Для служебного пользования
Экз. № 2
Уч. № 04-28/10дсп

Государственное казённое учреждение Волгоградской области
«Центр информационных технологий Волгоградской области» (ГКУ ВО «ЦИТ ВО»)

УТВЕРЖДАЮ
Директор ГКУ ВО «ЦИТ ВО»

_____ А.В. Несытов
«28» ____10____ 2018 г.
М.П.

СОГЛАСОВАНО
Председатель комитета
информационных технологий
Волгоградской области

_____ С.П. Торбин
«28» ____10____ 2018 г.
М.П.

Программа и методика приемочных испытаний пользовательских сегментов государственной информационной системы «Единая информационная система в сфере образования Волгоградской области»

ЛИСТ УТВЕРЖДЕНИЯ

СОГЛАСОВАНО
Председатель комитета
образования, науки и
молодежной
политики Волгоградской
области

_____ Л.М. Савина
«28» ____10____ 2018 г.
М.П.

СОГЛАСОВАНО
Начальник отдела информационной
безопасности ГКУ ВО «ЦИТ ВО»

_____ С.П. Барыкин
«28» ____10____ 2018 г.
М.П.

2018

К ВХОД. № 190 дсп (2018)

К ВХОД. № 210 дсп (2018)

Программа и методика приемочных испытаний пользовательских сегментов государственной информационной системы «Единая информационная система в сфере образования Волгоградской области»

Изм.	Лист	№ докум.	Подп.	Дата			
Разраб.		Копылов В.Е.			Система защиты информации государственной информационной системы «Единая информационная система в сфере образования Волгоградской области» Программа и методика приемочных испытаний пользовательских сегментов	Лит	Лист 1 / Листов 33
Пров.		Барыкин С.П.					
Н. контр.						ГКУ ВО «ЦИТ ВО»	

Подп. и дата | Инв № дубл. | Взамен инв. | Подп. и дата | Инв №

Содержание

Термины, сокращения и определения

В настоящем документе используются следующие сокращения, термины и соответствующие им определения.

Условное обозначение	Определение
Абонент	Организация–владелец пользовательского сегмента, в отношении которого проводятся приемочные испытания
АРМ	Автоматизированное рабочее место
АРМ.П	Автоматизированное рабочее место, предназначенное для взаимодействия с центральным сегментом через веб-сервис
АС	Автоматизированная система
ЗИ	Защита информации
ИС	Информационная система
ИР	Информационный ресурс
ИБ	Информационная безопасность
Лицензиат	Организация, имеющая лицензию на осуществлении деятельности по технической защите конфиденциальной информации, привлекаемая в соответствии с законодательством Абонентом для выполнения мероприятий, предусмотренных ПМИ
ПАК	Программно-аппаратный комплекс
ПМИ	Программа и методика приемочных испытаний пользовательских сегментов ГИС
Помещения	Помещения, в которых размещены технические средства АРМ.П
НСД	Несанкционированный доступ
Оператор	Комитет информационных технологий Волгоградской области
ПДн	Персональные данные
ППО	Прикладное программное обеспечение
ПО	Программное обеспечение
СВТ	Средство вычислительной техники
СЗИ	Система защиты информации
СПО	Специализированное программное обеспечение
СрЗИ	Средства защиты информации
ФСБ	Федеральная служба безопасности
ФСТЭК	Федеральная служба по техническому и экспортному контролю
ГИС	Государственная информационная система «Единая информационная система в сфере образования Волгоградской области»
Центральный сегмент	Сегмент централизованной обработки и хранения защищаемой информации ГИС
ЦОД	Единый центр обработки данных Волгоградской области
МЭ	Межсетевой экран
НДВ	Недекларированные возможности
СОВ	Система обнаружения вторжений
САВЗ	Средство антивирусной защиты

1. Объект испытаний

Объектом приемочных испытаний является АРМ.П, включая его СЗИ, предназначенное для подключения в качестве пользовательского сегмента к центральному сегменту ГИС (АРМ.П).

СЗИ АРМ.П должна быть реализована в соответствии с Техническим проектом на создание системы защиты информации государственной информационной системы «Единая информационная система в сфере образования Волгоградской области» (уч. № 04-28/1дсп от 18.01.2018 г.) и включать следующие подсистемы:

- подсистему защиты информации от НСД;
- подсистему межсетевого экранирования;
- подсистему антивирусной защиты;
- подсистему криптографической защиты;
- подсистему обеспечения резервного копирования.

2. Цель испытаний

Целью приемочных испытаний является определение возможности подключения АРМ.П к центральному сегменту ГИС путем распространения на него действия аттестата соответствия государственной информационной системы «Единая информационная система в сфере образования Волгоградской области» требованиям безопасности информации № 04-28/15дсп от 13.03.2018 г. Для проведения испытаний необходимо выполнение следующих мероприятий:

- проверка соответствия СЗИ АРМ.П проектным решениям, используемым в аттестованных сегментах ГИС;
- проверка соответствия АРМ.П требованиям Регламента подключения к центральному сегменту ГИС, утвержденного приказом № 8 от 05.03.2018 г. (далее – Регламент);
- проверка работоспособности СрЗИ, установленных на АРМ.П.

3. Общие положения

3.1. Документы, на основании которых проводят испытания

Основанием для проведения испытаний являются:

- приказ от 07 июня 2017 г. №71 и 62-о/д «Об утверждении Положения о государственной информационной системе Волгоградской области «Единая информационная система в сфере образования Волгоградской области»;
- Регламент;

- решение Оператора о возможности распространения действующего аттестата соответствия ГИС на подключаемый пользовательский сегмент ГИС (на основании заявки Абонента на подключение пользовательского сегмента).

Испытания проводятся в соответствии с требованиями, содержащимися в следующих нормативных документах:

- ГОСТ 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения;

- ГОСТ 34.603-92 Информационная технология. Виды испытаний автоматизированных систем;

- РД 50-34.698-90 Автоматизированные системы. Требования к содержанию документов;

- приказ ФСТЭК от 11 февраля 2013 г. №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

- приказ Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. №378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

- Регламент;

- технический проект на создание системы защиты информации государственной информационной системы «Единая информационная система в сфере образования Волгоградской области», утвержденный 18.01.2018 г. (уч. № 04-28/1дсп).

3.2. Место и продолжительность испытаний

Испытания проводятся по адресу размещения АРМ.П.

Сроки по проведению испытаний устанавливаются совместно Абонентом и Лицензиатом.

3.3. Организации, участвующие в испытаниях

В проведении испытаний участвуют Абонент и Лицензиат.

3.4. Испытания, проведенные ранее

Настоящий документ определяет первичный порядок проведения испытаний АРМ.П, в отношении которых ранее испытания не проводились.

3.5. Документы, предъявляемые на испытания

На испытания предоставляются:

- акт классификации АРМ.П;
- модель угроз безопасности информации, обрабатываемой на АРМ.П;
- документация на СрЗИ, развернутые на АРМ.П;
- эксплуатационная документация на СЗИ АРМ.П;
- организационно-распорядительная документация по защите информации на АРМ.П.

4. Объем испытаний

4.1. Этапы испытаний

Приемочные испытания проводятся в 2 этапа:

1) В ходе первого этапа испытаний осуществляются следующие мероприятия:

- проверка отсутствия известных уязвимостей в программном обеспечении АРМ.П (Приложение 1);
- проверка готовности пользователей и администраторов к эксплуатации СЗИ АРМ.П (Приложение 2);
- проверка соответствия выполненных настроек СрЗИ АРМ.П требованиям Технического проекта (уч. № 04-28/1дсп от 18.01.2018 г.) (Приложение 3);
- проверка полноты и качества разработанной организационно-распорядительной документации по защите информации (Приложение 4);
- проверка соответствия АРМ.П требованиям Регламента (Приложение 5).

2) Второй этап включает проверку правильности функционирования СрЗИ.

4.2. Последовательность проведения испытаний

Приемочные испытания проводятся в соответствии с методиками, описанными в настоящем документе. Представители Абонента, участвующие в проверке, вместе с представителями Лицензиата фиксируют соответствие либо несоответствие результатов выполнения функции ожидаемым результатам в Протоколе приемочных испытаний.

4.3. Требования по испытаниям СрЗИ

Приемочные испытания СрЗИ должны проводиться в соответствии с методиками испытаний, установленными настоящим документом.

Испытания проводятся Лицензиатом в присутствии персонала Абонента, ответственного за эксплуатацию АРМ.

4.4. Работы по завершении испытаний

По завершении приемочных испытаний участниками оформляется протокол приемочных испытаний АРМ.П. После оформления протокола Абонент направляет копию протокола приемочных испытаний Оператору.

5. Условия и порядок проведения испытаний

В процессе испытания производятся проверки и оценки, предусмотренные разделом 4 настоящего документа, и выполняется анализ результатов.

Испытания производятся по методикам, изложенным в Приложениях 1-5 настоящего документа.

6. Материально-техническое обеспечение испытаний

До проведения приемочных испытаний Абонент должен выполнить технические требования, предъявляемые к пользовательским сегментам при подключении к центральному сегменту ГИС (приложение 3 к Регламенту).

Состав СрЗИ, установленных на АРМ.П, должен соответствовать составу, утвержденному в Техническом проекте на создание системы защиты информации государственной информационной системы «Единая информационная система в сфере образования Волгоградской области», и включать СрЗИ, указанные в таблице 6.1.

Таблица № 6.1

Тип АРМ	Состав, используемых СрЗИ
АРМ.П	Средство защиты информации «Secret Net Studio» с модулями НСД, МЭ, САВЗ
	Средство криптографической защиты информации «Континент TLS VPN Клиент» (версия 1.2)
	СКЗИ "Крипто Про CSP 4.0"

В ходе испытаний должны использоваться сертифицированные ФСТЭК России программные средства контроля эффективности применения СрЗИ от НСД, приведенные в таблице № 6.2.

Таблица № 6.2

№ п/п	Наименование тестирующего средства	Сертификат соответствия
1	Программа фиксации и контроля исходного состояния программного комплекса «ФИКС» версия 2.0.2	Сертификат ФСТЭК России № 1548, действителен до 15 января 2020 г.
2	Сетевой сканер безопасности XSpider 7.8.24	Сертификат ФСТЭК России № 3247, действителен до 24 октября 2020 г.

№ п/п	Наименование тестирующего средства	Сертификат соответствия
3	Программа поиска и гарантированного уничтожения информации на дисках "TERRIER" версия 3.0	Сертификат ФСТЭК России № 1193, действителен до 16 мая 2018 г.
4	Средство контроля защищенности от НСД "Ревизор 1 XP"	Сертификат ФСТЭК России № 989, действителен до 08 февраля 2020 г.
5	Средство контроля защищенности от НСД "Ревизор 2 XP"	Сертификат ФСТЭК России № 990, действителен до 08 февраля 2020 г.

7. Метрологическое обеспечение испытаний

Требования к метрологическому обеспечению испытаний АРМ.П не предъявляются.

8. Отчетность

При оформлении протокола приемочных испытаний АРМ.П должны быть отражены следующие разделы:

– назначение испытаний и номер раздела ПМИ, по которому проводится испытание;

– состав технических и программных средств, используемых при испытаниях;

– указание методик, в соответствии с которыми проводились испытания, обработка и оценка результатов;

– обобщенные результаты испытаний;

– выводы о результатах испытаний и соответствии АРМ.П требованиям технического проекта.

Форма протокола испытаний приведена в приложении 6.

Приложение 1

Методика проверки отсутствия известных уязвимостей в программном обеспечении АРМ.П

Для проверки отсутствия известных уязвимостей в программном обеспечении в ходе приемочных испытаний выполняются следующие действия:

1) проводится сканирование АРМ.П сертифицированным сетевым сканером безопасности XSpider 7.8.24 с профилями Default, Safe Scan и Web Scan;

Проверка считается пройденной успешно, если в отчетах, полученных по результатам выполненных действий, отсутствуют сведения о выявленных (не устранённых) известных уязвимостях в программном обеспечении АРМ.П.

Приложение 2

Методика проверка готовности пользователей и администраторов к эксплуатации СЗИ АРМ.П

1) При проверке готовности администраторов пользовательского сегмента проверяются знания:

- описания технологического процесса обработки информации на объекте информатизации;
- Регламента;
- Руководства администратора системы защиты информации пользовательского сегмента государственной информационной системы «Единая информационная система в сфере образования Волгоградской области» уч. №04-28/5дсп от 28.02.2018 г.;
- руководства администраторов на используемые в пользовательских сегментах СрЗИ.

2) При проверке готовности пользователей АРМ.П проверяются знания:

- описания технологического процесса обработки информации на объекте информатизации;
- Регламента;
- руководств пользователей на используемые в СЗИ АРМ.П СрЗИ.

Проверка считается пройденной успешно, если пользователи показывают знания перечисленных документов, достаточные для эксплуатации СЗИ АРМ.П.

Приложение 3

Методика проверки соответствия выполненных настроек СЗИ АРМ.П Абонента требованиям технического проекта

№ п/п	Наименование проверки	Выполняемые действия	Критерий оценки успешности прохождения проверки
1.	Проверка настройки подсистемы защиты от НСД «Secret Net Studio»		
1.1.	Проверка характеристик паролей пользователей	Производится попытка смены пароля учетной записи пользователя на пароль содержащий менее 6 символов и состоящий из: и/или одного алфавита (цифры, символы, буквы). В настройках групповой политики проверяется установка смены пароля на срок не более 120 дней	Система выдает сообщение о невозможности задания пароля с тестируемыми характеристиками. Длина пароля должна быть не менее шести символов. Алфавит пароля не менее 70 символов. Период смены паролей не более чем через 120 дней
1.2.	Проверка блокирования доступа к информационной системе, при максимальном количестве неуспешных попыток аутентификации	Производится ввод неверного пароля для доступа к АРМ.П (5 попыток).	Учетная запись блокируется после 5-й попытки, разблокировка доступна только администратору ИБ
1.3.	Проверка блокирования сеанса доступа на АРМ.П	Бездействие пользователя на АРМ.П в течение 5 минут	Сеанс автоматически блокируется после 5 минут бездействия пользователя
1.4.	Проверка сокрытия парольной информации при аутентификации пользователей	Производится ввод парольной информации в окне аутентификации	Вводимые символы пароля не отображаются
1.5.	Проверка настройки разграничения доступа к информационным ресурсам АРМ.П	Проверяются свойства безопасности информационных ресурсов АРМ.П, включая принтеры и каталоги, на соответствие правам доступа, указанным в разрешительной системе	В настройках безопасности информационных ресурсов АРМ.П должны содержаться права доступа, только допущенным пользователям в соответствии с разрешительной системой
1.6.	Проверка разделения полномочий пользователей и	Пользователь, не обладающий правами администратора производит попытку смены	Выдается сообщение о недостаточности полномочий

№ п/п	Наименование проверки	Выполняемые действия	Критерий оценки успешности прохождения проверки
	администраторов АРМ.П	настроек безопасности учетной записи пользователя.	
1.7.	Проверка регистрации событий безопасности	Осуществляются попытки входа в систему по неверному идентификатору доступа, по верному идентификатору доступа. Осуществляются попытки запуска прикладного ПО, предназначенного для обработки защищаемой информации	В журналах событий безопасности ОС и СрЗИ от НСД отображаются записи содержащие сведения о успешном/неуспешном входе. И содержат, дату, время и идентификатор пользователя. А также записи о запуске, прикладного ПО, предназначенного для обработки защищаемой информации
1.8.	Проверка настройки механизмов защиты подсистемы защиты от НСД «Secret Net Studio»	Проверяются настройки механизмов: «Защитные подсистемы»; «Устройства».	Установлены следующие значения параметров безопасности: - максимальный период неактивности до блокировки экрана - 5 минут; - количество неудачных попыток аутентификации - 5 попыток; - время блокировки – 30 мин. - максимальный срок действия пароля – 90 дней; - минимальное количество символов в пароле – 6. Вновь подключаемые устройства, не входящие в состав ИС блокируются.
2.	Проверка настройки подсистемы защиты МЭ «Secret Net Studio»		
2.1.	Проверка режима функционирования подсистемы защиты МЭ «Secret Net Studio»	Проверка осуществляется путем попытки доступа при помощи утилиты «telnet» к информационным ресурсам АРМ.П. Дополнительно проводится проверка программным средством «Сетевой сканер безопасности XSpider 7.8.24» с профилем Default.	Доступ к информационным ресурсам для всех входящих подключений отсутствует.
2.2.	Проверка регистрации событий удаленного доступа	Осуществляется попытка доступа из ЛВС к информационным ресурсам АРМ.П с автоматизированного рабочего места, не входящего	В журнале событий безопасности средства межсетевого экранирования отражается информация о попытках санкционированного /

№ п/п	Наименование проверки	Выполняемые действия	Критерий оценки успешности прохождения проверки
		в состав информационной системы.	несанкционированного доступа
3.	Проверка подсистемы антивирусной защиты САВЗ «Secret Net Studio»		
3.1.	Проверка запрета на отключение компонентов защиты пользователями, не обладающими ролью администратора	Пользователь, не обладающий правами администратора, делает попытку отключения компонентов защиты антивирусного ПО.	Система устанавливает запрет на изменение настроек безопасности из учетной записи пользователя
3.2.	Проверка автоматического обновления с доверенного источника сети управления и передачи данных Волгоградской области	Просмотр даты обновления базы данных вирусных сигнатур	Интервал между обновлениями базы данных вирусных сигнатур не превышает 1 день
4.	Проверка подсистем обеспечения безопасных сетевых соединений		
4.1.	Проверка режима функционирования СКЗИ «Континент TLS VPN Клиент» (версия 1.2)	Проверка осуществляется установки соединения к веб-ресурсу tls.volganet.ru:4445 по каналу связи общих сетей передачи данных	Соединение установлено

Приложение 4

Методика проверки полноты и качества разработанной организационно-распорядительной документации по защите информации пользовательских сегментов ГИС требованиям технического проекта

№ п/п	Наименование проверки	Выполняемые действия	Критерий оценки успешности прохождения проверки
1.	Проверка наличия документа, содержащего правила и процедуры идентификации и аутентификации пользователей	Проверить наличие утвержденного документа	Документ имеется в наличии
2.	Проверка наличия документа, содержащего правила и процедуры идентификации и аутентификации устройств	Проверить наличие утвержденного документа	Документ имеется в наличии
3.	Проверка наличия документа, содержащего правила и процедуры управления идентификаторами	Проверить наличие утвержденного документа	Документ имеется в наличии
4.	Проверка наличия документа, содержащего правила и процедуры управления средствами аутентификации	Проверить наличие утвержденного документа	Документ имеется в наличии
5.	Проверка наличия документа, содержащего правила и процедуры управления учетными записями пользователей	Проверить наличие утвержденного документа	Документ имеется в наличии
6.	Проверка наличия документа, содержащего разрешительную систему допуска	Проверить наличие утвержденного документа	Документ имеется в наличии
7.	Проверка наличия документа, содержащего правила и процедуры управления информационными потоками	Проверить наличие утвержденного документа	Документ имеется в наличии
8.	Проверка наличия документа, содержащего ограничение количества неуспешных попыток входа в информационную систему	Проверить наличие утвержденного документа	Документ имеется в наличии
9.	Проверка наличия документа, определяющего время блокировки сеанса в случае бездействия пользователя	Проверить наличие утвержденного документа	Документ имеется в наличии
10.	Проверка наличия документа, содержащего разрешенное к использованию программное обеспечение	Проверить наличие утвержденного документа	Документ имеется в наличии
11.	Проверка наличия документа, содержащего правила и процедуры применения удаленного доступа	Проверить наличие утвержденного документа	Документ имеется в наличии
12.	Проверка наличия документа, содержащего правила и процедуры обеспечения доверенной загрузки средств вычислительной техники	Проверить наличие утвержденного документа	Документ имеется в наличии

№ п/п	Наименование проверки	Выполняемые действия	Критерий оценки успешности прохождения проверки
13.	Проверка наличия документа, содержащего правила и процедуры управления установкой (инсталляцией) компонентов программного обеспечения (в том числе управления составом и конфигурацией подлежащих установке компонентов программного обеспечения, параметрами установки, параметрами настройки компонентов программного обеспечения)	Проверить наличие утвержденного документа	Документ имеется в наличии
14.	Проверка наличия документа, содержащего правила контроля за установкой только разрешенного к использованию программного обеспечения и (или) его компонентов	Проверить наличие утвержденного документа	Документ имеется в наличии
15.	Проверка наличия документа, содержащего состав и содержание информации о событиях безопасности, подлежащих регистрации	Проверить наличие утвержденного документа	Документ имеется в наличии
16.	Проверка наличия документа, содержащего правила и процедуры сбора, записи и хранения информации о событиях безопасности	Проверить наличие утвержденного документа	Документ имеется в наличии
17.	Проверка наличия документа, содержащего правила и процедуры обновления и управления подсистемой антивирусной защиты	Проверить наличие утвержденного документа	Документ имеется в наличии
18.	Проверка наличия документа, содержащего правила и процедуры контроля целостности программного обеспечения	Проверить наличие утвержденного документа	Документ имеется в наличии
19.	Проверка наличия документа, содержащего правила и процедуры обновления программного обеспечения	Проверить наличие утвержденного документа	Документ имеется в наличии
20.	Проверка наличия документа, содержащего периодичность контроля работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации	Проверить наличие утвержденного документа	Документ имеется в наличии
21.	Проверка наличия документа, содержащего периодичность контроля состава технических средств, программного обеспечения и средств защиты информации	Проверить наличие утвержденного документа	Документ имеется в наличии
22.	Проверка наличия документа, содержащего периодичность контроля правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в ГИС	Проверить наличие утвержденного документа	Документ имеется в наличии
23.	Проверка наличия документа, содержащего правила и процедуры восстановления (в том числе планы по действиям персонала порядок применения компенсирующих мер)	Проверить наличие утвержденного документа	Документ имеется в наличии

№ п/п	Наименование проверки	Выполняемые действия	Критерий оценки успешности прохождения проверки
24.	Проверка наличия документа, определяющего границу контролируемой зоны	Проверить наличие утвержденного документа	Документ имеется в наличии
25.	Проверка наличия документа, содержащего правила и процедуры контроля и управления физическим доступом	Проверить наличие утвержденного документа	Документ имеется в наличии
26.	Проверка наличия документа, содержащего правила и процедуры защиты периметра информационной системы	Проверить наличие утвержденного документа	Документ имеется в наличии
27.	Проверка наличия документа, содержащего правила защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи	Проверить наличие утвержденного документа	Документ имеется в наличии
Дополнительная организационно-распорядительная документация, относящаяся только к пользовательским сегментам с клиент-серверным режимом взаимодействия с центральным сегментом ГИС (АРМ.П)			
28.	Проверка наличия документа, содержащего правила и процедуры контроля использования интерфейсов ввода (вывода)	Проверить наличие утвержденного документа	Документ имеется в наличии
29.	Проверка наличия журнала учета машинных носителей	Проверить наличие утвержденного документа	Документ имеется в наличии
30.	Проверка наличия документа, содержащего процедуры уничтожения (стирания) информации на машинных носителях	Проверить наличие утвержденного документа	Документ имеется в наличии
31.	Проверка наличия документа, содержащего правила и процедуры выявления, анализа и устранения уязвимостей	Проверить наличие утвержденного документа	Документ имеется в наличии
32.	Проверка наличия документа, содержащего правила и процедуры обнаружения и реагирования на поступление незапрашиваемой информации	Проверить наличие утвержденного документа	Документ имеется в наличии
33.	Проверка наличия документа, содержащего правила и процедуры резервного копирования информации	Проверить наличие утвержденного документа	Документ имеется в наличии
34.	Проверка наличия документа, содержащего правила и процедуры управления запуском программного обеспечения (в том числе списки программного обеспечения, ограничения запуска, параметры запуска компонентов программного обеспечения)	Проверить наличие утвержденного документа	Документ имеется в наличии

Приложение 5

Методика проверки соответствия АРМ.П требованиям Регламента

№ п/п	Наименование проверки	Критерий оценки успешности прохождения проверки
1.	**Проверка технических требований к пользовательским сегментам при подключении к центральному сегменту ГИС**	
1.1	Проверяется количество установленных ОС	На АРМ установлена одна ОС
1.2	Проверяется отсутствие в составе СВТ беспроводных клавиатур и беспроводных манипуляторов типа «мышь». Модули беспроводной связи СВТ должны быть деактивированы (отключены)	Беспроводные устройства не используются. Модули беспроводной связи отсутствуют или отключены.
1.3	Проверяется актуальность ОС	ОС официально поддерживается производителем (в т.ч. путем выпуска обновлений и исправлений уязвимостей)
1.4	Проверяется совместимость ОС со СрЗИ	ОС включена в перечень поддерживаемых операционных систем формуляров средств защиты информации
1.6	Проверяется файловая система	Используется файловая система NTFS
1.7	Проверяется правильность эксплуатации СрЗИ	СрЗИ установлены и настроены в соответствии с требованиями эксплуатационной документацией. На все установленные СрЗИ имеются акты установки
1.8	Проверяется актуальность сертификатов на установленные СКЗИ	Средство криптографической защиты информации «КриптоПро CSP» имеет действующий сертификат ФСБ Средство криптографической защиты информации «Континент TLS VPN Клиент» версия 1.2 имеет действующий сертификат ФСБ
1.9	Проверяется сертификат на установленное средство антивирусной защиты	Средства антивирусной защиты информации сертифицированы на соответствие требованиям руководящего документа «Требования к средствам антивирусной защиты» (ФСТЭК России, 2012) – не ниже 4 класса защиты
1.12	Проверяется класс защищенности СрЗИ от НСД	СрЗИ от НСД сертифицированы на соответствие требованиям руководящего документа «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) - не ниже 5 класса защищенности
1.14	Проверяется класс защиты средства межсетевого экранирования	Подключение к сетям передачи данных (локальным вычислительным сетям) осуществляется с использованием средства межсетевого

№ п/п	Наименование проверки	Критерий оценки успешности прохождения проверки
		экранирования, сертифицированного на соответствие требованиям руководящего документа «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1997) не ниже 3 класса защиты
1.15	Используемые СрЗИ проверяются на наличие недекларируемых возможностей	СрЗИ имеют сертификаты соответствия требованиям руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) – не ниже 4 уровня контроля
2.	**Проверка общих требований к составу организационных и технических мер по защите информации при подключении к центральному сегменту ГИС**	
2.1	Проверяется назначение ответственных лиц при эксплуатации пользовательского сегмента ГИС	Абонентом назначены: лицо, ответственное за обеспечение эксплуатации пользовательского сегмента ГИС; администратор ИБ, на которого возлагаются задачи организации работ по использованию применяемых средств защиты информации, инструктажа пользователей, контролю за соблюдением в пользовательских сегментах требований информационной безопасности, а также взаимодействию с администратором ИБ ГИС; пользователи, допущенные к работе в пользовательских сегментах ГИС; администраторы (технические специалисты), допущенные для обслуживания аппаратного и программного обеспечения пользовательских сегментов ГИС
2.2	Проверяется разделение функций (ролей) по обработке информации, администрированию системы защиты информации и обеспечению функционирования СВТ пользовательского сегмента ГИС	Выполнение функций (ролей) по обработке информации, администрированию системы защиты информации и обеспечению функционирования СВТ пользовательского сегмента ГИС возлагается на отдельные должностные лица
2.3	Проверяются права и привилегии по настройке СрЗИ	Права и привилегии по доступу к параметрам настройки средств защиты информации предоставляются исключительно администратору ИБ пользовательского сегмента ГИС

№ п/п	Наименование проверки	Критерий оценки успешности прохождения проверки
3.	**Проверка требований к защите информации при передаче по каналам связи**	
3.1	Проверяется используемые СКЗИ	Для обеспечения защиты конфиденциальной информации при передаче по каналам связи применяться сертифицированное СКЗИ класса КС1 и выше
3.2	Проверяется носители криптографических ключей	Для хранения криптографических ключей пользователи АРМ используют отчуждаемые (съемные) носители в защищенном исполнении, совместимые с применяемыми СКЗИ
3.3	Проверяется правильность ведения учета СКЗИ	Используемое СКЗИ, эксплуатационная и техническая документация к ним, ключевые носители подлежат поэкземплярному учету
4.	**Проверка требований к межсетевому взаимодействию**	
4.1	Проверяется технология подключения к сетям общего пользования	Пользовательские сегменты ГИС имеют подключения к сетям общего пользования. Информационное взаимодействие пользовательских сегментов АРМ.П с ресурсами сетей международного информационного обмена (в том числе, Интернет) осуществляется.
4.2	Проверяется возможность доступа к папкам (файлам) АРМ.П	Сетевой доступ к папкам (файлам) АРМ.П отсутствует
4.3	Проверяется возможность удаленного доступа к ресурсам АРМ.П (включая средства удаленного администрирования)	Удаленный доступ к АРМ ограничен подсистемой межсетевого экранирования СЗИ
4.4	Проверяется способ подключения средств печати документов, применяемые на АРМ.П	Средства печати документов, применяемые на АРМ.П подключаются непосредственно к АРМ (локально, не являются сетевыми) и сетевой доступ к ним исключен (не предоставляется)
5.	**Проверка требований к оборудованию Помещений**	
5.1	Проверяется реализация организационно-режимных мер, обеспечивающих контролируемое пребывание лиц в Помещениях и доступа к техническим средствам АРМ	Реализованы и поддерживаться организационно – режимные меры, обеспечивающие возможность пребывания и/или непосредственного доступа к техническим средствам только уполномоченных лиц или в сопровождении уполномоченных лиц Абонента
5.2	Проверка наличия замков на входных дверях Помещений	Входные двери Помещений оснащены замками
5.3	Проверка обеспечения закрытия Помещений на замок и их открытия только для санкционированного прохода, а также их опечатывания и постановку на охрану с использованием технических средств в нерабочее время	Обеспечено постоянное закрытие дверей Помещений на замок и их открытия только для санкционированного прохода, а также опечатывание Помещений по окончании рабочего дня или оборудование Помещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии Помещений

№ п/п	Наименование проверки	Критерий оценки успешности прохождения проверки
5.4	Проверка наличия документа, определяющего порядок сдачи Помещений под охрану и их вскрытия	Утвержден внутренний нормативный акт, определяющий правила доступа в Помещения в рабочее и нерабочее время, порядок сдачи Помещений под охрану и их вскрытия, в том числе в нештатных ситуациях, а также порядок действий в случае выявления случаев несанкционированного доступа в Помещения
5.5	Проверка организации сдачи ключей и Помещений под охрану, а также вскрытия Помещений	Осуществляется сдача ключей и Помещений под охрану, а также получение ключей и вскрытие Помещений производится лицами, работающими в этих Помещениях, по утвержденному руководством Абонента списку
5.6	Проверка наличия металлических решеток, ставней или охранной сигнализации на окнах Помещений первых и последних этажей	Окна Помещений, расположенных на первых или последних этажах, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в Помещения посторонних лиц, оборудованы металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению
5.7	Проверка обеспечения сохранности документов и ключевых носителей, отсутствия просмотра экранов мониторов АРМ посетителями.	Внутренняя планировка, оборудование и расположение рабочих мест в Помещениях обеспечивает пользователям сохранность доверенных им документов и сведений, содержащих конфиденциальную информацию, в том числе невозможность просмотра экранов мониторов посетителями, возможность безопасного хранения ключевых носителей и носителей конфиденциальной информации.
5.8	Проверка обеспечения хранения ключевых носителей в индивидуальных хранилищах с возможностью опечатывания личной печатью пользователя.	Для хранения ключевых носителей применяются индивидуальные хранилища (сейфы, металлические шкафы, пеналы и т.п.) с возможностью опечатывания личной печатью пользователя
5.9	Проверяются способы хранения съемных машинных носителей конфиденциальной информации	Хранение съемных машинных носителей конфиденциальной информации осуществляется в сейфах (металлических шкафах), оборудованных внутренними замками с двумя или более дубликатами ключей и приспособлениями для опечатывания замочных скважин или кодовыми замками
5.10	Проверяется наличие документа регламентирующего порядок доступа представителям коммерческих организаций к техническим средствам пользовательских сегментов ГИС для проведения их обслуживания и иных работ	Документ имеется в наличии. Документом предусмотрено предоставление доступа к техническим средствам пользовательских сегментов ГИС только после подписания представителем организации обязательства о неразглашении сведений конфиденциального характера

№ п/п	Наименование проверки	Критерий оценки успешности прохождения проверки
6.	**Проверка требований к защите от несанкционированного доступа**	
6.1	Проверка наличия у каждого пользователя АРМ индивидуального идентификатора (учетной записи).	С целью соблюдения принципа персональной ответственности за свои действия каждому пользователю, допущенному к работе в пользовательском сегменте ГИС, сопоставлено персональное уникальное имя (учетная запись пользователя).
6.2	Проверка способа аутентификации пользователей	Реализована двухфакторная аутентификация для доступа в систему для пользователей и администраторов с использованием аппаратных отчуждаемых идентификаторов (ключевых носителей)
6.3	Проверка блокировки учетных записей на АРМ после неудачных попыток ввода пароля.	Осуществляется блокировка учетных записей пользователей при 5 неудачных попытках регистрации (попыток входа) с возможностью автоматического разблокирования через 15 минут.
6.4	Проверяется возможность блокировки сеанса доступа к операционной системе при бездействии пользователя	Осуществляется блокировка сеанса доступа к операционной системе на АРМ после бездействия пользователя в течение 5 минут
6.5	Проверяется настройка отображения сведений пользователя при блокировке сеанса доступа	Сведения о пользователе не отображаться при блокировке сеанса доступа
6.6	Проверяется настройка отображения имени последнего входа пользователя	В диалоговом окне входа в операционную систему АРМ не отображается имя последнего пользователя, выполнившего вход
6.7	Проверяется настройка повторного использования идентификатора	Исключено повторное использование идентификатора пользователя (имени учетной записи) в течение трех лет
6.8	Проверка установленной минимальной длины пароля для входа в систему	Установленная минимальная длина пароля – 6 символов.
6.9	Проверка выполнения требований к сложности пароля	В «Локальных политиках безопасности» включен параметр «Пароль должен отвечать требованиям сложности»
6.10	Проверка выполнения требования к неповторяемости пароля	Организационно-распорядительной документацией Абонента определено, что при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4-х позициях
6.11	Проверка выполнения требования к максимальному сроку действия пароля	Периодичность смены пароля не превышает 120 дней
6.12	Проверка блокировки неактивных учетных записей	Осуществляется блокировка неактивных (неиспользуемых) учетных записей пользователей после периода времени неиспользования 90 дней
6.13	Проверка невозможности сохранения реквизитов доступа	Исключена возможность сохранения реквизитов доступа пользователей средствами операционной

№ п/п	Наименование проверки	Критерий оценки успешности прохождения проверки
		системы или используемого для доступа к АРМ.П программного обеспечения (функция запоминания паролей)
6.14	Проверка аварийного дампа оперативной памяти	Исключена возможность создания аварийного дампа оперативной памяти операционных систем
6.15	Проверка разграничения прав на доступ к системным файлам и папкам	На все папки, содержащие системные файлы операционной системы Windows и программного обеспечения СКЗИ «КриптоПро CSP» (по умолчанию «c:\Program Files\Crypto Pro\CSP\»), установлены права доступа, запрещающие запись всем пользователям, кроме Администратора (Administrator), Создателя/Владельца (Creator/Owner) и Системы (System)
6.16	Проверка способа обновления операционной системы	Обеспечена невозможность модификации операционной системы Windows через общедоступные каналы передачи данных (Windows Update, Remote Assistance, и т.п.)
6.17	Проверяется учетные записи, созданные в операционной системе по умолчанию	Пользователь Administrator переименован
6.18	Проверка учетных записей, созданных в операционной системе по умолчанию. Проверка способа входа в операционную систему	Учетная запись для гостевого входа (Guest) заблокирована
6.19		Исключено использование режима автоматического входа пользователя в операционную систему при ее загрузке
6.20	Проверка неиспользуемых ресурсов СВТ	Все неиспользуемые ресурсы СВТ (протоколы, сервисы, службы и т.п.) отключены (удалены)
6.21	Проверка невозможности беспроводного доступа к СВТ	Исключена возможность беспроводного доступа к СВТ пользовательского сегмента ГИС
6.22	Проверка возможности использования незарегистрированных (неучтенных) съемных машинных носителей информации (в том числе находящихся в личном пользовании) на АРМ.П	Возможность использования незарегистрированных (неучтенных) съемных машинных носителей информации (в том числе находящихся в личном пользовании) исключена с использованием СрЗИ от НСД
6.23	Проверка регистрации и учета машинных носителей информации	Применяемые на АРМ носители информации маркируются и учитываются в журнале учета машинных носителей
6.24	Проверка оборудования технических средств АРМ средствами контроля за вскрытием	Технические средства АРМ оборудованы средствами контроля за вскрытием
7.	**Проверка требований к обеспечению целостности среды функционирования.**	

№ п/п	Наименование проверки	Критерий оценки успешности прохождения проверки
7.1	Проверяется наличие утвержденного нормативного акта о порядке внесения изменений в состав и конфигурацию программного обеспечения, средств защиты информации и технических средств пользовательских сегментов, контроля неизменности используемых программных и технических средств, а также определяющий перечень лиц, имеющих право на внесение изменений и учитывающих необходимость согласования вносимых изменений с Оператором	Документ имеется в наличии
7.3	Проверка наличия дистрибутивов СКЗИ	Дистрибутивы СКЗИ имеются в наличии и получены от организаций, действующих на основании лицензии ФСБ на право распространения СКЗИ
7.4	Проверка наличия дистрибутивов СрЗИ	Дистрибутивы установленных на АРМ СрЗИ имеются в наличии
7.5	Проверка обеспечения контроля целостности	Контроль целостности обеспечивается СрЗИ при загрузке операционной системы
7.6	Проверка отсутствия средств разработки программного обеспечения и отладчики	Средства разработки программного обеспечения и отладчики отсутствуют
7.7	Проверка правильности хранения дистрибутивов СрЗИ	Обеспечивается защищенное хранение дистрибутивов программных средств, в том числе средств защиты информации, и документации на данные средства
7.8	Проверка разграничения прав доступа на установку и настройку СрЗИ	Права на установку и настройку СрЗИ имеет только администратор
7.9	Проверка наличия технического паспорта АРМ	Документ имеется в наличии
7.10	Проверяется организация резервного копирования	Резервное копирование конфиденциальной информации осуществляется, в соответствии с утвержденным Абонентом регламентом резервного копирования
8.	**Проверка требований к регистрации событий**	
8.1	Проверка регистрации событий входа пользователя в систему, либо загрузки операционной системы и её останова	Регистрируются события входа (выхода) пользователя (администратора) в систему (из системы) либо загрузки и инициализации операционной системы и ее программного останова
8.2	Проверка регистрации событий изменения конфигурации	Регистрируются события изменения конфигурации параметров безопасности и учетных записей

№ п/п	Наименование проверки	Критерий оценки успешности прохождения проверки
	параметров безопасности и учетных записей	пользователей
8.3	Проверка регистрации параметров событий безопасности (дата, время, идентификаторы субъектов и объектов доступа, тип и результат события)	Регистрируются следующие параметры: - дата и время события - идентификаторы субъектов и объектов доступа - тип события - результат события
9.	**Проверка требований к обеспечению отказоустойчивости**	
9.1	Проверка наличия в помещениях средств пожарной сигнализации	Помещения оборудованы средствами пожарной сигнализации
9.2	Проверка наличия средств бесперебойного питания в составе СВТ	СВТ АРМ подключаются к сети электропитания через источники бесперебойного питания
9.3	Проверка наличия документа, определяющего порядок действий при возникновении нештатных ситуаций, условия выполнения каждого действия (перечень событий, при наступлении которых необходимо совершить определенное действие и т.п.)	Документ имеется в наличии
10.	**Проверка требований к организации контроля состояния защиты информации.**	
10.1	Проверка наличия документа, регламентирующего порядок и периодичность проведения контроля состояния защиты информации пользовательского сегмента ГИС	Документ имеется в наличии

Приложение 6

Типовая форма протокола проведения приемочных испытаний автоматизированного рабочего места, предназначенного для подключения к «Автоматизированной системе обработки конфиденциальной информации Волгоградской области»

УТВЕРЖДАЮ

Руководитель Абонента

_____ _._._____

«___» _____ 2018 г.

УТВЕРЖДАЮ

Руководитель Лицензиата

_____ _._._____

«___» _____ 2018 г.

Автоматизированное рабочее место, предназначенное для подключения к государственной информационной системе «Единая информационная система в сфере образования Волгоградской области»

Наименование Абонента

Протокол проведения приемочных испытаний

Листов __

2018

Изм.	Лист.	№ документа	Подп.	Дата.		Лист 25

Инв № подл. | Подп. и дата | Взамен инв. | Инв № дубл. | Подп. и дата

АННОТАЦИЯ

Настоящий протокол составлен по результатам приемочных испытаний автоматизированного рабочего места *Абонента* (далее - АРМ), предназначенного для подключения к государственной информационной системе «Единая информационная система в сфере образования Волгоградской области» *через веб-сервис*, выполненных в соответствии с «Программой и методикой приемочных испытаний пользовательских сегментов государственной информационной системы «Единая информационная система в сфере образования Волгоградской области» от __._.2018 уч. № ____ (далее по тексту «ПМИ»).

СОДЕРЖАНИЕ

1. Общие положения

Объект испытаний:

Автоматизированное рабочее место, предназначенное для подключения к к государственной информационной системе «Единая информационная система в сфере образования Волгоградской области» (далее – АРМ).

Тип АРМ: *АРМ.П.*

Место испытаний:

- *адрес*

Дата и время испытаний:

- *дата и время начала испытаний*
- *дата и время окончания испытаний*

Состав комиссии по проведению испытаний

Члены комиссии		
_._._____	*должность*	*организация*
_._._____	*должность*	*организация*
_._._____	*должность*	*организация*
_._._____	*должность*	*организация*
_._._____	*должность*	*организация*
_._._____	*должность*	*организация*

2. Результаты испытаний

2.1. Проверка отсутствия известных уязвимостей в программном обеспечении АРМ.П

№ п/п	Используемое средство анализа	Наименование профиля проверки	Результат анализа
1.	Сетевой сканер безопасности XSpider 7.8.24	Default	Содержится в Приложении 1 к настоящему документу
		Safe Scan	
		Web Scan	

2.2. Проверка готовности пользователей и администраторов к эксплуатации СЗИ

№ п\п	Проверка	Результат
1.	**Проверка готовности администраторов к эксплуатации СЗИ**	
1.1		
1.2		
…		
2.	**Проверка готовности администраторов к эксплуатации СЗИ**	
2.1		
2.2		

2.3. Проверка соответствия выполненных настроек системы защиты информации АРМ требованиям технического проекта.

№ п/п	Наименование проверки	Результат
1.	Проверка настройки подсистемы защиты от НСД	
1.1		
1.2		
…		
2.	Проверка подсистемы межсетевого экранирования	
2.1.		
2.2.		
…		
3.	Проверка подсистемы обнаружения вторжений	
3.1.		
3.2.		
…		
4.	Проверка подсистемы антивирусной защиты	

№ п/п	Наименование проверки	Результат
4.1.		
4.2.		
…		

2.4. Проверка полноты и качества разработанной организационно-распорядительной документации по защите информации АРМ

№ п/п	Проверка	Предоставленный документ
1.		*Наименование документа от __.__.201_ г (уч. № ____)*
2.		*Наименование документа от __.__.201_ г (уч. № ____)*
…		*Наименование документа от __.__.201_ г (уч. № ____)*

2.5. Проверка соответствия АРМ.П требованиям Регламента подключения к к государственной информационной системе «Единая информационная система в сфере образования Волгоградской области», утвержденного приказом комитета информационных технологий Волгоградской области № 8 от 05.03.2018 г.

№ п/п	Наименование проверки	Результат
1.		
2.		
….		

3. Сведения об отказах, сбоях и аварийных ситуациях

Отказов, сбоев и аварийных ситуаций в процессе испытаний АРМ.П не наблюдалось.

4. Сведения о корректировках параметров объекта испытаний и технической документации

Корректировок параметров объекта испытаний и технической документации в процессе испытаний не проводилось.

5. Заключение комиссии

Результаты испытаний:

В ходе проведения приемочных испытаний АРМ, была обеспечена проверка выполнения ее функций во всех режимах функционирования, установленных в ПМИ.

Комиссия пришла к выводу о:

- *отсутствии известных уязвимостей в программном обеспечении АРМ;*
- *готовности пользователей и администраторов к эксплуатации АРМ;*
- *соответствии выполненных настроек системы защиты АРМ требованиям технического проекта;*
- *соответствии полноты и качества разработанной организационно-распорядительной документации по защите информации на АРМ;*
- *соответствии АРМ требованиям Регламента подключения к государственной информационной системе «Единая информационная система в сфере образования Волгоградской области», утвержденного приказом комитета информационных технологий Волгоградской области № 8 от 05.03.2018 г.*

Выводы:

По результатам проведения приемочных испытаний может быть составлен акт о готовности АРМ к подключению к государственной информационной системе «Единая информационная система в сфере образования Волгоградской области» и готовности приемки в постоянную эксплуатацию.

6. Замечания и рекомендации по результатам приемочных испытаний

Замечания по организации и реализации требований по защите информации отсутствуют.

7. Подписи членов комиссии по проведению приемочных испытаний

Члены комиссии:

От Абонента _·_· _____

_·_· _____

От *Лицензиата* _·_· _____

_·_· _____

Инв № подл.	Подп. и дата	Взамен инв.	Инв № дубл.	Подп. и дата

Изм.	Лист.	№ документа	Подп.	Дата.		Лист
						32

Лист регистрации изменений

Номера листов (страниц)					Всего листов (страниц) в докум.	№ докумен-та	Входящий № сопрово-дительного докум. и дата	Подп.	Дата
Изм.	измененных	Заменен-ных	новых	аннули-рованных					