МИНИСТЕРСТВО ОБРАЗОВАНИЯ НОВОСИБИРСКОЙ ОБЛАСТИ

ПРИКАЗ

29 ИЮН 2022 № 1184

О внесении изменений в приказ министерства образования Новосибирской области от 07.05.2018 № 1097

П р и к а з ы в а ю:

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. В пункте 1:

1) подпункт 4 признать утратившим силу;

2) дополнить подпунктом 11 следующего содержания:

«11. «Инструкция по организации антивирусной защиты в информационных системах министерства образования Новосибирской области.».

2. В пункте 2 «государственного бюджетного учреждения дополнительного профессионального образования Новосибирской области «Областной центр информационных технологий» (Перкова В.Г.)» заменить словами «государственного автономного учреждения дополнительного профессионального образования Новосибирской области «Новосибирский институт повышения квалификации и переподготовки работников образования» (Умбрашко К.Б.)».

3. В Инструкции администратора информационной безопасности в министерстве образования Новосибирской области:

1) абзацы четырнадцатый, шестнадцатый, двадцать третий, тридцать шестой раздела 3 признать утратившими силу;

2) в разделе 4:

а) абзац четвертый изложить в следующей редакции:

«Участвовать в экспертной комиссии по проведению мероприятий по защите персональных данных, контролю за соблюдением порядка обращения с документами, содержащими персональные данные в министерстве;»;

б) абзацы пятый, седьмой признать утратившим силу.

4. В Инструкции администратора информационной системы персональных данных в министерстве образования Новосибирской области:

1) в разделе 3:

а) в абзаце пятом слова «осуществлять конфигурацию» заменить словами «осуществлять управление конфигурацией»;

б) абзацы семнадцатый, двадцатый, двадцать первый, двадцать второй, двадцать третий, двадцать четвертый признать утратившими силу.

5. В Инструкции оператора информационной системы персональных данных в министерстве образования Новосибирской области:

абзац четвертый раздела 2 изложить в следующей редакции:

«Оператор в своей работе руководствуется локальными актами министерства, руководящими и нормативными документами ФСТЭК России, ФСБ России.».

6. В Инструкции по реагированию на инциденты информационной безопасности в информационных системах персональных данных в министерстве образования Новосибирской области:

абзац второй раздела 1 изложить в следующей редакции:

«Настоящая Инструкция разработана на основании Приказа ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»; Методического документа «Меры защиты информации в государственных информационных системах, утверждённого ФСТЭК России 11.02.2014.».

7. В Инструкции о порядке обеспечения конфиденциальности при обработке персональных данных в министерстве образования Новосибирской области:

1) абзац шестнадцатый раздела 1 признать утратившим силу;

2) абзац четвертый раздела 3 изложить в следующей редакции:

«Допуск лиц к обработке персональных данных с использованием средств автоматизации осуществляется на основании приказа министерства образования Новосибирской области.»;

3) абзац второй Приложения № 3 изложить в следующей редакции:

«В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и Указом Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера» информация, предоставленная в Ваше распоряжение, относится к персональным данным работника, поэтому является конфиденциальной.».

8. В Инструкции пользователя по обеспечению безопасности при возникновении нештатных ситуаций в информационных системах министерства образования Новосибирской области:

1) в пункте 10 раздела II слово «серверах» исключить;

2) в разделе III:

а) в пункте 12 слова «департамент информатизации и развития телекоммуникационных технологий Новосибирской области» заменить словами «министерство цифрового развития и связи Новосибирской области»;

б) в пункте 22 слова «(блокирование счетов пользователя и т.д.)» исключить.

9. В Инструкции по организации парольной защиты в информационных системах персональных данных министерства образования Новосибирской области:

разделы II, III изложить в следующей редакции:

«II. Требования по организации парольной защиты

2. Личные пароли должны создаваться пользователями самостоятельно с учетом следующих требований:

длина личного 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.

3. В случае формирования личных паролей пользователей централизованно, ответственность за правильность их формирования и распределения возлагается на сотрудников министерства цифрового развития и связи Новосибирской области, а также Администратора ИСПДн.

4. Полная плановая смена личных паролей проводится не реже одного раза в 3 месяца.

5. Внеплановая смена личного пароля пользователя или удаление учетной записи в случае прекращения его полномочий (увольнение) должна производиться сотрудниками министерства цифрового развития и связи Новосибирской области или Администратором ИСПДн немедленно после окончания последнего сеанса работы пользователя в АРМ и в ИСПДн соответственно.

6. Устанавливается ограничение на количество неуспешных попыток аутентификации (ввода логина и пароля) пользователя, равное 3, после чего учетная запись блокируется.

7. Разблокирование учетной записи пользователя осуществляется сотрудниками министерства цифрового развития и связи Новосибирской области или Администратором ИСПДн.

8. После 15 минут бездействия (неактивности) пользователя в АРМ происходит автоматическое блокирование сеанса доступа в АРМ.

«II. Ответственность при организации парольной защиты

9. Пользователь несет персональную ответственность за сохранность данных аутентификации (персонального логина и пароля) к АРМ.».

10. Дополнить Инструкцией по организации антивирусной защиты в информационных системах министерства образования Новосибирской области согласно приложению к настоящему приказу.

Министр С.В. Федорчук

Галушко Г.А.
238-73-41

ПРИЛОЖЕНИЕ
к приказу Минобразования
Новосибирской области
от 29 ИЮН 2022 № 1284

«УТВЕРЖДЕНА
приказом Минобразования
Новосибирской области
от 07.05.2018 № 1097

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

I. Общие положения

1. Инструкция разработана в целях реализации мер по антивирусной защите информационных систем (далее – ИС) министерства образования Новосибирской области (далее – Министерство, оператор) и регулирует вопросы организации антивирусной защиты и требования к порядку проведения антивирусного контроля при работе в ИС Министерства.

2. Меры по антивирусной защите обеспечивают обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

3. Установка и настройка средств антивирусной защиты осуществляется уполномоченными сотрудниками государственного бюджетного учреждения Новосибирской области «Центр защиты информации Новосибирской области» (далее – ГБУ НСО «ЦЗИ НСО») в соответствии с эксплуатационной документацией на применяемые средства антивирусной защиты.

II. Обеспечение антивирусной защиты

4. Порядок организации антивирусной защиты.

1) для обеспечения антивирусной защиты ИС Министерства допускаются к использованию только сертифицированные ФСТЭК России лицензионные антивирусные средства;

2) антивирусное средство защиты устанавливается на все средства вычислительной техники (СВТ) (при наличии технической возможности), входящие в ИС Министерства и подверженные внедрению (заражению) вредоносными компьютерными программами (вирусами) через съемные машинные носители информации или сетевые подключения, в том числе к сетям

общего пользования (вложения электронной почты, веб- и другие сетевые сервисы);

3) в ИС Министерства права на установку, конфигурирование и правление (администрирование) средствами антивирусной защиты предоставлены только уполномоченным сотрудникам ГБУ НСО «ЦЗИ НСО;

4) для реализации антивирусной защиты в ИС Министерства предоставляется доступ средствам антивирусной защиты к объектам ИС, которые подвергаются проверке;

5) должностные лица Министерства не должны допускать использования в ИС Министерства программного обеспечения и данных, не связанных с выполнением своих должностных обязанностей;

6) уполномоченными сотрудниками Министерства организуется проведение периодических проверок компонентов ИС на наличие вредоносных компьютерных программ (вирусов);

7) проверка выделенных наиболее критичных компонентов ИС (памяти ядра, запущенных процессов, объектов автозапуска, загрузочных секторов, системных папок) на наличие вредоносных компьютерных программ (вирусов) осуществляется в автоматическом режиме по расписанию (один раз в сутки);

8) расширенный (полный) антивирусный контроль всех компонентов ИС проводится в автоматическом режиме с периодичностью один раз в месяц;

9) в ИС Министерства осуществляется автоматическая проверка в масштабе времени, близком к реальному, объектов (файлов) из внешних источников (съемных машинных носителей информации, сетевых подключений, и других внешних источников) при загрузке, открытии или исполнении таких файлов;

10) файлы, помещаемые в электронный архив, в обязательном порядке проходят антивирусный контроль. Контроль исходящей информации (в случае передачи информации на внешнем съемном носителе) проводится непосредственно перед архивированием и отправкой (записью на съемный носитель) (при наличии такой процедуры).

5. Порядок проведения антивирусного контроля.

1) при возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь ИС Министерства инициирует внеочередной антивирусный контроль своей рабочей станции для определения факта наличия или отсутствия компьютерного вируса;

2) в случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователи ИС Министерства обязаны:

а) приостановить работу;

б) немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора информационной безопасности в Министерстве, уполномоченного сотрудника ГБУ НСО «ЦЗИ НСО», владельца зараженных файлов, а также другие структурные подразделения Министерства, использующие эти файлы в работе;

в) совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;

г) провести лечение или уничтожение зараженных файлов.

6. Обновление базы данных признаков вредоносных компьютерных программ (вирусов).

1) получение из доверенных источников и установку обновлений базы данных признаков вредоносных компьютерных программ (вирусов) обеспечивают уполномоченные сотрудники ГБУ НСО «ЦЗИ НСО»;

2) в ИС Министерства обеспечивается контроль целостности обновлений базы данных признаков вредоносных компьютерных программ (вирусов) на соответствие предоставляемых производителем СЗИ контрольным суммам;

3) в ИС Министерства обеспечивается централизованное управление обновлением базы данных признаков вредоносных компьютерных программ (вирусов) уполномоченными сотрудниками ГБУ НСО «ЦЗИ НСО».

III. Ответственность при организации антивирусной защиты

7. Оператор несет ответственность за правонарушения в сфере информации, информационных технологий и защиты информации в соответствии с законодательством Российской Федерации.

8. Лица, виновные в нарушении требований Инструкции, привлекаются к дисциплинарной, административной, гражданско-правовой, уголовной ответственности в порядке, установленном законодательством Российской Федерации.».