МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
Хабаровского края
(Минобрнауки Хабаровского края)

РАСПОРЯЖЕНИЕ

13.06.2023 № 826
г. Хабаровск

О государственной информационной системе "Государственная итоговая аттестация"

В соответствии с пунктом 2 статьи 98 Федерального закона от 29 декабря 2012 г. № 273-ФЗ "Об образовании в Российской Федерации", постановлением Правительства Российской Федерации от 29 ноября 2021 г. № 2085 "О федеральной информационной системе обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования, и приема граждан в образовательные организации для получения среднего профессионального и высшего образования и региональных информационных системах обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования":

1. Установить, что региональной информационной системой обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования, является государственная информационная система "Государственная итоговая аттестация" (далее – ГИС ГИА).

2. Утвердить:

1) Положение о ГИС ГИА;

2) Требования по обеспечению информационной безопасности удаленного автоматизированного рабочего места пользователя при обмене информацией в защищенной сети передачи данных краевого государственного казенного учреждения "Региональный центр оценки качества образования" (далее – КГКУ РЦОКО).

3. Ввести в эксплуатацию ГИС ГИА с 1 июля 2023 г.

4. Функции по эксплуатации, сопровождению, развитию ГИС ГИА и обеспечению требований безопасности информации при эксплуатации ГИС ГИА возложить на КГКУ РЦОКО.

Министр В.Г. Хлебникова

002278

УТВЕРЖДЕНО
распоряжением
министерства
образования и науки
Хабаровского края
от "13" 06. 2023 г. № 826

ПОЛОЖЕНИЕ
о государственной информационной системе "Государственная итоговая аттестация"

1. Общие положения

1.1. Настоящее положение определяет назначение и функциональные задачи государственной информационной системе "Государственная итоговая аттестация" (далее также – ГИС ГИА, система), структуру ГИС ГИА, пользователей ГИС ГИА, их роли, развитие ГИС ГИА, требования к защите информации в ГИС ГИА и порядок предоставления доступа к ГИС ГИА.

1.2. ГИС ГИА является региональной государственной информационной системой, обеспечивающей проведение государственной итоговой аттестации обучающихся, освоивших образовательные программы основного общего и среднего общего образования (далее – государственная итоговая аттестация), в том числе в форме единого государственного экзамена.

1.3. Сведения, составляющие государственную тайну, не подлежат обработке в ГИС ГИА.

1.4. Оператором ГИС ГИА является министерство образования и науки Хабаровского края (далее – Оператор). Функции по эксплуатации, сопровождению, развитию ГИС ГИА и обеспечению требований безопасности информации при эксплуатации ГИС ГИА возложены на краевое государственное казенное учреждение "Региональный центр оценки качества образования" (далее – КГКУ РЦОКО).

2. Назначение и функциональные задачи

2.1. Назначение ГИС ГИА:

1) создание единого информационного пространства для участников ГИС ГИА при проведении государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования, и приема граждан в образовательные организации для получения среднего профессионального и высшего образования и региональных информационных системах обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования;

2) информационное взаимодействие с Федеральной информационной

системой обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования, и приема граждан в образовательные организации для получения среднего профессионального и высшего образования и региональных информационных системах обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования (далее – ФИС ГИА и Приёма).

2.2. Функциональные задачи ГИС ГИА:

1) получение и передача контрольно-измерительных материалов для проведения итоговой аттестации обучающихся, освоивших образовательные программы основного общего образования;

2) формирование пакетов документов для проведения итоговой аттестации обучающихся, освоивших образовательные программы основного общего образования;

3) получение и обработка бланков итоговых экзаменов;

4) перевод бланков итоговых экзаменов в машиночитаемый вид (сканирование);

5) распознавание данных сканирования в специальном программном обеспечении;

6) сверка данных распознавания и сканирования (верификация);

7) проверка верифицированных данных итоговых экзаменов (экспертиза);

8) составление итоговых протоколов по результатам экспертизы;

9) хранение и передача информации по защищенным каналам связи.

3. Структура ГИС ГИА

ГИС ГИА состоит из независимых логических функциональных модулей (подсистем), взаимодействующих между собой:

подсистема "Планирование ЕГЭ";
подсистема "Планирование ГИА-9";
подсистема "Станция Администратора";
подсистема "Станция Сканирования";
подсистема "Станция Распознавания";
подсистема "Станция Верификации";
подсистема "Станция Старшего верификатора";
подсистема "управления БД";
подсистема "ОФИС";
подсистема "Станция печати".

4. Роли пользователей ГИС ГИА

4.1. Пользователями ГИС ГИА являются лица, уполномоченные на использование ГИС ГИА и получившее доступ в ГИС ГИА из числа сотрудников оператора КГКУ РЦОКО.

4.2. Роли пользователей ГИС ГИА определяют функции и полномочия пользователей в системе:

администратор информационной безопасности – специалист, исполняющий функции обслуживания, контроля и мониторинга событий, фиксируемых системами безопасности, контроля выполнения положений и требований нормативных документов по обеспечению информационной безопасности;

администратор ГИС ГИА – специалист, имеющий административный доступ к ГИС ГИА и обеспечивающий доступ к информационным ресурсам ГИС ГИА, управление информационными ресурсами, включая планирование баз данных, управление доступом пользователей в систему, определение ограничений и процедур, а также выполнение иных административных функций;

администратор проектов – лицо, осуществляющее распознавание в фоновом режиме, автоматизированную выгрузку данных в ГИС ГИА;

оператор станции сканирования – лицо, ответственное за сканирование и регистрацию бланков итоговых экзаменов;

оператор станции экспертизы – лицо, ответственное за распечатку изображений развернутых ответов для проверки экспертами предметной комиссии и протоколов для заполнения экспертами предметной комиссии, предоставление критериев оценивания, информирование о результатах работы предметной комиссии;

оператор станции верификации – лицо, ответственное за верификацию;

оператор станции распознавания – лицо, ответственное за распознавание;

оператор станции апелляции и коррекции – лицо, которое вносит в ГИС ГИА результаты рассмотрения апелляции, включая вложение копий необходимой апелляционной документации;

старший верификатор – лицо, ответственное за верификацию, сверку данных участников экзамена с данными внесенными в ГИС ГИА;

эксперт – лицо, ответственное за проверку экзаменационных работ и составление итоговых протоколов о прохождении экзамена.

5. Защита информации в ГИС ГИА

5.1. Защита информации в ГИС ГИА осуществляется в соответствии с действующим законодательством в сфере защиты информации.

5.3. Ответственным за обеспечение информационной безопасности назначается специалист КГКУ РЦОКО из числа штатных сотрудников.

6. Порядок предоставления доступа к ГИС ГИА

Доступ штатных сотрудников КГКУ РЦОКО организован на основании внутреннего распорядка и утвержденного списка доступа к ГИС ГИА.

7. Взаимодействие с внешними информационными системами

7.1. С целью проведения репликацией баз данных регионального и федерального уровня, ГИС ГИА взаимодействует с ФИС ГИА и Приема.

Взаимодействие информационных систем осуществляется с использованием защищенных сетей передачи данных КГКУ РЦОКО и оператора ФИС ГИА и Приема.

7.2. С целью формирования региональной информационной системы

данными об участниках экзаменов, экзаменов и иных сведений, в ГИС ГИА импортируются сведения, полученные от образовательных организаций Хабаровского края реализующих программы среднего общего образования и основного общего образования, и органов местного самоуправления, осуществляющих управление в сфере образования края.

Данные формируются в локальных автономных информационных системах персональных данных и передаются с помощью защищенной сети передачи данных КГКУ РЦОКО.

7.3. Требования по обеспечению информационной безопасности удаленного автоматизированного рабочего места пользователя при обмене информацией в защищенной сети передачи данных КГКУ РЦОКО устанавливаются оператором ГИС ГИА.

8. Финансирование ГИС ГИА

Финансирование ГИС ГИА осуществляется за счет средств краевого бюджета в пределах бюджетных ассигнований КГКУ РЦОКО.

Заместитель министра – начальник
управления инфраструктуры,
имущественного комплекса
и информатизации образования В.А. Бруцкий

УТВЕРЖДЕНЫ
распоряжением
министерства
образования и науки
Хабаровского края
от "13" 06. 2023 г. № 826

ТРЕБОВАНИЯ

по обеспечению информационной безопасности удаленного автоматизированного рабочего места пользователя при обмене информацией в защищенной сети передачи данных КГКУ РЦОКО

1. Общие положения

Защищенная сеть передачи данных КГКУ РЦОКО построена на базе технологии VipNet. Сеть зарегистрирована под № 1400 (далее – сеть VipNet № 1400).

Термины и сокращения:

АО – аппаратное обеспечение;

АРМ – удаленное автоматизированное рабочее место пользователя;

ВВК – воздействие вредоносного кода;

ВК – вредоносный код;

ЛВС – локальная вычислительная сеть;

НСД – несанкционированный доступ;

ОС – операционная система;

ПО – программное обеспечение;

ПАК – программно-аппаратный комплекс;

Пользователь – сотрудник организации, которому предоставлен доступ к сети ViPNet № 1400;

СрЗИ – средства защиты информации;

СКЗИ – средства криптографической защиты информации, обеспечивающие создание защищенного соединения и создание квалифицированной электронной подписи.

Защита ПО и АО от НСД и воздействия вредоносного кода при установке и использовании АРМ пользователя является составной частью общей задачи обеспечения безопасности информации внешних систем по отношению к АРМ пользователя. Наряду с применением СрЗИ от НСД и ВВК, необходимо выполнение целого ряда мер, включающего в себя организационно-технические и административные мероприятия, связанные с обеспечением правильности функционирования технических средств обработки и передачи информации, а также установление соответствующих правил для обслуживающего персонала, допущенного к работе с информацией ограниченного доступа.

Состав СрЗИ, применяемых на АРМ пользователя, зависит от способа

взаимодействия АРМ пользователя с защищаемой сетью ViPNet № 1400.

По способу взаимодействия с защищаемой сетью ViPNet № 1400 АРМ пользователя подразделяется на следующие типы:

тип 1. АРМ, взаимодействующий с сетью посредством прямого подключения к сети Интернет;

тип 2. АРМ, взаимодействующий с сетью посредством подключения к сети Интернет через ЛВС организации;

тип 3. АРМ, взаимодействующий с сетью посредством подключения по выделенным каналам связи через ЛВС организации.

2. Организация работ по защите от несанкционированного доступа

2.1. Защита информации от НСД должна обеспечиваться на всех технологических этапах обработки информации, в том числе при проведении ремонтных и регламентных работ. Защита информации от НСД должна предусматривать контроль эффективности средств защиты от НСД. Этот контроль может быть либо периодическим, либо инициироваться по мере необходимости пользователем или администратором информационной безопасности, периодичность контроля должна быть задокументирована в организационно-распорядительной документации организации эксплуатирующей АРМ пользователя. В организации, эксплуатирующей АРМ пользователя, приказом руководителя должно быть назначено лицо ответственное за обеспечение безопасности информации (далее – администратор информационной безопасности, АИБ), на которого возлагаются задачи организации работ по использованию АРМ пользователя, выработки соответствующих инструкций для пользователей, а также осуществления контроля за соблюдением описанных ниже требований.

2.2. Требования по размещению технических средств:

1) при размещении АРМ пользователя принимаются меры по исключению НСД в помещения, в которых размещен АРМ пользователя, посторонних лиц, по роду своей деятельности, не являющихся персоналом, допущенным к работе в этих помещениях;

2) внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им конфиденциальных документов и сведений, включая ключевую информацию.

2.3. Требования по установке общесистемного и специального ПО:

1) к установке общесистемного и специального ПО допускаются лица, уполномоченные приказом руководителя организации на проведение таких работ;

2) на технических средствах, предназначенных для работы с АРМ пользователя, а также на АРМ пользователя использовать только лицензионное ПО фирм-изготовителей;

3) установку ПО АРМ пользователя необходимо производить только с зарегистрированного, защищенного от записи носителя информации, исполь-

зование незарегистрированных, личных носителей информации не допускается;

4) на АРМ пользователя не должны устанавливаться средства разработки и отладчики ПО;

5) принятие мер, исключающих возможность несанкционированного не обнаруживаемого изменения аппаратной части технических средств, на которых установлено ПО АРМ пользователя (например, путем опечатывания системного блока и разъемов АРМ пользователя);

6) после завершения процесса установки должны быть выполнены действия, необходимые для осуществления периодического контроля целостности, установленного ПО на АРМ пользователя;

7) программное обеспечение, устанавливаемое на АРМ пользователя, не должно содержать возможностей, позволяющих:

модифицировать содержимое произвольных областей памяти;

модифицировать собственный код и код других подпрограмм;

модифицировать память, выделенную для других подпрограмм;

передавать управление в область собственных данных и данных других подпрограмм;

не санкционированно модифицировать файлы, содержащие исполняемые коды при их хранении на жестком диске;

повышать предоставленные привилегии;

модифицировать настройки ОС;

использовать недокументированные фирмой-разработчиком функции ОС.

3. Требования по защите от несанкционированного доступа при эксплуатации удаленного автоматизированного рабочего места пользователя

При организации работ по защите информации от НСД необходимо учитывать следующие требования:

1) необходимо разработать и применить политику назначения и смены паролей (для входа в ОС, BIOS, при шифровании на пароле и т.д.), использовать фильтры паролей в соответствии со следующими правилами:

длина пароля должна быть не менее 8-ми символов;

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

пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т. д.), а также общепринятые сокращения (USER, ADMIN, ALEX и т. д.);

при смене пароля новое значение должно отличаться от предыдущего не менее, чем в 4-х позициях;

личный пароль пользователь не имеет права сообщать никому;

периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 6-и месяцев. Число неудачных попыток ввода пароля должно быть ограничено числом 10.

Указанная политика обязательна для всех учетных записей, зарегистрированных в ОС;

2) средствами BIOS должна быть исключена возможность работы на АРМ пользователя, если во время его начальной загрузки не проходят встроенные тесты;

3) запрещается:

оставлять без контроля вычислительные средства, на которых эксплуатируется АРМ пользователя, после ввода ключевой информации либо иной информации ограниченного доступа;

осуществлять несанкционированное администратором информационной безопасности копирование ключевых носителей;

разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и т.п. иные средства отображения информации;

записывать на ключевые носители постороннюю информацию;

4) администратор информационной безопасности должен сконфигурировать ОС, в среде которой планируется использовать АРМ пользователя, и осуществлять периодический контроль сделанных настроек в соответствии со следующими требованиями:

не использовать нестандартные, измененные или отладочные версии ОС;

исключить возможность загрузки и использования ОС, отличной от предусмотренной штатной работой;

исключить возможность удаленного управления, администрирования и модификации ОС и ее настроек;

режимы безопасности, реализованные в ОС, должны быть настроены на максимальный уровень;

всем пользователям и группам, зарегистрированным в ОС, необходимо назначить минимально возможные для нормальной работы права;

должно быть исключено попадание в систему программ, позволяющих, пользуясь ошибками ОС, повышать предоставленные привилегии;

необходимо регулярно устанавливать пакеты обновления безопасности ОС (Service Packs, Hot fix и т.п.), обновлять антивирусные базы, а также исследовать информационные ресурсы по вопросам компьютерной безопасности с целью своевременной минимизации опасных последствий от возможного воздействия на ОС;

необходимо организовать и использовать систему аудита, организовать регулярный анализ результатов аудита;

необходимо организовать и использовать комплекс мероприятий антивирусной защиты;

необходимо исключить одновременную работу ОС с загруженной ключевой информацией нескольких пользователей.

4. Средства защиты от несанкционированного доступа

Для работы АРМ пользователя требуется применять программные, программно-аппаратные СрЗИ от НСД имеющих сертификат соответствия ФСТЭК России, таких как: "Secret Net Studio", "Соболь", и т.п. Сертификаты соответствия ФСТЭК России, формуляры, а также дистрибутивы с которых

производится установка СрЗИ от НСД должны быть в наличии у организации и должны быть предоставлены по требованию владельца VipNet сети № 1400.

5. Требования по обеспечению защиты от воздействий вредоносного кода

Вредоносный код – любой программный код (компьютерный вирус, троян, сетевой червь), приводящий к нарушению функционирования средств вычислительной техники и/или предназначенный для искажения, модификации, уничтожения, блокирования или несанкционированного копирования информации. Вредоносный код способен создавать свои копии, сохраняющие все его свойства и требующие для своего размножения другие программы, каналы связи или машинные носители.

Возможен следующий характер проявлений действий ВК:

искажение изображения на экране монитора;

искажение символов, вводимых с клавиатуры;

блокирование клавиатуры, звуковые эффекты;

стирание или порча отдельных частей диска или файлов;

повреждение загрузочных секторов жесткого диска ПЭВМ и серверов;

остановка загрузки или зависание компьютера, значительное замедление его работы;

уничтожение или искажение информации о системной конфигурации АРМ пользователя.

Вредоносный код может попасть на компьютер со сменного носителя (CD- ROM, USB флеш-накопителей и других носителей, даже если эти носители не содержат файлов), при загрузке файлов из сети, с сообщением, полученным по электронной почте, а также через уязвимости операционных систем просто при наличии сетевого подключения компьютера к локальной вычислительной сети.

При наличии технической возможности, обновление средств защиты и сигнатурных баз производится централизованно, с рабочего места администратора информационной безопасности, администратора программных средств защиты от воздействий вредоносного кода при условии его назначения. При проведении централизованных обновлений используется механизм ведения протокола средств защиты. Обновление сигнатурных баз должно выполняться ежедневно при наличии технической возможности, при отсутствии технической возможности выполнения обновления сигнатурных баз ежедневно, обновления должны выполняться не реже одного раза в 5 дней. Периодичность и способ обновления сигнатурных баз должны быть задокументированы в организационно-распорядительной документации по обеспечению безопасности информации организации.

В целях обеспечения защиты от воздействий вредоносного кода пользователю АРМ запрещается:

самостоятельно устанавливать программное обеспечение, в том числе командные файлы;

использовать при работе "зараженный" вредоносным кодом либо с подозрением на "заражение" носитель и/или файл;

использовать личные носители на АРМ пользователя;

использовать служебные носители на домашних компьютерах и в неслужебных целях;

самостоятельно проводить "лечение" носителя и/или файла;

самостоятельно отключать, удалять и изменять настройки установленных средств защиты.

Пользователь АРМ обязан:

проводить контроль на отсутствие ВК любых сменных и подключаемых носителей (CD-дисков, DVD-дисков, USB флеш-накопителей и т.п.) и файлов (ключевые носители средств криптографической защиты информации контролю на отсутствие ВК не подвергаются);

при появлении сообщений, формируемых средствами защиты информации, об обнаружении вредоносного кода пользователь АРМ должен немедленно прекратить работу и сообщить об этом руководителю и администратору информационной безопасности (или сотруднику, выполняющему эти функции);

при невозможности запуска средств защиты информации или при ошибках в процессе их выполнения пользователь АРМ должен немедленно прекратить работу и сообщить об этом руководителю и администратору информационной безопасности (или сотруднику, выполняющему эти функции).

Правила и рекомендации пользователю АРМ по защите от воздействий вредоносного кода:

первичный входной контроль на отсутствие ВК носителей, предназначенных для многоразовой записи информации (перезаписываемых компакт-дисков и DVD-дисков, USB флеш-накопителей и других подобных носителей) проводит пользователь при первом применении носителя на данном компьютере. Последующие контроли носителя производить перед каждым просмотром состава и содержимого файлов;

в целях исключения автозапуска исполняемых файлов со сменных носителей (CD, DVD, USB флеш-накопителей и т.п.) пользователю рекомендуется при присоединении носителя к компьютеру (вставка CD/DVD в лоток, вставка USB флеш-накопителей в порт USB) удерживать некоторое время (20-30 секунд) нажатой клавишу «Shift»;

входной контроль на отсутствие ВК компакт-дисков и DVD-дисков, предназначенных для одноразовой записи информации, проводит получатель (владелец) диска однократно с момента приобретения (получения) диска перед использованием его на компьютерах.

6. Средства по обеспечению антивирусной защиты

Для работы АРМ пользователя требуется применять программные средства антивирусной защиты имеющих сертификат соответствия ФСТЭК России, таких как: "Kaspersky Endpoint Security для Windows", "Dr. Web Enterprise Security Suite", и т.п. Сертификаты соответствия ФСТЭК Росси, формуляры, а также дистрибутивы с которых производится установка средств антивирусной защиты должны быть в наличии у организации и должны быть предоставлены

по требованию владельца VipNet сети № 1400.

7. Средства межсетевого экранирования

Взаимодействие всех типов АРМ (1, 2, 3) с защищаемой сетью должно быть защищено с помощью с средства межсетевого экранирования уровня хоста ViPNet Client.

Межсетевой экран уровня хоста ViPNet Client должен иметь действующие сертификаты соответствия ФСТЭК России, формуляры, а также дистрибутивы, с которых производится установка, должны быть в наличии у организации и должны быть предоставлены по требованию владельца VipNet сети № 1400.

Настройками межсетевого экрана должна быть АРМ пользователя должен быть сегментирован (отделен) от АРМ находящихся в ЛВС организации не задействованных в работе с сетью VipNet № 1400.

8. Требования по обращению со средствами криптографической защиты информации

Установка, настройка и сопровождение СКЗИ осуществляется администратором информационной безопасности организации в соответствии с требованиями законодательства Российской Федерации и эксплуатационной документации к СКЗИ.

Формуляр на СКЗИ в электронном виде, находящийся в составе документации на СКЗИ, выводится администратором информационной безопасности организации на бумажный носитель и заполняется от руки в части раздела "Сведения о закреплении изделия при эксплуатации". Ответственное хранение формуляра осуществляется администратором информационной безопасности организации.

Запрещается полное или частичное воспроизведение, тиражирование и распространение оптических носителей, содержащих дистрибутивы СКЗИ, а также лицензионных ключей СКЗИ.

Заместитель министра – начальник
управления инфраструктуры,
имущественного комплекса
и информатизации образования — В.А. Бруцкий