МИНИСТЕРСТВО ОБРАЗОВАНИЯ НОВОСИБИРСКОЙ ОБЛАСТИ

ПРИКАЗ

01 ИЮЛ 2022 1312

г. Новосибирск

О реализации мер по обеспечению безопасности защищаемой информации, обрабатываемой в информационных системах министерства образования Новосибирской области

В целях выполнения требований законодательства Российской Федерации в области защиты информации (в том числе персональных данных), не содержащей сведения, составляющие государственную тайну (далее – защищаемая информация), и реализации мер по обеспечению безопасности защищаемой информации, обрабатываемой в информационных системах министерства образования Новосибирской области, **п р и к а з ы в а ю**:

1. Утвердить прилагаемые:

1) Правила идентификации и аутентификации субъектов доступа и объектов доступа в информационных системах министерства образования Новосибирской области;

2) Регламент выявления инцидентов безопасности и реагирования на них;

3) Правила защиты информации при выводе из эксплуатации информационной системы или после принятия решения об окончании обработки информации ограниченного доступа;

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

5) Инструкцию по контролю защищенности информации в информационных системах министерства образования Новосибирской области.

2. Признать утратившим силу приказ министерства образования Новосибирской области от 18.02.2019 № 336 «Об утверждении Положения об управлении доступом субъектов доступа к объектам доступа в информационной системе персональных данных министерства образования Новосибирской области».

3. Контроль за исполнением настоящего приказа оставляю за собой.

Министр С.В. Федорчук

Галушко Г.А.
238-73-41

УТВЕРЖДЕНЫ
приказом Минобразования
Новосибирской области
от 01 ИЮЛ 2022 № 1312

ПРАВИЛА
идентификации и аутентификации субъектов доступа и объектов доступа в информационных системах министерства образования Новосибирской области
(далее – Правила)

I. Общие положения

1. Правила разработаны в целях реализации мер защиты информации по идентификации и аутентификации субъектов доступа и объектов доступа в информационных системах (далее – ИС) министерства образования Новосибирской области (далее – Министерство, оператор).

2. Меры по идентификации и аутентификации субъектов доступа и объектов доступа обеспечивают присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

II. Идентификация и аутентификация пользователей, являющихся внутренними пользователями

3. При доступе в ИС Министерства осуществляется идентификация и аутентификация внутренних пользователей, и процессов, запускаемых от имени этих пользователей, а также процессов, запускаемых от имени системных учетных записей.

4. К внутренним пользователям относятся должностные лица оператора (пользователи, администраторы), выполняющие свои должностные обязанности (функции) с использованием информации, информационных технологий и технических средств ИС Министерства в соответствии с должностными регламентами (инструкциями) и которым в ИС Министерства присвоены учетные записи.

5. В качестве внутренних пользователей дополнительно рассматриваются должностные лица обладателя информации, уполномоченного лица и (или) оператора иной информационной системы, а также сотрудники сторонних организаций, привлекаемые на договорной основе для администрирования (управления) системой защиты информации ИС Министерства, обеспечения функционирования ИС Министерства (ремонт, гарантийное обслуживание,

регламентные и иные работы) в соответствии с принятыми соглашениями и организационно-распорядительными документами Министерства.

6. Для каждого внутреннего пользователя в ИС Министерства заводятся учетные записи.

7. Пользователи ИС Министерства однозначно идентифицируются и аутентифицируются для всех видов доступа, кроме тех видов доступа, которые определяются как действия, разрешенные до идентификации и аутентификации в соответствии с Правилами управления доступом в ИС Министерства.

8. Аутентификация пользователя в ИС Министерства осуществляется с использованием паролей. Также применяются аппаратные средства в случае многофакторной (двухфакторной) аутентификации.

9. В ИС Министерства обеспечивается возможность однозначного сопоставления идентификатора пользователя с запускаемыми от его имени процессами.

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

10. В ИС Министерства реализовываются 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 через период неиспользования не более 90 дней.

11. Создание, присвоение и уничтожение идентификаторов пользователей и устройств осуществляют лица с полномочиями системных администраторов ИС, обеспечивающие функционирование ИС Министерства.

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

12. В ИС Министерства реализовываются следующие функции управления средствами аутентификации (аутентификационной информацией) пользователей и устройств:

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

2) выдача средств аутентификации пользователям;

3) генерация и выдача начальной аутентификационной информации (начальных значений средств аутентификации) с последующей сменой пользователями начальной аутентификационной информации;

4) установление характеристик пароля:

а) длина пароля не менее восьми символов;

б) алфавит пароля не менее 60 символов;

в) максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 10 попыток;

г) блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 5 до 30 минут;

д) 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 неправомерного доступа к ней и модифицирования.

13. В случае утраты и (или) компрометации личного пароля пользователя ИС Министерства производится внеплановая смена (сброс) личного пароля владельца скомпрометированного пароля.

14. В случае прекращения полномочий пользователя ИС (увольнение, переход на другую работу внутри организации и т.п.) производится удаление его учетной записи после окончания последнего сеанса работы данного пользователя с системой.

15. Управление средствами аутентификации (аутентификационной информацией) пользователей ИС и принятие мер в случае утраты и (или) компрометации средств аутентификации (аутентификационной информации) осуществляют лица с полномочиями системных администраторов ИС Министерства, обеспечивающие функционирование ИС Министерства.

16. Руководители структурных подразделений Министерства обеспечивают своевременное доведение информации о прекращении полномочий пользователей ИС Министерства до лиц, осуществляющих управление средствами аутентификации (аутентификационной информацией) пользователей ИС.

V. Защита обратной связи при вводе аутентификационной информации

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

18. 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

19. Оператор и его работники несут ответственность за правонарушения в сфере информации, информационных технологий и защиты информации в соответствии с законодательством Российской Федерации.

УТВЕРЖДЕН
приказом Минобразования
Новосибирской области
от 01 ИЮЛ 2022 № 1312

РЕГЛАМЕНТ
выявления инцидентов безопасности и реагирования на них
(далее – Регламент)

I. Общие положения

1. Регламент определяет правила и процедуры выявления и реагирования на инциденты информационной безопасности (далее – ИБ) в министерстве образования Новосибирской области (далее – Министерство).

2. Под инцидентом ИБ понимается непредвиденное или нежелательное событие (группа событий), которое привело (может привести) к сбоям или нарушению функционирования информационной системы (далее – ИС) и (или) к возникновению угроз безопасности информации (далее – инцидент).

3. Ответственными за выявление и реагирование на инциденты ИБ в ИС Министерства являются лица, ответственные за управление (администрирование) системой защиты информации ИС Министерства, лица с правами системных администраторов, обеспечивающие функционирование ИС Министерства, и ответственный за организацию работ по защите информации, не содержащей сведения, составляющие государственную тайну, содержащейся в ИС Министерства (далее – ответственный за защиту информации).

II. Этапы реагирования на инциденты безопасности

4. Жизненный цикл реагирования на инциденты ИБ состоит из следующих стадий:

1) обнаружение и регистрация инцидента;

2) устранение причин и последствий инцидента;

3) расследование инцидента;

4) реализация корректирующих мероприятий.

5. В ходе выявления инцидентов и реагирования на них осуществляются:

1) обнаружение и идентификация инцидентов, в том числе событий, приводящих к возникновению инцидентов;

2) своевременное информирование пользователями ИС ответственного за защиту информации, содержащейся в ИС Министерства, о возникновении инцидентов в информационной системе пользователями и ответственными лицами;

3) анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;

4) планирование и принятие мер по устранению инцидентов, в том числе по восстановлению ИС и ее сегментов в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

5) планирование и принятие мер по предотвращению повторного возникновения инцидентов.

III. Обнаружение инцидентов информационной безопасности

6. В качестве источников информации об инцидентах используются:

1) журналы регистрации событий и оповещения системного и прикладного программного обеспечения ИС, средств защиты информации;

2) информация, получаемая от сотрудников Министерства и иных лиц, уполномоченных на проведение работ по обеспечению функционирования ИС Министерства (ремонт, гарантийное, техническое обслуживание, регламентные и иные работы), администрированию (управлению) системой защиты информации ИС Министерства и иных работ в соответствии с заключенными контрактами, соглашениями, договорами;

3) информация, полученная по результатам контроля (анализа) защищенности ИС и контроля эффективности системы защиты информации.

IV. Информирование об инцидентах, анализ инцидентов

7. Лица, ответственные за выявление и реагирование на инциденты ИБ в ИС Министерства, получают информацию о случившихся инцидентах и принимают меры по их устранению.

8. Некорректное функционирование ИС Министерства может являться индикатором атаки или нарушения функционирования системы безопасности. Сотрудники Министерства, а также иные лица, имеющие доступ к ИС Министерства (в том числе осуществляющие техническое сопровождение ИС Министерства и ее компонентов), обязаны при получении информации обо всех нетипичных событиях, указывающих на возникновение инцидента ИБ, незамедлительно сообщить о них ответственным за выявление и реагирование на инциденты ИБ в ИС Министерства.

9. К нетипичным событиям, о которых следует уведомлять ответственных за выявление и реагирование на инциденты, относятся:

1) сбои (перезагрузки) в работе, неправильное срабатывание технических средств, программного обеспечения (системного программного обеспечения, программного обеспечения общего назначения, специализированного программного обеспечения) и средств защиты информации;

2) нарушения правил разграничения доступа (в том числе самопроизвольное появление новых учетных записей);

3) самопроизвольное появление новых файлов;

4) изменения в размерах и датах файлов, не соответствующие фактическим датам обращения и внесения изменений;

5) попытки записи в системные файлы;

6) самопроизвольные модификация или удаление данных;

7) отказ в обслуживании (отсутствие доступа к программным и техническим средствам);

8) необъяснимо низкая производительность системы (слишком долгое время отклика системы);

9) аномальное поведение системы (например, появление сообщений на экране, частые и необъяснимые звуковые сигналы);

10) неконтролируемое внесение изменений в систему, ее настройки и параметры;

11) хищение (утрата) носителей защищаемой информации, технических средств, входящих в состав ИС;

12) хищение (утрата) ключевых документов, ключей от помещений и хранилищ, личных печатей, удостоверений, пропусков;

13) нарушение целостности установленных защитных пломб;

14) заражение компонентов ИС Министерства вредоносной программой;

15) несанкционированное проникновение в помещения, где расположены компоненты ИС Министерства и ведется обработка защищаемой информации;

16) другие нетипичные события, происходящие в системе.

10. К инцидентам ИБ не относятся:

1) неудачные попытки вторжений в ИС Министерства, которые были обнаружены и нейтрализованы с использованием средств защиты информации;

2) неудачные попытки заражения компонентов ИС Министерства вредоносной программой, которые были обнаружены и нейтрализованы с использованием средств защиты информации.

11. Все сотрудники Министерства, лица, выполняющие работы и оказывающие услуги на договорной основе, и имеющие доступ к ИС Министерства, должны быть ознакомлены с процедурой информирования о выявленных инцидентах ИБ и иных нетипичных событиях.

12. Ответственные за выявление и реагирование на инциденты в ИС Министерства проводят сбор информации, связанной с нетипичным событием, о котором поступило сообщение, для подтверждения и локализации инцидента ИБ.

V. Реагирование на инциденты ИБ

13. В случае наличия признаков инцидента ИБ ответственные за выявление и реагирование на инциденты в ИС Министерства определяют предварительную степень важности инцидента, проводят первоочередные меры, направленные на локализацию инцидента ИБ, препятствующие его распространению (в том числе ограничение доступа к объектам, задействованным в инциденте ИБ) и минимизацию его последствий, принимают решение о необходимости проведения расследования.

14. Для реагирования на инциденты ИБ ответственные за выявление и реагирование на инциденты в ИС Министерства привлекают при необходимости сотрудников Министерства, а также внешних экспертов. Необходимость привлечения тех или иных специалистов определяется в зависимости от характера инцидента.

15. В случае вовлечения внешних экспертов заключается письменное соглашение о конфиденциальности между Министерства и привлеченной стороной.

16. После локализации инцидента осуществляется ликвидация последствий и восстановление системы (приведение системы к штатному режиму функционирования), проводится расследование и анализ произошедшего инцидента.

17. В ходе анализа инцидента по возможности выявляются следующие показатели:

1) факт или потенциальная возможность реализации угрозы безопасности защищаемой информации (далее – угрозы);

2) опасность угрозы;

3) область, перечень информационных ресурсов, затрагиваемые воздействием угрозы;

4) потенциальные нарушители, цели и причины реализации угрозы;

5) перечень мер по локализации и остановке распространения действия угрозы.

VI. Анализ причин и оценка результата

18. Расследование инцидента ИБ проводится с целью раскрытия причинно-следственных связей и получения следующей информации:

1) причины и условия возникновения инцидента ИБ;

2) источники инцидента ИБ (нарушители);

3) цели реализации инцидента ИБ;

4) способы осуществления инцидента ИБ;

5) данные о характере и размерах причиненного в результате инцидента ИБ ущерба.

19. По результатам проведенного расследования инцидента ответственные за выявление и реагирование на инциденты в ИС Министерства проводят:

1) переоценку рисков, повлекших возникновение инцидента ИБ;

2) анализ перечня защитных мер для минимизации выявленных рисков в случае повторения инцидента ИБ;

3) анализ инструкций и правил обеспечения информационной безопасности, включая настоящий документ;

4) инструктаж (информирование об угрозах безопасности информации, правилах эксплуатации системы защиты информации ИС и отдельных средств защиты информации) сотрудников Министерства для повышения их осведомленности в части информационной безопасности.

УТВЕРЖДЕНЫ
приказом Минобразования
Новосибирской области
от 01 ИЮЛ 2022 № 1312

ПРАВИЛА
защиты информации при выводе из эксплуатации информационной системы или после принятия решения об окончании обработки информации ограниченного доступа
(далее – Правила)

I. Общие положения

1. Правила разработаны в целях обеспечения защиты информации при выводе из эксплуатации информационных систем министерства образования Новосибирской области (далее – ИС, Министерство (оператор)).

2. Меры по обеспечению защиты информации при выводе из эксплуатации ИС Министерства или после принятия решения об окончании обработки информации обеспечиваются путем выполнения требований к порядку вывода ИС из эксплуатации и дальнейшему хранению содержащейся в ее базах данных информации.

II. Требования к порядку вывода ИС из эксплуатации и дальнейшего хранения содержащейся в ее базах данных информации

3. Основанием для вывода ИС из эксплуатации является:

1) завершение срока эксплуатации ИС, в случае если такой срок был установлен правовым актом оператора о вводе ИС в эксплуатацию;

2) нецелесообразность эксплуатации ИС, в том числе низкая эффективность используемых технических средств и программного обеспечения, изменение правового регулирования, принятие управленческих решений, а также наличие иных изменений, препятствующих эксплуатации ИС;

3) финансово-экономическая неэффективность эксплуатации ИС.

4. При наличии одного или нескольких оснований для вывода ИС из эксплуатации, указанных в пункте 3 Правил, оператор утверждает правовой акт о выводе ИС из эксплуатации.

5. Правовой акт о выводе ИС из эксплуатации включает:

1) основание для вывода ИС из эксплуатации;

2) перечень и сроки реализации мероприятий по выводу ИС из эксплуатации;

3) порядок, сроки, режим хранения и дальнейшего использования информационных ресурсов, включая порядок обеспечения доступа к информационным ресурсам выводимой из эксплуатации ИС и обеспечения

защиты информации, содержащейся в выводимой из эксплуатации ИС;

4) порядок, сроки и способы информирования пользователей о выводе ИС из эксплуатации.

6. Перечень мероприятий по выводу ИС из эксплуатации включает:

1) подготовку правовых актов, связанных с выводом ИС из эксплуатации;

2) работы по выводу ИС из эксплуатации, в том числе работы по деинсталляции программного обеспечения ИС, по реализации прав на программное обеспечение ИС, демонтажу и списанию технических средств ИС (при отсутствии потребности в дальнейшей эксплуатации в деятельности оператора), обеспечению хранения и дальнейшего использования информационных ресурсов ИС;

3) обеспечение защиты информации в соответствии с документацией на ИС и организационно-распорядительными документами по защите информации, в том числе архивирование информации, содержащейся в ИС, уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации.

7. Если нормативными правовыми актами Российской Федерации не установлено иное, то сроки хранения информации, содержащейся в базах данных ИС, определяются оператором и не могут быть меньше сроков хранения информации, которые установлены для хранения документов в бумажном виде, содержащих такую информацию.

8. Срок вывода ИС из эксплуатации не может быть ранее срока окончания последнего мероприятия, предусмотренного правовым актом о выводе ИС из эксплуатации.

III. Обеспечение защиты информации при выводе из эксплуатации информационных систем или после принятия решения об окончании обработки информации

9. Обеспечение защиты информации при выводе из эксплуатации ИС или после принятия решения об окончании обработки информации, содержащейся в ИС, осуществляется Министерством в соответствии с эксплуатационной документацией на систему защиты информации ИС и организационно-распорядительными документами по защите информации и в том числе включает:

1) архивирование информации, содержащейся в ИС;

2) уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации.

10. Архивирование информации, содержащейся в ИС, обеспечивается при необходимости дальнейшего использования информации в деятельности Министерства и осуществляется, в том числе, в соответствии с требованиями законодательства об архивном деле в Российской Федерации.

11. Архивирование информации, содержащейся в ИС, обеспечивается лицами с полномочиями системных администраторов ИС, обеспечивающими функционирование ИС.

12. Уничтожение (стирание) данных и остаточной информации с машинных носителей информации производится при необходимости передачи машинного носителя информации другому пользователю ИС или в сторонние организации для ремонта, технического обслуживания или дальнейшего уничтожения. При выводе из эксплуатации машинных носителей информации, на которых осуществлялись хранение и обработка информации, осуществляется физическое уничтожение этих машинных носителей информации.

13. Процедуры уничтожения (стирания) информации, хранящейся на машинных носителях информации, а также физическое уничтожение машинных носителей информации производится ответственным за защиту информации, не содержащей сведения, составляющие государственную тайну, содержащейся в ИС, в соответствии с Правилами обращения с машинными носителями информации в информационных системах Министерства, утверждёнными приказом Министерства.

УТВЕРЖДЕНЫ
приказом Минобразования
Новосибирской области
от 01 ИЮЛ 2022 № 1312

ПРАВИЛА
регистрации событий безопасности в информационных системах министерства образования Новосибирской области
(далее – Правила)

I. Общие положения

1. 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 министерства образования Новосибирской области (далее – ИС, Министерство).

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

2. В ИС подлежат регистрации 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	Дата и время изменения правил разграничения доступа к виртуальному и

	компонентам виртуальной инфраструктуры	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 ИС, 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, обеспечивают, в том числе, 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 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 Правил;

2) генерацию (сбор, запись) записей регистрации (аудита) для событий безопасности, подлежащих регистрации (аудиту) в соответствии с пунктом 2 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 Правил.

7. Объем памяти для хранения информации о событиях безопасности рассчитывается и выделяется администратором информационной безопасности ИС с учетом типов событий безопасности, подлежащих регистрации в соответствии с в пункте 2 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) проводится администратором информационной безопасности не реже двух раз в месяц для всех событий, подлежащих регистрации, и обеспечивает своевременное выявление признаков инцидентов безопасности в ИС.

9. В случае выявления признаков инцидентов безопасности в ИС 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 ИС обеспечивается 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 исключительно администратору информационной безопасности и администратору виртуальной инфраструктуры.

УТВЕРЖДЕНА
приказом Минобразования
Новосибирской области
от 01 ИЮЛ 2022 № 1312

ИНСТРУКЦИЯ
по контролю защищенности информации в информационных системах министерства образования Новосибирской области (далее – Инструкция)

I. Общие положения

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

II. Выявление, анализ и устранение уязвимостей информационной системы

2. В ИС при выявлении (поиске), анализе и устранении уязвимостей проводятся:

1) 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;

2) разработка по результатам выявления (поиска) уязвимостей отчетов с описанием выявленных уязвимостей и планом мероприятий по их устранению;

3) анализ отчетов с результатами поиска уязвимостей и оценки достаточности реализованных мер защиты информации;

4) 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;

5) информирование должностных лиц Министерства (пользователей, администраторов) о результатах поиска уязвимостей и оценки достаточности реализованных мер защиты информации.

3. 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.

4. 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.

5. 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 осуществляются действия (корректировка настроек средств защиты информации, изменение режима и порядка использования ИС), направленные на устранение возможности использования выявленных уязвимостей.

6. В ИС 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.

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

8. 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 для нарушения безопасности информации.

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

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

10. В ИС 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.

11. При контроле установки обновлений осуществляются проверки соответствия версий общесистемного, прикладного и специального программного (микропрограммного) обеспечения, включая программное

обеспечение средств защиты информации, установленного в ИС и выпущенного разработчиком, а также наличие отметок в эксплуатационной документации (формуляр или паспорт) об установке (применении) обновлений.

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

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

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

1) контроль работоспособности (неотключения) программного обеспечения и средств защиты информации;

2) проверка правильности функционирования (тестирование на тестовых данных, приводящих к известному результату) программного обеспечения и средств защиты информации;

3) контроль соответствия настроек программного обеспечения и средств защиты информации параметрам настройки, приведенным в эксплуатационной документации на систему защиты информации и средства защиты информации;

4) 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.

5) 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.

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

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

1) 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;

2) 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;

3) контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации и принятие мер, направленных на устранение выявленных недостатков;

4) исключение (восстановление) из состава ИС Минобразования Новосибирской области несанкционированно установленных (удаленных) технических средств, программного обеспечения и средств защиты информации.

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

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

16. При контроле правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в ИС осуществляется:

1) контроль правил генерации и смены паролей пользователей в соответствии с Правилами идентификации и аутентификации пользователей в информационных системах министерства образования Новосибирской области, утвержденными приказом Министерства;

2) контроль заведения и удаления учетных записей пользователей в соответствии с Правилами управления доступом субъектов доступа к объектам доступа в информационных системах министерства образования Новосибирской области, утвержденными приказом Министерства;

3) контроль реализации правил разграничения доступом в соответствии с Положением;

4) контроль реализации полномочий пользователей в соответствии с Положением;

5) 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 Министерстве;

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

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