственности за ее нарушение.

II. Общий порядок действий при возникновении нештатных ситуаций

6. В настоящей Инструкции под нештатной ситуацией понимается происшествие, связанное со сбоем в функционировании элементов ИС, предоставляемых пользователям ИС, а так же с вероятностью потери защищаемой информации.

7. К нештатным ситуациям относятся следующие ситуации:

сбой в работе программного обеспечения («зависание» компьютера, медленная скорость работы программы, ошибки в работе программы и т. п.);

отключение электричества;

сбой в локальной вычислительной сети (отсутствие доступа в локальную сеть, отсутствие доступа в интернет, отсутствие связи с сервером и т. п.);

выход из строя сервера;

потеря данных (отсутствие возможности сохранить внесенные данные, отсутствие связи с сервером, повреждение файлов и т. п.);

обнаружен вирус;

обнаружена утечка информации (взлом учетной записи пользователя, обнаружение посторонних устройств в системном блоке, обнаружена попытка распечатывания или сканирования документов на принтере и т. п.);

взлом системы (web-сервера, и др.) или несанкционированный доступ;

попытка несанкционированного доступа (обнаружены попытки подбора пароля, доступ постороннего лица в помещение и т. п.);

компрометация ключей (утеря носителя ключевой информации и т. п.), несанкционированный доступ постороннего лица в место физического хранения носителя информации, к устройству хранения информации, визуальный осмотр носителя информации посторонним лицом или подозрение, что данные факты имели место, взлом учётной записи пользователя);

компрометация пароля (взлом учетной записи пользователя, визуальный осмотр посторонним лицом клавиатуры при вводе пароля пользователем и т. п.);

физическое повреждение локально-вычислительной сети (далее – ЛВС) или персонального компьютера (далее – ПК) (не включается ПК, при попытке включения отображается синий или черный экраны, повреждены провода и т. п.);

стихийное бедствие;

иные нештатные ситуации, не включенные в данный список, но влекущие за собой повреждение элементов ИС и возможность потери защищаемой информации, и названные таковыми пользователем ИС или администратором безопасности ИС.

8. При возникновении нештатных ситуаций во время работы сотрудник, обнаруживший нештатную ситуацию, немедленно ставит в известность администратора ИСПДн (либо администратора информационной безопасности, либо ответственного за организацию обработки персональных данных в министерстве). В случае, если поставить в известность администратора ИСПДн

(либо администратора информационной безопасности, либо ответственного за организацию обработки персональных данных в министерстве) не представляется возможным, пользователем, обнаружившим нештатную ситуацию, составляется служебная записка в свободной форме с описанием нештатной ситуации, и передается руководителю подразделения.

9. Администратор ИСПДн (либо администратор информационной безопасности) проводит предварительный анализ ситуации и, в случае невозможности исправить положение, ставит в известность своего непосредственного начальника для определения дальнейших действий.

10. По факту возникновения и устранения нештатной ситуации заносится запись в «Журнал учета нештатных ситуаций ИС, выполнения профилактических работ, установки и модификации программных средств на рабочих станциях и серверах ИС министерства.

11. При необходимости, проводится служебное расследование по факту возникновения нештатной ситуации и выяснению ее причин.

III. Особенности действий при возникновении наиболее распространенных нештатных ситуаций

12. Сбой программного обеспечения. администратор ИСПДн (либо администратор информационной безопасности) совместно с сотрудником, у которого произошла нештатная ситуация, выясняют причину сбоя. Если исправить ошибку своими силами не удалось, в департамент информатизации и развития телекоммуникационных технологий Новосибирской области направляется информационное сообщение с сопроводительными материалами о возникшей ситуации.

13. Отключение электричества. администратор ИСПДн (либо администратор информационной безопасности) совместно с сотрудником, у которого произошла нештатная ситуация, проводят анализ на наличие потерь и (или) разрушения данных и программного обеспечения (далее – ПО), а так же проверяют работоспособность оборудования. В случае необходимости, производится восстановление ПО и данных из последней резервной копии.

14. Сбой в локальной вычислительной сети (ЛВС). администратор ИСПДн (либо администратор информационной безопасности) проводит анализ на наличие потерь и (или) разрушения данных и ПО. В случае необходимости, производится восстановление ПО и данных из последней резервной копии.

15. Выход из строя сервера. администратор ИСПДн (либо администратор информационной безопасности), ответственный за эксплуатацию сервера, проводит меры по немедленному вводу в действие резервного сервера (если есть) для обеспечения непрерывной работы пользователей ИСПДн министерства. При необходимости производятся работы по восстановлению ПО и данных из резервных копий.

16. Потеря данных. При обнаружении потери данных администратор ИСПДн (либо администратор информационной безопасности) проводит мероприятия по поиску и устранению причин потери данных (антивирусная проверка, целостность и работоспособность ПО, целостность и

работоспособность оборудования и др.). При необходимости, производится восстановление ПО и данных из резервных копий.

17. Обнаружен вирус. При обнаружении вируса производится локализация вируса с целью предотвращения его дальнейшего распространения, для чего следует физически отсоединить «зараженный» компьютер от ЛВС и провести анализ состояния компьютера. Анализ проводится администратором ИСПДн (либо администратором информационной безопасности). Результатом анализа может быть попытка сохранения (спасения данных), так как после перезагрузки ЭВМ данные могут быть уже потеряны. После успешной ликвидации вируса, сохраненные данные также необходимо подвергнуть проверке на наличие вируса. При обнаружении вируса следует руководствоваться «Инструкцией по организации антивирусной защиты на объектах вычислительной техники в министерстве образования Новосибирской области». После ликвидации вируса необходимо провести внеочередную антивирусную проверку на всех ЭВМ министерства с применением обновленных антивирусных баз. При необходимости производится восстановление ПО и данных из резервных копий. Проводится служебное расследование по факту появления вируса в ЭВМ (ЛВС).

18. Обнаружена утечка информации. При обнаружении утечки информации ставится в известность администратор информационной безопасности (либо администратор ИСПДн). Проводится служебное расследование. Если утечка информации произошла по техническим причинам, проводится анализ защищенности системы и, если необходимо, принимаются меры по устранению уязвимостей и предотвращению их возникновения.

19. Взлом системы (Web-сервера и др.) или несанкционированный доступ (НСД). При обнаружении взлома сервера проводится, по возможности, временное отключение сервера от сети для проверки на вирусы и троянских закладок. Возможен временный переход на резервный сервер. Учитывая, что программные закладки могут быть не обнаружены антивирусным ПО, следует особенно тщательно проверить целостность исполняемых файлов в соответствии с хэш-функциями эталонного программного обеспечения, а также проанализировать состояние файлов-скриптов и журналы сервера. Необходимо сменить все пароли, которые имели отношение к данному серверу. В случае необходимости производится восстановление ПО и данных из эталонного архива и резервных копий. По результатам анализа ситуации следует проверить вероятность проникновения несанкционированных программ в ЛВС министерства, после чего провести аналогичные работы по проверке и восстановлению ПО и данных на других ЭВМ. По факту взлома сервера проводится служебное расследование.

20. Попытка несанкционированного доступа (НСД). При обнаружении утечки информации ставится в известность администратор информационной безопасности (либо администратор ИСПДн). При попытке НСД проводится анализ ситуации на основе информации журналов регистрации попыток НСД и предыдущих попыток НСД. По результатам анализа, в случае необходимости, принимаются меры по предотвращению НСД, если есть реальная угроза НСД. Так же рекомендуется провести внеплановую смену паролей. В случае появления обновлений ПО, устраняющих уязвимости системы безопасности, следует применить такие обновления.

21. Компрометация ключей. При обнаружении утечки информации ставится в известность администратор информационной безопасности и начальник подразделения. При компрометации ключей следует руководствоваться инструкциями к применяемой системе криптозащиты.

22. Компрометация пароля. При обнаружении утечки информации ставится в известность администратор информационной безопасности и начальник подразделения. При компрометации пароля необходимо немедленно сменить пароль, проанализировать ситуацию на наличие последствий компрометации и принять необходимые меры по минимизации возможного (или нанесенного) ущерба (блокирование счетов пользователей и т.д.). При необходимости, проводится служебное расследование.

23. Физическое повреждение ЛВС или ПК. Ставится в известность администратор ИСПДн (либо администратор информационной безопасности). Определяется причина повреждения ЛВС или ПК и возможные угрозы безопасности информации. В случае возникновения подозрения на целенаправленный вывод оборудования из строя проводится служебное расследование. Проводится проверка ПО на наличие вредоносных программ-закладок, целостность ПО и данных. Проводится анализ электронных журналов. При необходимости проводятся меры по восстановлению ПО и данных из резервных копий.

24. Стихийное бедствие. При возникновении стихийных бедствий следует руководствоваться документами, регламентирующими поведение в чрезвычайных ситуациях, принятых в министерстве.

IV. Меры против возникновения нештатных ситуаций

25. Администратором ИСПДн совместно с администратором информационной безопасности периодически, не реже 1 раза в год, должен проводиться анализ зарегистрированных нештатных ситуаций для выработки мероприятий по их предотвращению.

26. В общем случае, для предотвращения нештатных ситуаций необходимо четкое соблюдение требований нормативных документов министерства и инструкций по эксплуатации оборудования и ПО.

27. Рекомендации по предотвращению некоторых типичных нештатных ситуаций:

сбой программного обеспечения – применять лицензионное ПО, регулярно проводить антивирусный контроль и профилактические работы на ЭВМ (проверка диска и др.);

отключение электричества – использовать источники бесперебойного питания на критически важных технологических участках министерства;

сбой ЛВС – обеспечение бесперебойной работы ЛВС путем применения надежных сетевых технологий и резервных систем;

выход из строя серверов – применять надежные программно-технические средства. Допускать к работе с серверным оборудованием только квалифицированных специалистов;

потеря данных – периодически проводить анализ системных журналов работы ПО с целью выяснения «узких» мест в технологии и возможной утечки (или потери) информации. Проводить с администраторами ИСПДн, администратором информационной безопасности, сотрудниками разъяснительные и обучающие собрания. Обеспечить резервное копирование данных;

обнаружение вируса – соблюдать требования «Инструкции по организации антивирусной защиты на объектах вычислительной техники в министерстве образования Новосибирской области»;

утечка информации – применять средства защиты от НСД. Регулярно проводить анализ журналов попыток НСД и работы по совершенствованию системы защиты информации;

попытка несанкционированного доступа (НСД) – по возможности, установить регистрацию попыток НСД на всех технологических участках, где возможен несанкционированный доступ, с оповещением администратора ИСПДн (либо администратора информационной безопасности) о попытках НСД;

компрометация паролей – соблюдать требования «Инструкции по организации парольной защиты».

Физическое повреждение ЛВС или ПК – физическая защита компонентов сети (серверов, маршрутизаторов и др.), ограничение доступа к ним.

Стихийное бедствие – проводить обучающие собрания и тренировки персонала министерства по вопросам гражданской обороны.».

ПРИЛОЖЕНИЕ № 2
к приказу Минобразования
Новосибирской области
от 12.12.18 № 3223

«УТВЕРЖДЕНА
приказом Минобразования
Новосибирской области
от 07.05.2018 № 1097

ИНСТРУКЦИЯ
по организации парольной защиты в информационных системах персональных данных министерства образования Новосибирской области (далее – Инструкция)

I. Общие положения

1. Настоящая Инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах персональных данных министерства образования Новосибирской области (далее – ИСПДн Минобразования Новосибирской области), а также контроль действий пользователей и обслуживающего персонала системы при работе с паролями.

II. Требования по организации парольной защиты

2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей в ИСПДн и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на Администратора ИСПДн и Администратора информационной безопасности (далее – ИБ), содержащих механизмы идентификации и аутентификации (подтверждения подлинности) пользователей по значениям паролей.

3. Личные пароли должны генерироваться и распределяться централизованно с учетом следующих требований:

длина пароля должна быть не менее 8 символов;

в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);

пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;

личный пароль пользователь не имеет права сообщать никому.

4. Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

5. В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на Администратора ИСПДн и Администратора ИБ. Для генерации «стойких» значений паролей могут применяться специальные программные средства. Система централизованной генерации и распределения паролей должна исключать возможность ознакомления самих уполномоченных сотрудников министерства образования Новосибирской области (далее – министерство).

6. Внеплановая смена личного пароля или удаление учетной записи пользователя автоматизированной системы в случае прекращения его полномочий (увольнение, переход на другую работу внутри министерства и т.п.) должна производиться Администратором ИСПДн немедленно после окончания последнего сеанса работы данного пользователя с системой.

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

8. В случае компрометации личного пароля пользователя автоматизированной системы должны быть немедленно предприняты меры в соответствии с пунктом 6 или пунктом 7 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

III. Ответственность при организации парольной защиты

9. Ответственность за организацию парольной защиты ИСПДн и установление порядка ее проведения, в соответствии с требованиями настоящей Инструкции, возлагается на Администратора ИСПДн.

10. Ответственность за поддержание установленного порядка и соблюдение требований настоящей Инструкции возлагается на ответственного за организацию обработки ПДн в ИСПДн и пользователей (операторов) ИСПДн.

11. Периодический контроль за выполнением всех требований настоящей Инструкции, и состоянием антивирусной защиты осуществляется Администратором ИБ.».

Лист ознакомления

____

N п/п	Фамилия, имя, отчество	Дата	Подпись
1	2	3	5