АДМИНИСТРАЦИЯ БАРАБИНСКОГО РАЙОНА

ПОСТАНОВЛЕНИЕ

от 22.12.2016 № 1368

Об утверждении инструкций и ознакомлении с ними ответственных лиц

В связи с проведением работ по защите информации ограниченного доступа (в том числе персональных данных), не содержащей сведения, составляющие государственную тайну (далее – Информация), в сегменте регионального сегмента единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам на территории Барабинского района (далее – сегмент РИС «Контингент» администрации Барабинского района),

ПОСТАНОВЛЯЮ:

1 Утвердить следующие внутренние документы администрации Барабинского района:

1.1. Инструкцию пользователя сегмента регионального сегмента единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам на территории Барабинского района (Приложение № 1).

1.2. Инструкцию по порядку обращения со средствами защиты информации в сегменте регионального сегмента единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам на территории Барабинского района (Приложение № 2).

1.3. Типовую форму акта установки средств защиты информации на объекте вычислительной техники - автоматизированное рабочее место на базе автономной ПЭВМ (Приложение № 3).

1.4. Правила идентификации и аутентификации субъектов доступа и объектов доступа в сегменте регионального сегмента единой федеральной

межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам на территории Барабинского района (Приложение № 4).

1.5. Правила по ограничению программной среды в сегменте регионального сегмента единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам на территории Барабинского района (Приложение № 5).

1.6. Перечень программного обеспечения, разрешенного к использованию в сегменте регионального сегмента единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам на территории Барабинского района (Приложение № 6).

1.7. Правила регистрации событий безопасности в сегменте регионального сегмента единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам на территории Барабинского района Новосибирской области (Приложение № 7).

1.8. Перечень событий безопасности в информационных системах администрации Барабинского района, подлежащих регистрации (Приложение № 8).

1.9. Инструкцию по контролю защищенности информации в информационных системах администрации Барабинского района (Приложение № 9);

1.10. Инструкцию по антивирусной защите в сегменте регионального сегмента единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам на Барабинского района (Приложение № 10).

1.11. Ознакомить с вышеперечисленными инструкциями лиц, осуществляющих обработку Информации, и ответственных за обеспечение безопасности информации в сегменте РИС «Контингент» Управления образования администрации Барабинского района.

2. Контроль за исполнением требований настоящего постановления возложить на заместителя Главы администрации Барабинского района С.В.Цейнара.

Глава Барабинского района Е.В.Бессонов

Игнатьева Т.А., 22081

Приложение № 1
к постановлению от «___» _____ 201__ г. № _____

ИНСТРУКЦИЯ

Пользователя сегмента регионального сегмента единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам на территории Барабинского района

1. Общие положения

1.1 Инструкция пользователя сегмента регионального сегмента единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам на территории Барабинского района (далее – сегмент РИС «Контингент» администрации Барабинского района) (далее – Инструкция) определяет функциональные обязанности, права и ответственность пользователей сегмента РИС «Контингент» администрации Барабинского района, в которых обрабатывается информация согласно утвержденному Перечню информационных систем и информации, обрабатываемой в администрации Барабинского района.

1.2 Настоящая Инструкция подготовлена в соответствии с требованиями нормативно-методических документов ФСТЭК России и ФСБ России по защите информации ограниченного доступа (в том числе персональные данные), не содержащая сведения, составляющие государственную тайну (далее – Информация), обрабатываемой с использованием средств автоматизации.

1.3 В настоящей Инструкции используются следующие понятия и определения:

1.3.1 Автоматизированное рабочее место (АРМ) – объект вычислительной техники, созданный на базе автономных средств вычислительной техники с необходимым для решения конкретных задач периферийным оборудованием.

1.3.2 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.

1.3.3 Конфиденциальность информации – обязательное для соблюдения лицом, получившим доступ к информации, требование не допускать ее распространение без наличия иного законного основания.

1.3.4 Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

1.3.5 Несанкционированный доступ к информации – доступ к информации с нарушением установленных прав доступа, приводящий к нарушению конфиденциальности персональных данных, к утечке, искажению, подделке, уничтожению, блокированию доступа к информации.

1.3.6 Средство защиты информации (СЗИ) – программные, программно-аппаратные, аппаратные средства, предназначенные и используемые для защиты информации в информационных системах.

1.3.7 Пользователь информационной системы – лицо, участвующее в функционировании информационной системы или использующее результаты ее функционирования.

1.3.8 Утеря пароля – события, приводящие к невозможности восстановления пароля в памяти лица, владеющего данным паролем.

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

2 Обязанности пользователя

2.1 Пользователь сегмента РИС «Контингент» администрации Барабинского района обязан:

2.1.1 Знать и выполнять требования:

- настоящей инструкции;
- внутренних распорядительных документов по режиму обработки Информации, учету, хранению и пересылке носителей информации, обеспечению безопасности Информации;
- нормативных правовых актов действующего законодательства в области защиты Информации.

2.1.2 Хранить в тайне Информацию, ставшую ему известной во время работы или иным путем, и пресекать действия других лиц, которые могут привести к разглашению Информации. О таких фактах, а также о других причинах или условиях возможной утечки Информации немедленно информировать Ответственного за обработку и защиту информации, Администратора ИС и/или Администратора информационной безопасности (далее – ИБ).

2.1.3 При определении информации, подлежащей защите, использовать «Перечень защищаемой информации, не содержащей сведения, составляющие государственную тайну, обрабатываемой в программных комплексах, входящих в состав сегмента РИС «Контингент»», утвержденный Главой Барабинского района.

2.1.4 Знать и выполнять правила работы со средствами защиты информации (средствами разграничения доступа), используемыми на персональных компьютерах в соответствии с инструкциями, требованиями, регламентирующими функционирование установленных средств защиты.

2.1.5 Хранить в тайне свой пароль доступа в сегменте РИС «Контингент» администрации Барабинского района, а также информацию о системе защиты, установленной в сегменте РИС «Контингент» администрации Барабинского района.

2.1.6 Немедленно ставить в известность Администратора ИС и/или Администратора ИБ:

- в случае утери носителя с Информацией и/или при подозрении компрометации личных ключей и паролей;
- нарушений целостности пломб (наклеек с защитной и идентификационной

докладов, научных работ и т.д.;

- выполнять работы с документами, содержащими Информацию, на дому, выносить их из служебных помещений, снимать копии или производить выписки из таких документов без разрешения Ответственного за обработку и защиту информации;
- оставлять на рабочих столах, в столах и незакрытых сейфах документы, содержащие Информацию, а также оставлять незапертыми и не опечатанными после окончания работы сейфы, помещения и хранилища с документами, содержащими Информацию;
- использовать компоненты программного и аппаратного обеспечения сегмента РИС «Контингент»администрации Барабинского района в неслужебных целях;
- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств АРМ или устанавливать дополнительно любые программные и аппаратные средства (в том числе отключать (блокировать) СЗИ);
- осуществлять обработку Информации в присутствии посторонних (не допущенных к данной информации) лиц;
- подключать к АРМ и корпоративной информационной сети личные внешние носители и мобильные устройства;
- записывать и хранить Информацию на неучтенных носителях информации;
- оставлять включенной без присмотра свое АРМ, не активизировав средства защиты информации от НСД (временную блокировку экрана);
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок – ставить в известность Администратора ИС и/или Администратора ИБ.
- обсуждать с посторонними лицами процедуры доступа к сегменту РИС «Контингент»администрации Барабинского района и обрабатываемую Информацию.

2.8 Без согласования с Администратором ИБ Пользователю запрещается:

- производить установку программных средств;
- самостоятельно устанавливать, тиражировать или модифицировать программное и аппаратное обеспечение;
- изменять установленный алгоритм функционирования аттестованного сегмента РИС «Контингент»администрации Барабинского района;
- запускать на рабочем месте файлы, не связанные с исполнением Пользователем служебных обязанностей;
- открывать общий доступ к папкам на своей рабочей станции;
- привлекать посторонних лиц для производства ремонта или настройки АРМ сегмента РИС «Контингент» администрации Барабинского района.

3 Права пользователя

3.1 Пользователь имеет право:

3.1.1 Требовать от своего непосредственного руководителя обеспечения организационно-технических условий, необходимых для исполнения обязанностей.

3.1.2 Получать доступ к информации, материалам, техническим средствам, помещениям, необходимых для надлежащего исполнения своих обязанностей.

4 Ответственность пользователя

4.1 Пользователь несет ответственность за соблюдение требований настоящей инструкции, а также нормативных документов в области защиты информации.

4.2 Пользователь несет ответственность за нарушения в работе аттестованного сегмента РИС «Контингент»администрации Барабинского района, вызванные его неправомерными действиями или неправильным использованием предоставленных прав, предусмотренных настоящей инструкцией.

4.3 Пользователь отвечает за правильность включения и выключения АРМ сегмента РИС «Контингент»администрации Барабинского района и всех действий при работе с ним.

4.4 За разглашение Информации, а также за нарушение порядка работы с документами или машинными носителями информации, работники могут быть привлечены к дисциплинарной или иной предусмотренной законодательством ответственности.

Приложение № 2
к постановлению от «___» _____ 201__ г. № ____

ИНСТРУКЦИЯ

по порядку обращения со средствами защиты информации в сегменте регионального сегмента единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам на территории Барабинского района

1. Общие положения

1.1. Инструкция по порядку обращения со средствами защиты информации в сегменте регионального сегмента единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам на территории Барабинского района (далее – сегмент РИС «Контингент» администрации Барабинского района) (далее – Инструкция) регламентирует порядок обращения со средствами защиты информации в процессе получения, хранения, доставки, передачи, встраивания в прикладные системы, тестирования в целях защиты информации, обрабатываемой с использованием средств автоматизации.

1.2. Настоящая Инструкция подготовлена в соответствии с требованиями нормативно-методических документов ФСТЭК России и ФСБ России по защите информации ограниченного доступа (в том числе персональных данных), не содержащую сведения, составляющие государственную тайну.

1.3. В настоящей Инструкции используются следующие понятия и определения:

1.3.1. Доступ к информации – возможность получения информации и ее использования.

1.3.2. Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

1.3.3. Контролируемая зона – пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, а также транспортных, технических или иных средств. Границей контролируемой зоны может быть: периметр охраняемой территории предприятия (учреждения), ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения.

1.3.4. Средство защиты информации (СЗИ) – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации, не являющееся криптосредством.

1.4. Для обеспечения безопасности информации при ее обработке в сегменте РИС «Контингент» администрации Барабинского района должны использоваться сертифицированные в системе сертификации ФСТЭК России СЗИ (имеющие положительное заключение экспертной организации о соответствии требованиям нормативных документов по безопасности информации).

2. Учет СЗИ

2.1. Инсталлирующие СЗИ носители и установленные СЗИ подлежат поэкземплярному учету администратором информационной безопасности (далее – ИБ).

2.2. Программные СЗИ учитываются совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование. Если аппаратные или аппаратно-программные СЗИ подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств, то такие СЗИ учитываются также совместно с соответствующими аппаратными средствами.

2.3. Эксплуатационная и техническая документация к СЗИ подлежит поэкземплярному учету администратором ИБ.

2.4. СЗИ, а также эксплуатационная и техническая документация к СЗИ должны быть упакованы в прочную упаковку, исключающую возможность их физического повреждения и внешнего воздействия.

2.5. Полученные упаковки с СЗИ, а также с эксплуатационной и технической документацией к ним, вскрываются администратором ИБ. Администратор ИБ проверяет целостность упаковки и содержимого.

2.6. Уничтожение СЗИ:

2.6.1. СЗИ уничтожаются (утилизируются) по решению комиссии по проведению мероприятий по защите информации совместно с Администратором ИБ.

2.6.2. Намеченные к уничтожению (утилизации) СЗИ изымаются из аппаратных средств, с которыми они функционировали. При этом СЗИ считаются изъятыми из аппаратных средств, если исполнена предусмотренная эксплуатационной и технической документацией к СЗИ процедура удаления программного обеспечения СЗИ, и они полностью отсоединены от аппаратных средств.

2.6.3. Пригодные для дальнейшего использования узлы и детали аппаратных средств общего назначения используются после уничтожения СЗИ без ограничений.

2.7. Эксплуатационная и техническая документация к СЗИ уничтожается путем сжигания или с помощью любых бумагорезательных машин.

3. Эксплуатация хранилищ

3.1. Инсталлирующие СЗИ носители, эксплуатационная и техническая документация к СЗИ должна храниться в металлических хранилищах (ящиках, шкафах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

4. Контроль безопасности СЗИ

4.1. Текущий контроль за организацией и обеспечением функционирования СЗИ возлагается на Ответственного за обработку и защиту информации и Администратора ИБ в пределах их полномочий.

5. Модификация программного обеспечения и аппаратных и технических средств

5.1. Все изменения конфигурации сегмента РИС «Контингент» администрации Барабинского района должны производиться только на основании заявок пользователей

сегмента РИС «Контингент» администрации Барабинского района, согласованных с Ответственным за обработку и защиту информации, на имя Администратора ИБ.

5.2. Право внесения изменений в конфигурацию сегмента РИС «Контингент» администрации Барабинского района предоставляется:

- в отношении системных и прикладных программных средств, а также в отношении аппаратных средств – уполномоченному Администратору ИС;
- в отношении СЗИ – уполномоченному Администратору ИБ.

5.3. Изменение конфигурации сегмента РИС «Контингент» администрации Барабинского района, кроме уполномоченных работников, запрещено.

5.4. Установка, изменение (обновление) и удаление системных и прикладных программных средств производится Администратором сегмента РИС «Контингент» администрации Барабинского района.

5.5. Подготовка модификаций программного обеспечения (далее – ПО) средств вычислительной техники (далее – СВТ), тестирование, стендовые испытания и передача исходных текстов, документации и дистрибутивных носителей программ в архив эталонных дистрибутивов, и другие необходимые действия производятся Администратором ИС.

5.6. Установка и обновление общего программного обеспечения на СВТ производится с оригинальных лицензионных дистрибутивных носителей (компакт дисков и т.п.), полученных установленным порядком, а прикладного ПО – с эталонных копий программных средств.

5.7. Все добавляемые программные и аппаратные компоненты должны быть предварительно установленным порядком проверены на работоспособность, а также отсутствие опасных функций.

5.8. После установки (обновления) ПО Администратор ИС должен произвести настройку средств управления доступом к компонентам данной задачи (программного средства) в соответствии с ее (его) формуляром. Администратор ИБ должен проверить работоспособность ПО и правильность настройки СЗИ.

5.9. При изъятии СВТ из состава сегмента РИС «Контингент» администрации Барабинского района его передача на склад, в ремонт или в другое подразделение для решения иных задач осуществляется только после того, как Администратор ИБ снимет с данной СВТ средства защиты и предпримет необходимые меры для затирания защищаемой информации, которая хранилась на дисках СВТ. Факт уничтожения защищаемой информации, находившейся на диске СВТ, оформляется актом за подписью Администратора ИБ.

6. Экстренная модификация (обстоятельства форс-мажор)

6.1. В исключительных случаях (сбой ПО, не позволяющий продолжить работу), требующих безотлагательного изменения ПО, допускается корректировка программ непосредственно на СВТ. Факт внесения изменений в ПО СВТ фиксируется актом за подписями Администратора ИС, Администратора ИБ и пользователя данного СВТ. В акте указывается причина модификации, перечисляются файлы, подвергшиеся изменению, и указывается лицо(а), проводившее изменения.

6.2. В течение следующего дня после составления акта Администратором сегмента, Администратором ИБ при участии пользователей сегмента РИС «Контингент»

администрации Барабинского района выясняются причины и состав проведенных экстренных изменений, и принимается решение о необходимости подготовки исправительной модификации ПО или восстановления ПО СВТ с эталонной копии. Необходимость участия в разбирательстве пользователя сегмента РИС «Контингент» администрации Барабинского района определяется руководством. Результат разбирательства оформляется в виде согласованного решения и хранится у Администратора ИС, копии передаются Администратору ИБ.

7. Ответственность

7.1. Пользователи сегмента РИС «Контингент» администрации Барабинского района несут персональную ответственность за сохранность полученных СЗИ, эксплуатационной и технической документации к СЗИ, за соблюдение положений настоящей Инструкции.

7.2. Ответственный за обработку и защиту информации в сегменте РИС «Контингент»администрации Барабинского района несет ответственность за соответствие проводимых им мероприятий по организации и обеспечению безопасности обработки информации с использованием СЗИ лицензионным требованиям и условиям эксплуатационной и технической документации к СЗИ, а также настоящей Инструкции.

Приложение № 3
к постановлению от «___» _____201_ г. № _____

ТИПОВАЯ ФОРМА

УТВЕРЖДАЮ
Глава Барабинского района
_____Е.В.Бессонов

«____»_____ 201_ г.

АКТ

установки средств защиты информации
на объекте вычислительной техники – автоматизированное рабочее место
на базе автономной ПЭВМ (инв. № _____)

«____» _____ 201_ года произведена установка следующих средств защиты информации:

№ п/п	Наименование и тип технического средства	Заводской (серийный) номер	Сведения о сертификате	Место и дата установки
1				
2				

Монтаж средств защиты информации выполнен в соответствии с требованиями технической документации. В ходе инструментальной проверки установлено, что средства защиты информации работоспособны и обеспечивают защищенность информации.

После установки комплекса _____ системный блок инв. № _____ опечатан специальным защитным знаком с надписью «НЕ ВСКРЫВАТЬ» и логотипом организации-исполнителя. Вскрытие системных блоков без согласования с организацией-исполнителем запрещено.

Председатель комиссии: _____ _____
(фамилия, имя, отчество) (подпись)

Члены комиссии: _____ _____
(фамилия, имя, отчество) (подпись)

_____ _____
(фамилия, имя, отчество) (подпись)

_____ _____
(фамилия, имя, отчество) (подпись)

«___» _____ 20__г.

Приложение № 4
к постановлению от «___» _____ 201_ г. № _____

ПРАВИЛА
идентификации и аутентификации субъектов доступа и объектов доступа в сегменте регионального сегмента единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам на территории Барабинского района

1. Общие положения

1.1. Данные 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 сегменте регионального сегмента единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам на территории Барабинского района (далее – сегмент РИС «Контингент» администрации Барабинского района) и контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

2. Идентификация и аутентификация пользователей, являющихся внутренними пользователями

2.1. При доступе в сегменте РИС «Контингент» администрации Барабинского района осуществляется идентификация и аутентификация пользователей, являющихся работниками администрации Барабинского района (внутренних пользователей), и процессов, запускаемых от имени этих пользователей, а также процессов, запускаемых от имени системных учетных записей. К внутренним пользователям относятся должностные лица администрации Барабинского района:

- администратор ИС;
- администратор информационной безопасности (ИБ);
- ответственные работники по работе с ИС, выполняющие свои должностные обязанности (функции) в соответствии с должностными регламентами (инструкциями), утвержденными в учреждении и которым в сегменте РИС «Контингент»администрации Барабинского района присвоены учетные записи. .

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 сегмента РИС «Контингент» администрации Барабинского

района (ремонт, гарантийное обслуживание, регламентные и иные работы) в соответствии с организационно-распорядительными документами администрации Барабинского района. Для каждого внутреннего пользователя в сегменте РИС «Контингент»администрации Барабинского района должны быть заведены учетные записи.

2.2. Пользователи сегмента РИС «Контингент» администрации Барабинского района 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 сегменте регионального сегмента единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам на территории Новосибирской области администрации Барабинского района».

2.3. Аутентификация пользователя в сегменте РИС «Контингент»администрации Барабинского района осуществляется с использованием паролей. Также на усмотрение администратора ИБ могут применяться аппаратные средства в случае многофакторной (двухфакторной) аутентификации.

2.4. В сегменте РИС «Контингент» администрации Барабинского района обеспечивается возможность однозначного сопоставления идентификатора пользователя с запускаемыми от его имени процессами.

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

3.1. В сегменте РИС «Контингент» администрации Барабинского района устанавливаются и реализуются следующие функции управления идентификаторами пользователей и устройств:

- формирование идентификатора, который однозначно идентифицирует пользователя и (или) устройство;
- присвоение идентификатора пользователю и (или) устройству;
- предотвращение повторного использования идентификатора пользователя и (или) устройства в течение одного года;
- блокирование идентификатора пользователя после 90 дней неиспользования.

3.2. В качестве ответственного за создание, присвоение и уничтожение идентификаторов пользователей и устройство пределен Администратор ИБ.

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

4.1. В сегменте РИС «Контингент». администрации Барабинского района устанавливаются и реализуются следующие функции управления средствами аутентификации (аутентификационной информацией) пользователей и устройств:

- изменение аутентификационной информации (средств аутентификации), заданных их производителями и (или) используемых при внедрении системы защиты сегмента РИС «Контингент»администрации Барабинского района;
- выдача средств аутентификации пользователям;
- генерация и выдача начальной аутентификационной информации (начальных значений средств аутентификации);
- установление характеристик пароля: длина пароля не менее шести символов, алфавит пароля не менее 60 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 –5 минут, смена паролей не более чем через 120 дней;
- блокирование (прекращение действия) и замена утерянных, скомпрометированных или поврежденных средств аутентификации;
- назначение необходимых характеристик средств аутентификации (в том числе механизма пароля);
- обновление аутентификационной информации (замена средств аутентификации) с периодичностью не более, чем через 120 дней;
- защита аутентификационной информации от неправомерных доступа к ней и модифицирования.

4.2. В случае компрометации личного пароля пользователя сегмента РИС «Контингент» администрации Барабинского района должны быть немедленно предприняты меры в зависимости от полномочий владельца скомпрометированного пароля:

- Внеплановая смена личного пароля или удаление учетной записи пользователя сегмента РИС «Контингент»администрации Барабинского района в случае прекращения его полномочий (увольнение, переход на другую работу внутри организации и т.п.) должна производиться Администратором ИБ немедленно после окончания последнего сеанса работы данного пользователя с системой.
- Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри организации другие обстоятельства) Администратора ИБ и других работников, которым по роду работы были предоставлены полномочия по управлению парольной защитой сегмента РИС «Контингент»администрации Барабинского района.

4.3. 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.

5. Защита обратной связи при вводе аутентификационной информации

5.1. В сегменте РИС «Контингент» администрации Барабинского района осуществляется защита аутентификационной информации в процессе ее ввода для аутентификации от возможного использования лицами, не имеющими на это полномочий.

5.2. 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.

6. Ответственность при организации идентификации и аутентификации

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

6.2. Ответственность за поддержание установленного порядка и соблюдение требований настоящих Правил возлагается на Администратора ИБ и пользователей сегмента РИС «Контингент»администрации Барабинского района.

6.3. Периодический контроль за выполнением всех требований настоящих Правил осуществляется комиссией по проведению мероприятий по защите информации.

Приложение № 5
к постановлению от «___» _____ 201__ г. № _____

ПРАВИЛА

по ограничению программной среды в сегменте регионального сегмента единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам на территории Барабинского района

1. Общие положения

1.1. Настоящие Правила регламентируют контроль использования в сегменте регионального сегмента единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам на территории Барабинского района (далее – сегмент РИС «Контингент» администрации Барабинского района) программного обеспечения, разрешенного к использованию, и возможности восстановления программного обеспечения при возникновении внештатных ситуаций.

2. Установка (инсталляция) только разрешенного к использованию программного обеспечения и его компонентов

2.1. Установка (инсталляция) в сегменте РИС «Контингент» администрации Барабинского района программного обеспечения (вида, типа, класса программного обеспечения) и (или) его компонентов осуществляется с учетом Перечня программного обеспечения, разрешенного к использованию в сегменте РИС «Контингент» администрации Барабинского района.

2.2. Установка (инсталляция) в сегменте РИС «Контингент» администрации Барабинского района программного обеспечения и (или) его компонентов осуществляется только от имени администратора.

2.3. В сегменте РИС «Контингент» администрации Барабинского района администратором информационной безопасности обеспечивается контроль не реже одного раза в три месяца установленного (инсталлированного) в сегменте РИС «Контингент» администрации Барабинского района программного обеспечения на предмет соответствия его «Перечню программного обеспечения, разрешенного к использованию в сегменте регионального сегмента единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам на территории Барабинского района», а также на предмет отсутствия программного обеспечения, запрещенного в сегменте РИС «Контингент»администрации Барабинского района к установке.

2.4. Пересмотр «Перечня программного обеспечения, разрешенного к использованию в сегменте регионального сегмента единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам на территории Барабинского района области, может осуществляться по заявке пользователя,

согласованной с непосредственным руководителем пользователя и администратором информационной безопасности.

3. Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций

3.1. Возможность восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций предусматривает:

– восстановление программного обеспечения, включая программное обеспечение средств защиты информации, из резервных копий (дистрибутивов) программного обеспечения – выполняется администраторами в рамках, возложенных на них функций;

– восстановление и проверку работоспособности системы защиты информации, обеспечивающей необходимый уровень защищенности информации, - выполняется администратором информационной безопасности;

– возврат сегмента РИС «Контингент» администрации Барабинского района в начальное состояние (до возникновения нештатной ситуации), обеспечивающее их штатное функционирование, или восстановление отдельных функциональных возможностей сегмента РИС «Контингент» администрации Барабинского района, позволяющих решать задачи по обработке информации - выполняется администраторами в рамках возложенных на них функций.

3.2. В случае, когда восстановление работоспособности системы защиты информации невозможно, администратором информационной безопасности, должны применяться компенсирующие меры защиты информации.

Приложение № 6
к постановлению от «___» _____ 201__ г. № ___

ПЕРЕЧЕНЬ

программного обеспечения, разрешенного к использованию в сегменте регионального сегмента единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам на территории Барабинского района

Наименование	Версия	Производитель	Автозапуск при запуске операционной системы	Дополнительные параметры запуска*
«ФЛАК ОО-1»	19.1.0.0	ГИВЦ	Автозапуск	
«ФЛАК ОШ-1, ОШ-S»	12.0.0.0	ГИВЦ	Автозапуск	
Adobe Flash Player 10 AtiveX	10.1.536 4	Adobe Systems Incorporated	Автозапуск	
Adobe Flash Player 18 NPAPI	18.0.0.2 09	Adobe Systems Incorporated	Автозапуск	
Adobe Shockwaver Player 11,5	11.5.6.6 06	Adobe Systems, Inc	Автозапуск	
Clik				

*В дополнительных параметрах запуска указывается:

– ограничение запуска компонентов программного обеспечения от имени администраторов информационной безопасности (например, разрешение такого запуска только для программного обеспечения средств защиты информации: сенсоры систем обнаружения вторжений, агенты систем мониторинга событий информационной безопасности, средства антивирусной защиты);

– параметры запуска компонентов программного обеспечения от имени учетной записи администратора информационной безопасности таким образом, чтобы текущий пользователь средства вычислительной техники не мог получить через данные компоненты доступ к объектам доступа, на доступ к которым у него нет прав.

Приложение № 7
к постановлению от «___»_____ 201__ г. № _____

ПРАВИЛА

регистрации событий безопасности в сегменте регионального сегмента единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам на территории Барабинского района

1.Общие положения

1.1. 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 сегменте регионального сегмента единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам на территории Барабинского района (далее – сегмент РИС «Контингент» администрации Барабинского района).

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

2.1. В сегменте РИС «Контингент» администрации Барабинского района подлежат регистрации в текущий момент времени события безопасности, утвержденные «Перечнем событий безопасности в сегменте регионального сегмента единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам на территории Барабинского района, подлежащих регистрации».

2.2. Состав и содержание информации о событиях безопасности, подлежащих регистрации, определяются в соответствии с пунктом 3 настоящих Правил.

2.3. Сроки хранения соответствующих записей регистрационных журналов должны обеспечивать возможность обнаружения, идентификации и анализа инцидентов, возникших в сегмент РИС «Контингент» администрации Барабинского района, в течение 3 месяцев.

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

3.1. 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.

3.2. Состав и содержание информации о событиях безопасности, включаемой в записи регистрации о событиях безопасности, приведены в «Перечне событий безопасности в сегменте регионального сегмента единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам на территории Барабинского района, подлежащих регистрации».

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

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

– возможность выбора администратором информационной безопасности событий безопасности, подлежащих регистрации в текущий момент времени из перечня событий безопасности, определенных в соответствии с «Перечнем событий безопасности в сегменте регионального сегмента единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам на территории Барабинского района, подлежащих регистрации»;

– генерацию (сбор, запись) записей регистрации (аудита) для событий безопасности, подлежащих регистрации (аудиту) в соответствии с «Перечнем событий безопасности в сегменте регионального сегмента единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам на территории Барабинского района, подлежащих регистрации», с составом и содержанием информации, установленными для соответствующего типа события;

– хранение информации о событиях безопасности в течение времени, установленного в соответствии с пунктом 2 настоящих правил.

4.2. Объем памяти для хранения информации о событиях безопасности рассчитывается и выделяется администратором информационной безопасности сегмента РИС «Контингент» администрации Барабинского района с учетом типов событий безопасности, подлежащих регистрации в соответствии с «Перечнем событий безопасности в сегменте регионального сегмента единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам на территории Барабинского района, подлежащих регистрации», составом и содержанием информации о событиях безопасности, подлежащих регистрации, прогнозируемой частоты возникновения подлежащих регистрации событий безопасности, срока хранения информации о зарегистрированных событиях безопасности.

5. Реагирование на сбои при регистрации событий безопасности

5.1. В сегменте РИС «Контингент» администрации Барабинского района реагирование на сбои при регистрации событий безопасности (в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти) должно предусматривать:

– предупреждение (сигнализация, индикация) администратора информационной безопасности о сбоях (аппаратных и программных ошибках, сбоях в механизмах сбора информации или переполнения объема (емкости) памяти) при регистрации событий безопасности;

– реагирование на сбои при регистрации событий безопасности путем изменения администратором информационной безопасности параметров сбора, записи и хранения информации о событиях безопасности, в том числе отключение записи информации о событиях безопасности от части компонентов сегмента РИС «Контингент» администрации Барабинского района, запись поверх устаревших хранимых записей событий безопасности.

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

6.1. Мониторинг (просмотр и анализ) записей регистрации (аудита) должен проводиться администратором информационной безопасности не реже одного раза в неделю для всех событий, подлежащих регистрации в соответствии с «Перечнем событий безопасности в сегменте регионального сегмента единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам на территории Барабинского района, подлежащих регистрации», и обеспечивать своевременное выявление признаков инцидентов безопасности в ИС.

6.2. В случае выявления признаков инцидентов безопасности в сегменте РИС «Контингент» администрации Барабинского района администратор информационной безопасности осуществляет планирование и проведение мероприятий по реагированию на выявленные инциденты безопасности.

7. Генерирование временных меток и (или) синхронизация системного времени в информационной системе

7.1. В сегменте РИС «Контингент» администрации Барабинского района осуществляется генерирование надежных меток времени и синхронизация системного времени.

7.1.1. Получение меток времени, включающих дату и время, используемых при генерации записей регистрации (аудита) событий безопасности в сегменте РИС «Контингент администрации Барабинского района достигается посредством применения внутренних системных часов информационной системы или путем синхронизации системного времени.

8. Защита информации о событиях безопасности

8.1. Защита информации о событиях безопасности (записях регистрации (аудита)) в сегменте РИС «Контингент» администрации Барабинского района 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.

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

Приложение № 8
к постановлению от «___» _____ 201_ г. №_____

ПЕРЕЧЕНЬ

событий безопасности в сегменте регионального сегмента единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам на территории Барабинского района, подлежащих регистрации

№	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	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.	Запуск (завершение) работы	Дата и время запуска (завершения) работы

№	События безопасности, подлежащие регистрации	Состав и содержание информации о событиях безопасности
	компонентов виртуальной инфраструктуры	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

Приложение № 9
к постановлению от «___» _____ 201_ г. №_____

ИНСТРУКЦИЯ

по контролю защищенности информации в сегменте регионального сегмента единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам на территории Барабинского района

1. Общие положения

1.1. Настоящая инструкция регламентирует контроль уровня защищенности информации, обрабатываемой в сегменте регионального сегмента единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам на территории Барабинского района (далее – сегмент РИС «Контингент» администрации Барабинского района), 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 сегменте РИС «Контингент» администрации Барабинского района 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 администрации Барабинского района (Оператора) (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.

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 сегменте РИС «Контингент» администрации Барабинского района.

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 (настройки средств защиты информации, изменение режима и порядка использования сегмента РИС «Контингент» администрации Барабинского района), направленные на устранение возможности использования выявленных уязвимостей.

2.5. В сегменте РИС «Контингент» администрации Барабинского района 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 сегменте РИС «Контингент» администрации Барабинского района 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. Администратор информационной безопасности проводит анализ журналов регистрации событий безопасности (журнала аудита) в целях определения, были ли выявленные уязвимости ранее использованы в сегмент РИС «Контингент» администрации Барабинского района для нарушения безопасности информации.

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

3.1. В сегменте РИС «Контингент» администрации Барабинского района 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 сегменте РИС «Контингент» администрации Барабинского района 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 сегменте РИС «Контингент» администрации Барабинского района 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 сегменте регионального сегмента единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам на территории Барабинского района, 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 сегмента РИС «Контингент» администрации Барабинского района 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 сегмента РИС «Контингент» администрации Барабинского района 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 сегменте РИС «Контингент» администрации Барабинского района осуществляется:

6.1.1. контроль правил генерации и смены паролей пользователей в соответствии с «Правилами идентификации и аутентификации пользователей в сегменте регионального сегмента единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам на территории Барабинского района»;

6.1.2. контроль заведения и удаления учетных записей пользователей в соответствии с «Положением об управлении доступом субъектов доступа к объектам доступа в сегменте регионального сегмента единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам на территории Барабинского района»;

6.1.3. контроль реализации правил разграничения доступом в соответствии с «Положением об управлении доступом субъектов доступа к объектам доступа в сегменте регионального сегмента единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам на территории Барабинского района»;

6.1.4. контроль реализации полномочий пользователей в соответствии с «Положением об управлении доступом субъектов доступа к объектам доступа в сегменте регионального сегмента единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам на территории Барабинского района»;

6.1.5. 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 администрации Барабинского района;

6.1.6. 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 сегменте РИС «Контингент» администрации Барабинского района проводится администратором информационной безопасности не реже одного раза в три месяца.

Приложение № 10
к постановлению от «___» _____ 201_ г. №_____

ИНСТРУКЦИЯ

по антивирусной защите в сегменте регионального сегмента единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам на территории Барабинского района

Общие положения

1.1 Настоящая Инструкция предназначена для всех работников администрации Барабинского района (далее – сегмент РИС «Контингент» администрации Барабинского района), имеющих доступ к сегменту РИС «Контингент» администрации Барабинского района.

1.2 Инструкция устанавливает требования и ответственность при организации защиты информации от воздействия вредоносных компьютерных вирусов.

1.3 Инструкция регулирует вопросы организации антивирусной защиты и требования к порядку проведения антивирусного контроля при работе в сегменте РИС «Контингент» администрации Барабинского района.

2 Обеспечение антивирусной защиты

2.1 Порядок организации антивирусной защиты.

2.1.1 Для организации антивирусной защиты сегмента РИС «Контингент» администрации Барабинского района допускаются к использованию только сертифицированные ФСТЭК России лицензионные антивирусные средства общего применения.

2.1.2 Антивирусное средство защиты должно быть установлено на все средства вычислительной техники (СВТ) (при наличии технической возможности), входящие в сегменте РИС «Контингент» администрации Барабинского района.

2.1.3 В сегменте РИС «Контингент» администрации Барабинского района права по управлению (администрированию) средствами антивирусной защиты предоставлены только администратору информационной безопасности.

2.1.4 Разработка и осуществление мероприятий по проведению антивирусного контроля осуществляется ответственным за обработку и защиту информации с привлечением (при необходимости) администратора информационной безопасности и /или специалистов лицензированной организации.

2.1.5 Должностные лица не должны допускать использования в сегменте РИС «Контингент» администрации Барабинского района программного обеспечения и данных, не связанных с выполнением должностных обязанностей.

2.1.6 Расширенный антивирусный контроль проводится администратором информационной безопасности не реже одного раза в месяц и при необходимости, в случае подозрений в заражении вирусной программой.

2.1.7 При загрузке, открытии или исполнении объектов (файлов) из внешних источников средствами антивирусной защиты проводится автоматическая проверка объектов (файлов).

объектов (файлов).

2.2 Порядок проведения антивирусного контроля.

2.2.1 Устанавливаемое (изменяемое) программное обеспечение предварительно проверяется администратором информационной безопасности на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера, должна быть выполнена антивирусная проверка администратором информационной безопасности.

2.2.2 При загрузке компьютера средствами антивирусной защиты проводится антивирусный контроль в автоматическом режиме.

2.2.3 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 сегмент РИС «Контингент» администрации Барабинского района самостоятельно или вместе с администратором информационной безопасности проводит внеочередной антивирусный контроль своей рабочей станции для определения факта наличия или отсутствия компьютерного вируса.

2.2.4 В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователи сегмента РИС «Контингент» администрации Барабинского района обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя и администратора информационной безопасности, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов;
- в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, направить зараженный вирусом файл на съемном носителе информации администратору информационной безопасности для дальнейшей передачи его в организацию, с которой заключен договор на антивирусную поддержку (при наличии);
- по факту обнаружения зараженных вирусом файлов составить служебную записку администратору информационной безопасности, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

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

2.3.1 Администратор информационной безопасности обеспечивает получение из доверенных источников и установку обновлений базы данных признаков вредоносных компьютерных программ (вирусов).

2.3.2 Контроль целостности обновлений базы данных признаков вредоносных компьютерных программ (вирусов) обеспечивается путем автоматического получения или предварительно скачиваемых обновлений из официальных источников, например, с

сервера обновлений производителя антивирусного средства.

3 Ответственность при организации антивирусной защиты

3.1 Ответственность за организацию антивирусной защиты сегмента РИС «Контингент» администрации Барабинского района в соответствии с требованиями настоящей Инструкции возлагается на администратора информационной безопасности.

3.2 Ответственность за соблюдение требований настоящей Инструкции возлагается на администратора информационной безопасности, администратора сегмент РИС «Контингент» администрации Барабинского района, и пользователей, эксплуатирующих сегмент РИС «Контингент» администрации Барабинского района.