УТВЕРЖДАЮ
Директор ОГКУ
«Центр по
сопровождению закупок»
_____А.С.Ахметшин
01.03 2024 г.

Программа и методика приемочных испытаний внешних сегментов государственной информационной системы «АЦК-Госзаказ»

Содержание

Список сокращений

Абонент	– организация – владелец внешнего сегмента, в отношении которого проводятся приемочные испытания
АРМ	– автоматизированное рабочее место
БД	– база данных
ГИС	– государственная информационная система
ЗСПД	– защищенная сеть передачи данных
ИБ	– информационная безопасность
КВ	– компьютерный вирус
КЗ	– контролируемая зона
МЭ	– межсетевой экран
НСД	– несанкционированный доступ
ОС	– операционная система
ПДн	– персональные данные
ПМВ	– программно-математические воздействия
ПО	– программное обеспечение
ПЭМИН	– побочные электромагнитные излучения и наводки
РД	– руководящий документ
СрЗИ	– средство защиты информации
СЗИ	– система защиты информации
СКЗИ	– средство криптографической защиты информации
ЭВМ	– электронно-вычислительная машина

1. Объект испытаний

Объектом приемочных испытаний является сегмент Абонента, включая его технические средства, программное обеспечение, СЗИ, предназначенный для подключения в качестве внешнего сегмента к ГИС «АЦК-Госзаказ».

СЗИ сегмента Абонента должна быть реализована в соответствии с «Системой защиты информации, обрабатываемой в государственной информационной системе автоматизации процесса управления государственными закупками Ульяновской области «АЦК-Госзаказ» и включать следующие функциональные подсистемы:

- Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)
- Управление доступом субъектов доступа к объектам доступа (УПД)
- Ограничение программной среды (ОПС)
- Защита машинных носителей информации (ЗНИ)
- Регистрация событий безопасности (РСБ)
- Антивирусная защита (АВЗ)
- Контроль (анализ) защищенности информации (АНЗ)
- Обеспечение целостности информационной системы и информации (ОЦЛ)
- Обеспечение доступности информации (ОДТ)
- Защита технических средств (ЗТС)
- Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)
- Выявление инцидентов и реагирование на них (ИНЦ)

2. Цель испытаний

Целью приемочных испытаний является определение возможности подключения сегмента Абонента к ГИС «АЦК-Госзаказ» путем распространения на него действия аттестата соответствия государственной информационной системы автоматизации процесса управления государственными закупками Ульяновской области «АЦК-Госзаказ» требованиям безопасности информации. Для проведения испытаний необходимо выполнение следующих мероприятий:

- проверка соответствия СЗИ сегмента проектным решениям, используемым в аттестованных внешних сегментах ГИС;

- проверка работоспособности СрЗИ, установленных в сегменте Абонента.

3. Общие положения

3.1. Документы, на основании которых проводят испытания

Основанием для проведения испытаний являются:

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

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

- приказ ФСТЭК от 11 февраля 2013 г. N.17 «Об утверждении Требований о Защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
- ГОСТ 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения;
- 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»;
- «Система защиты информации, обрабатываемой в государственной информационной системе автоматизации процесса управления государственными закупками Ульяновской области «АЦК-Госзаказ»

3.2 Место проведения испытаний

Испытания проводятся по адресу размещения сегмента Абонента.

3.3 Организации, участвующие в испытаниях

В проведении испытаний участвует Абонент и Лицензиат (при условии привлечения Абонентом).

3.4 Испытания, проведенные ранее

Настоящий документ определяет первичный порядок проведения испытаний сегмента Абонента, в отношении которого ранее испытания не проводились.

3.5 Документы, предъявляемые на испытаниях

На испытаниях предоставляются:

a. акт классификации сегмента АРМ;

b. актуальные угрозы безопасности информации в сегменте Абонента;

c. документация на СрЗИ, развернутые в сегменте Абонента;

d. организационно-распорядительная документация по защите информации на сегмент Абонента.

4. Объем испытаний

4.1. Этапы испытаний

Приемочные испытания проводятся в 2 этапа:

1) В ходе первого этапа испытаний осуществляются следующие мероприятия:

a. проверка классификации сегмента и оценка актуальных угроз безопасности информации сегмента (Приложение 1);

b. проверка отсутствия известных уязвимостей в сегменте или применение дополнительных (компенсирующих) мер, препятствующих эксплуатации уязвимостей нарушителями (Приложение 2);

c. проверка готовности пользователей и администраторов к эксплуатации СЗИ сегмента (Приложение 3);

d. проверка выполненных настроек СрЗИ сегмента (Приложение 4);

e. проверка полноты и качества разработанной организационно-распорядительной документации по защите информации (Приложение 5);

f. проверка соответствия системы защиты информации сегмента аттестованному ранее сегменту информационной системы (Приложение 6).

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, совместно с представителями привлечённого Лицензиата или без них 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 методика-

ми испытаний, установленными настоящим документом.
Испытания проводятся или Лицензиатом (в случае привлечения Лицензиата) в присутствии персонала Абонента, ответственного за эксплуатацию технических средств сегмента или персоналом Абонента, ответственного за эксплуатацию технических средств сегмента.

4.4. Работы по завершении испытаний

По завершении приемочных испытаний участниками оформляется протокол приемочных испытаний сегмента Абонента. После оформления протокола Абонент направляет копию протокола приемочных испытаний Оператору.

5. Условия и порядок проведения испытаний

В процессе испытания производятся проверка и оценка, 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 сегментам при подключении к ГИС.
Состав СрЗИ, установленных в сегменте, должен соответствовать составу, указанному в таблице 1.1, 1.2 и 1.3 («Внешний пользователь (вариант подключения №1)») или в таблице 2.1 («Внешний пользователь (вариант подключения №2)»).

Таблица 1.1

Состав средств защиты информации
АРМ администратора безопасности
сегмента «Внешний пользователь (вариант подключения №1)»
ГИС «АЦК-Госзаказ»

№ п/п	СрЗИ	Место установки
1.	Программное изделие Dr. Web Enterprise Security Suite	АРМ администратора безопасности
2.	Средство защиты информации Secret Net Studio	
3.	Программный комплекс САЗ XSpider	

Таблица 1.2

Состав средств защиты информации

АРМ пользователя

сегмента «Внешний пользователь (вариант подключения №1)»

ГИС «АЦК-Госзаказ»

№ п/п	СрЗИ	Место установки
1.	Программное изделие Dr. Web Enterprise Security Suite	АРМ пользователя
2.	Средство защиты информации Secret Net Studio	
3.	Программный комплекс САЗ RedCheck	

Таблица 1.3

Состав программно-аппаратных средств защиты информации

сегмента «Внешний пользователь (вариант подключения №1)»

ГИС «АЦК-Госзаказ»

№ п/п	СрЗИ и СКЗИ	Место установки	Сведения о сертификате
1.	Средство криптографической защиты информации и МЭ ПАК ViPNet Coordinator HW1000	Место расположения сегмента Абонента	Сертификат ФСТЭК России № 3692, выдан 26.01.2017, действителен до 26.01.2025

Таблица 2.1

Состав средств защиты информации

сегмента «Внешний пользователь (вариант подключения №2)»

№ п/п	СрЗИ	Место установки
1.	Программный комплекс САЗ RedCheck	АРМ пользователя
2.	Программное изделие Secret Net Studio. Модуль: Антивирус по технологии Касперского	
3.	Средство защиты информации Secret Net Studio	
4.	Программный комплекс VipNet Client 4 (версия 4.5)	

В ходе испытаний должны использоваться сертифицированные ФСТЭК России программные средства контроля эффективности применения СрЗИ от НСД, приведенные в таблице 3.

Таблица 3

№ п/п	Наименование тестирующего средства	Сертификат соответствия
1.	Сетевой сканер безопасности RedCheck	Сертификат ФСТЭК России № 3172 выдан 23.06.2014, действителен до 23.06.2025 г.
2.	Сетевой сканер безопасности XSpider	Сертификат ФСТЭК России № 3247 выдан 24.10.2014, действителен до 24.10.2025 г.

7. Отчетность

При оформлении протокола приемочных испытаний сегмента должны быть отражены следующие разделы:

–назначение испытаний и номер раздела ПиМ, 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 сегмента, сегменту информационной системы, в отношении которого были проведены аттестационные испытания.

Форма протокола испытаний приведена в приложении 7.

Приложение 1

Методика проверки классификации сегмента и оценки актуальных угроз безопасности информации сегмента

Уровень защищенности персональных данных сегмента Абонента должен соответствовать 4 (четвертому) уровню защищенности персональных данных УЗ4 или выше.

Класс защищенности сегмента Абонента должен соответствовать 3 (третьему) уровню защищенности - К3 или выше.

Перечень актуальных угроз безопасности информации сегмента Абонента не должен выходить за рамки перечня актуальных угроз безопасности информации ГИС «АЦК-Госзаказ»:

УБИ.003	Угроза анализа криптографических алгоритмов и их реализации
УБИ.004	Угроза аппаратного сброса пароля BIOS
УБИ.006	Угроза внедрения кода или данных
УБИ.007	Угроза воздействия на программы с высокими привилегиями
УБИ.008	Угроза восстановления аутентификационной информации
УБИ.009	Угроза восстановления предыдущей уязвимой версии BIOS
УБИ.012	Угроза деструктивного изменения конфигурации/среды окружения программ
УБИ.013	Угроза деструктивного использования декларированного функционала BIOS
УБИ.014	Угроза длительного удержания вычислительных ресурсов пользователями
УБИ.015	Угроза доступа к защищаемым файлам с использованием обходного пути
УБИ.016	Угроза доступа к локальным файлам сервера при помощи URL
УБИ.017	Угроза доступа/перехвата/изменения HTTP cookies
УБИ.018	Угроза загрузки нештатной операционной системы
УБИ.019	Угроза заражения DNS-кеша
УБИ.022	Угроза избыточного выделения оперативной памяти
УБИ.023	Угроза изменения компонентов системы
УБИ.025	Угроза изменения системных и глобальных переменных
УБИ.026	Угроза искажения XML-схемы
УБИ.027	Угроза искажения вводимой и выводимой на периферийные устройства информации
УБИ.028	Угроза использования альтернативных путей доступа к ресурсам

УБИ.030	Угроза использования информации идентификации/аутентификации, заданной по умолчанию
УБИ.031	Угроза использования механизмов авторизации для повышения привилегий
УБИ.032	Угроза использования поддельных цифровых подписей BIOS
УБИ.033	Угроза использования слабостей кодирования входных данных
УБИ.034	Угроза использования слабостей протоколов сетевого/локального обмена данными
УБИ.036	Угроза исследования механизмов работы программы
УБИ.037	Угроза исследования приложения через отчёты об ошибках
УБИ.039	Угроза исчерпания запаса ключей, необходимых для обновления BIOS
УБИ.041	Угроза межсайтового скриптинга
УБИ.042	Угроза межсайтовой подделки запроса
УБИ.045	Угроза нарушения изоляции среды исполнения BIOS
УБИ.049	Угроза нарушения целостности данных кеша
УБИ.051	Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания
УБИ.053	Угроза невозможности управления правами пользователей BIOS
УБИ.054	Угроза недобросовестного исполнения обязательств поставщиками облачных услуг
УБИ.061	Угроза некорректного задания структуры данных транзакции
УБИ.062	Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера
УБИ.063	Угроза некорректного использования функционала программного и аппаратного обеспечения
УБИ.065	Угроза неопределённости в распределении ответственности между ролями в облаке
УБИ.067	Угроза неправомерного ознакомления с защищаемой информацией
УБИ.068	Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением
УБИ.069	Угроза неправомерных действий в каналах связи
УБИ.071	Угроза несанкционированного восстановления удалённой защищаемой информации
УБИ.072	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS
УБИ.073	Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети
УБИ.074	Угроза несанкционированного доступа к аутентификационной информации
УБИ.086	Угроза несанкционированного изменения аутентификационной информации
УБИ.087	Угроза несанкционированного использования привилегированных функций BIOS
УБИ.088	Угроза несанкционированного копирования защищаемой информации

УБИ.089	Угроза несанкционированного редактирования реестра
УБИ.090	Угроза несанкционированного создания учётной записи пользователя
УБИ.091	Угроза несанкционированного удаления защищаемой информации
УБИ.093	Угроза несанкционированного управления буфером
УБИ.095	Угроза несанкционированного управления указателями
УБИ.098	Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб
УБИ.099	Угроза обнаружения хостов
УБИ.100	Угроза обхода некорректно настроенных механизмов аутентификации
УБИ.102	Угроза опосредованного управления группой программ через совместно используемые данные
УБИ.103	Угроза определения типов объектов защиты
УБИ.104	Угроза определения топологии вычислительной сети
УБИ.109	Угроза перебора всех настроек и параметров приложения
УБИ.111	Угроза передачи данных по скрытым каналам
УБИ.113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники
УБИ.114	Угроза переполнения целочисленных переменных
УБИ.115	Угроза перехвата вводимой и выводимой на периферийные устройства информации
УБИ.116	Угроза перехвата данных, передаваемых по вычислительной сети
УБИ.117	Угроза перехвата привилегированного потока
УБИ.118	Угроза перехвата привилегированного процесса
УБИ.121	Угроза повреждения системного реестра
УБИ.122	Угроза повышения привилегий
УБИ.123	Угроза подбора пароля BIOS
УБИ.124	Угроза подделки записей журнала регистрации событий
УБИ.127	Угроза подмены действия пользователя путём обмана
УБИ.128	Угроза подмены доверенного пользователя
УБИ.129	Угроза подмены резервной копии программного обеспечения BIOS
УБИ.130	Угроза подмены содержимого сетевых ресурсов
УБИ.131	Угроза подмены субъекта сетевого доступа
УБИ.132	Угроза получения предварительной информации об объекте защиты
УБИ.139	Угроза преодоления физической защиты

УБИ.140	Угроза приведения системы в состояние «отказ в обслуживании»
УБИ.143	Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации
УБИ.144	Угроза программного сброса пароля BIOS
УБИ.145	Угроза пропуска проверки целостности программного обеспечения
УБИ.149	Угроза сбоя обработки специальным образом изменённых файлов
УБИ.150	Угроза сбоя процесса обновления BIOS
УБИ.152	Угроза удаления аутентификационной информации
УБИ.153	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов
УБИ.154	Угроза установки уязвимых версий обновления программного обеспечения BIOS
УБИ.155	Угроза утраты вычислительных ресурсов
УБИ.156	Угроза утраты носителей информации
УБИ.157	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации
УБИ.158	Угроза форматирования носителей информации
УБИ.159	Угроза «форсированного веб-браузинга»
УБИ.160	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации
УБИ.163	Угроза перехвата исключения/сигнала из привилегированного блока функций
УБИ.165	Угроза включения в проект не достоверно испытанных компонентов
УБИ.166	Угроза внедрения системной избыточности
УБИ.167	Угроза заражения компьютера при посещении неблагонадёжных сайтов
УБИ.168	Угроза «кражи» учётной записи доступа к сетевым сервисам
УБИ.170	Угроза неправомерного шифрования информации
УБИ.171	Угроза скрытного включения вычислительного устройства в состав бот-сети
УБИ.172	Угроза распространения «почтовых червей»
УБИ.173	Угроза «спама» веб-сервера
УБИ.174	Угроза «фарминга»
УБИ.175	Угроза «фишинга»
УБИ.177	Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью
УБИ.178	Угроза несанкционированного использования системных и сетевых утилит
УБИ.179	Угроза несанкционированной модификации защищаемой информации

УБИ.180	Угроза отказа подсистемы обеспечения температурного режима
УБИ.182	Угроза физического устаревания аппаратных компонентов
УБИ.184	Угроза агрегирования данных, обрабатываемых с помощью мобильного устройства
УБИ.185	Угроза несанкционированного изменения параметров настройки средств защиты информации
УБИ.186	Угроза внедрения вредоносного кода через рекламу, сервисы и контент
УБИ.187	Угроза несанкционированного воздействия на средство защиты информации
УБИ.188	Угроза подмены программного обеспечения
УБИ.189	Угроза маскирования действий вредоносного кода
УБИ.190	Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет
УБИ.191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения
УБИ.192	Угроза использования уязвимых версий программного обеспечения
УБИ.193	Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика
УБИ.197	Угроза хищения аутентификационной информации из временных файлов cookie
УБИ.198	Угроза скрытной журналу регистрации вредоносной программой учетных записей администраторов
УБИ.201	Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере
УБИ.203	Угроза утечки информации с неподключенных к сети Интернет компьютеров
УБИ.205	Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты
УБИ.208	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники
УБИ.209	Угроза несанкционированного доступа к защищаемой памяти ядра процессора
УБИ.211	Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем
УБИ.212	Угроза перехвата управления информационной системой
УБИ.214	Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации
УБИ.215	Угроза несанкционированного доступа к системе при помощи сторонних сервисов
УБИ.217	Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения

Приложение 2

Методика проверки отсутствия известных уязвимостей в программном обеспечении сегмента Абонента

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

1) проводится сканирование технических средств, программного обеспечения и средств защиты информации сегмента сертифицированным сетевым сканером безопасности XSpider 7.8.24 с профилями Default, Safe Scan и Web Scan или RedCheck;
2) при необходимости проводится устранение выявленных уязвимостей;
3) в случае невозможности устранения выявленных уязвимостей должны быть предприняты дополнительные меры защиты информации, направленные на устранение выявленных уязвимостей или исключающие возможность использования нарушителем выявленных уязвимостей.

Проверка считается пройденной успешно, если по результатам анализа уязвимостей подтверждено, что в сегменте отсутствуют уязвимости, содержащиеся в банке данных угроз безопасности информации ФСТЭК России, а также в иных источниках, или их использование (эксплуатация) нарушителем невозможно.

Приложение 3

Методика проверка готовности пользователей и администраторов к эксплуатации СЗИ сегмента

1) При проверке готовности администраторов сегмента проверяются знания:
   a. описания технологического процесса обработки информации на объекте информатизации;
   b. руководства администратора информационной безопасности внешнего сегмента государственной информационной системы автоматизации процесса управления государственными закупками Ульяновской области «АЦК-Госзаказ»;
   c. руководства администраторов на используемые в сегменте СрЗИ.
2) При проверке готовности пользователей сегмента проверяются знания:
   a. описания технологического процесса обработки информации на объекте информатизации;
   b. руководств пользователей на используемые в СЗИ сегмента СрЗИ.

Проверка считается пройденной успешно, если пользователи показывают знания перечисленных документов, достаточные для эксплуатации СрЗИ сегмента.

Приложение 4

Методика проверки выполненных настроек СрЗИ сегмента Абонента

№ п/п	Наименование проверки	Выполняемые действия	Критерий оценки успешности прохождения проверки
	Проверка настройки Secret Net Studio		
1.	Проверка характеристик паролей пользователя	Производится попытка смены пароля учетной записи пользователя на пароль содержащий менее 8 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 8 символов. Алфавит пароля не менее 60 символов. Период смены паролей не более чем через 120 дней
2.	Проверка блокирования доступа к информационной системе, при максимальном количестве неуспешных попыток аутентификации	Производится ввод неверного пароля для доступа (5 попыток).	Учетная запись блокируется после 5-й попытки, разблокировка доступна только администратору ИБ
3.	Проверка блокирования сеанса	Бездействие пользователя на в течение 5 минут	Сеанс автоматически блокируется после 5 минут бездействия пользователя
4.	Проверка сокрытия парольной информации при аутентификации пользователей	Производится ввод парольной информации в окне аутентификации	Вводимые символы пароля не отображаются
5.	Проверка настройки разграничения доступа информационным ресурсам	Проверяются свойства безопасности информационных ресурсов сегмента, включая принтеры и каталоги, на соответствие правам доступа, указанным в разрешительной системе доступа	В настройках безопасности информационных ресурсов сегмента должны содержаться права доступа, только допущенным пользователям в соответствии с разрешительной системой и списком допущенных лиц.
6.	Проверка разделения полномочий	Пользователь, не обладающий правами администратора производит	Выдается сообщение о недостаточности полномочий

	пользователей и администраторов	попытку смены настроек безопасности учетной записи пользователя	
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
8.	Проверка настройки механизмов защиты от НСД	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 — 8. Вновь подключаемые устройства, не входящие в состав ИС блокируются.
9.	Проверка режима функционирования МЭ «Secret Net Studio»	Проверка осуществляется путем попытки доступа при помощи утилиты «telnet» к информационным ресурсам сегмента. Дополнительно проводится проверка программным средством RedCheck или xSpider	Доступ к информационным ресурсам для всех входящих подключений отсутствует.
10.	Проверка регистрации событий удаленного доступа	Осуществляется попытка доступа из ЛВС к информационным ресурсам сегмента с рабочего места, не входящего в состав сегмента.	В журнале событий безопасности средства межсетевого экранирования отражается информация о попытках санкционированного/несанкционированного доступа.
	Проверка антивирусной системы защиты информации		
11.	Проверка запрета на отключение компонентов защиты пользователями, не обладающими правами администратора	Пользователь, обладающими правами администратора, делает попытку отключить компоненты защиты антивирусного средства.	Система устанавливает запрет на изменение настроек безопасности из учётной записи пользователя.
12.	Проверка автоматического обновления с доверенного	Просмотр даты обновления базы данныхвирусных сигнатур	Интервал между обновлениями базы данных вирусных сигнатур не превышает один день

	источника		
	Проверка обеспечения безопасных сетевых соединений		
13.	Проверка наличия СКЗИ VipNet Client или ViPNet Coordinator	Проверка наличия установленного СКЗИ VipNet Client или ViPNet Coordinator	Присутствует

Приложение 5

Методика проверки полноты и качества разработанной организационно-распорядительной документации по защите информации внешних сегментов ГИС.

№ 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 доступа	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 ИС	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 раз-	Проверить наличие утвержденного документа	Документ имеется в наличии

№ п/п	Наименование проверки	Выполняемые действия	Критерий оценки успешности прохождения проверки
	решенное к использованию программное обеспечение		
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 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
13.	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
14.	Проверка наличия документа, содержащего состав и содержание информации о событиях безопасности, подлежащих регистрации	Проверить наличие утвержденного документа	Документ имеется в наличии
15.	Проверка наличия документа, содержащего правила и процедуры сбора, записи и хранения информации о событиях безопасности	Проверить наличие утвержденного документа	Документ имеется в наличии
16.	Проверка наличия документа, содержащего правила и процедуры обновления и управления антивирусной защитой	Проверить наличие утвержденного документа	Документ имеется в наличии
17.	Проверка наличия документа, содержащего правила и процедуры обновления программного	Проверить наличие утвержденного документа	Документ имеется в наличии

№ п/п	Наименование проверки	Выполняемые действия	Критерий оценки успешности прохождения проверки
	обеспечения		
18.	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
19.	Проверка наличия документа, содержащего периодичность контроля состава технических средств, программного обеспечения и средств защиты информации	Проверить наличие утвержденного документа	Документ имеется в наличии
20.	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
21.	Проверка наличия документа, содержащего правила и процедуры восстановления информации	Проверить наличие утвержденного документа	Документ имеется в наличии
22.	Проверка наличия документа, определяющего границу контролируемой зоны	Проверить наличие утвержденного документа	Документ имеется в наличии
23.	Проверка наличия документа, содержащего правила и процедуры контроля и управления физическим доступом	Проверить наличие утвержденного документа	Документ имеется в наличии
24.	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
25.	Проверка наличия журнала учета машинных	Проверить наличие утвержденного документа	Документ имеется в наличии

№ п/п	Наименование проверки	Выполняемые действия	Критерий оценки успешности прохождения проверки
	носителе		
26.	Проверка наличия документа, содержащего процедуры уничтожения (стирания) информации на машинных носителях	Проверить наличие утвержденного документа	Документ имеется в наличии
27.	Проверка наличия документа, содержащего правила и процедуры выявления, анализа и устранения уязвимостей	Проверить наличие утвержденного документа	Документ имеется в наличии
28.	Проверка наличия документа, содержащего правила и процедуры резервного копирования	Проверить наличие утвержденного документа	Документ имеется в наличии

Приложение 6

Методика проверки соответствия системы защиты информации сегмента аттестованному ранее сегменту информационной системы

№ п/п	Наименование проверки	Критерий оценки успешности прохождения проверки
1.	Проверяется отсутствие в составе СВТ беспроводных клавиатур и беспроводных мышей. Модули беспроводной связи СВТ должны быть деактивированы или отключены	Беспроводные устройства не используются. Модули беспроводной связи отсутствуют или отключены.
2.	Проверяется совместимость ОС со СрЗИ	ОС включена в перечень поддерживаемых операционных систем формуляров средств защиты информации
3.	Проверяется правильность эксплуатации СрЗИ	СрЗИ установлены и настроены в соответствии с требованиями эксплуатационной документацией. На все установленные СрЗИ имеются акты установки
4.	Проверяется актуальность сертификатов на установленные СКЗИ и СрЗИ	Есть действующие сертификаты соответствия на все СКЗИ и СрЗИ, применяемые в сегменте
5.	Проверяется назначение ответственных лиц при эксплуатации сегмента	Абонентом назначены: лицо, ответственное за обеспечение эксплуатации пользовательского сегмента ГИС; администратор безопасности, 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 безопасности ГИС; пользователи, допущенные к работе в пользовательских сегментах ГИС; администраторы (технические специалисты), допущенные для обслуживания аппаратного и программного обеспечения сегментов
6.	Проверяется разделение функций (ролей) по обработке информации, администрированию системы защиты информации и обеспечению функционирования СВТ сегмента	Выполнение функций (ролей) по обработке информации, администрированию системы защиты информации и обеспечению функционирования СВТ сегмента возлагается на отдельные должностные лица
7.	Проверяются права и привилегии по настройке СрЗИ	Права и привилегии по доступу к параметрам настройки средств защиты информации предоставляются исключительно администратору безопасности
8.	Проверяется используемые СКЗИ	Для обеспечения защиты конфиденциальной информации при передаче информации по каналам связи применяются сертифицированные СКЗИ класса КС3 и выше
9.	Проверяется возможность удаленного доступа к ресурсам сегмента	Удаленный доступ к ресурсам сегмента ограничен подсистемой межсетевого экранирования

10.	Проверяется реализация организационно-режимных мер, обеспечивающих контролируемое пребывание лиц в Помещениях и доступа к техническим средствам сегмента	Реализованы и поддерживаются организационно режимные меры, обеспечивающие возможность пребывания и/или непосредственного доступа к техническим средствам сегмента. Имеются списки доступа.
11.	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
12.	Проверка наличия у каждого пользователя сегмента индивидуального идентификатора (учетной записи).	С целью соблюдения принципа персональной ответственности за свои действия каждому пользователю, допущенному к работе в сегменте ГИС, сопоставлено персональное уникальное имя (учетная запись пользователя).
13.	Проверка блокировки учетных записей пользователей после неудачных попыток ввода пароля	Осуществляется блокировка учетных записей пользователей при 5 неудачных попытках регистрации (попыток входа) с возможностью автоматического разблокирования через 15 мин
14.	Проверяется возможность блокировки сеанса доступа к операционной системе при бездействии пользователя	Осуществляется блокировка сеанса доступа к операционной системе после бездействия пользователя в течение 5 минут.
15.	Проверяется настройка отображения сведений пользователя при блокировке сеанса доступа	Сведения о пользователе не отображается при блокировке сеанса доступа.
16.	Проверяется настройка отображения имени последнего входа пользователя	В диалоговом окне входа в операционную систему не отображается имя последнего пользователя, выполнившего вход
17.	Проверяется настройка повторного использования идентификаторов	Исключено повторное использование идентификатора пользователя.
18.	Проверка установленной минимальной длины пароля	Установлена минимальная длина пароля — 8 символов.
19.	Проверка выполнения требования к не повторяемости пароля	Организационно-распорядительной документацией Абонента определено, что при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях.
20.	Проверка выполнения требования к максимальному сроку действия пароля	Периодичность смены пароля не превышает 120 дней
21.	Проверка блокировки неактивных учетных записей	Осуществляется блокировка неактивных (неиспользуемых) учетных записей пользователей после периода времени неиспользования 90 дней
22.	Проверка невозможности сохранения реквизитов доступа	Исключена возможность сохранения реквизитов доступа пользователей
23.	Проверка способа обновления операционной системы	Обеспечена невозможность модификации операционной системы Windows через общедоступные каналы передачи данных
24.	Проверяется учетные записи, созданные в операционной системе по молчанию	Пользователь Administrator переименован
25.	Проверка учетных записей, созданных в операционной системе по	Учетная запись для гостевого входа (Guest) заблокирована

	умолчанию. Проверка способа входа в операционную систему.	
26.	Проверка невозможности беспроводного доступа	Исключена возможность беспроводного доступа к СВТ сегмента
27.	Проверка возможности использования незарегистрированных (неучтенных) съемных машинных носителей информации (в том числе находящихся в личном пользовании	Возможность использования незарегистрированных (неучтенных) съемных машинных носителей информации (в том числе находящихся в личном пользовании) исключена с использованием СрЗИ от НСД
28.	Проверка регистрации и учета машинных носителей информации	Применяемые носители информации маркируются и учитываются в журнале учета машинных носителей
29.	Проверка оборудования технических средств АРМ средствами контроля за вскрытием	Технические средства АРМ оборудованы средствами контроля за вскрытием
30.	Проверка наличия дистрибутивов СКЗИ	Дистрибутивы СКЗИ имеются в наличии и получены от организаций, действующих на основании лицензии ФСБ на право распространения СКЗИ
31.	Проверка наличия дистрибутивов СрЗИ	Дистрибутивы установленных СрЗИ имеются в наличии
32.	Проверка отсутствия средств разработки программного обеспечения и отладчики	Средства разработки программного обеспечения и отладки отсутствуют
33.	Проверка правильности хранения дистрибутивов СрЗИ	Обеспечивается защищенное хранение дистрибутивов программных средств, в том числе средств защиты информации, и документации на данные средства
34.	Проверка разграничения прав доступа на установку и настройку СрЗИ	Права на установку и настройку СрЗИ имеет только администратор
35.	Проверка наличия технического паспорта сегмента	Документ имеется в наличии
36.	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
37.	Проверка регистрации событий изменения конфигурации и параметров безопасности учетной записи	Регистрируются события изменения конфигурации и параметров безопасности учетной записи
38.	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
39.	Проверка наличия документа, определяющего порядок действий при возникновении нештатных ситуации, условия выполнения каждого действия (перечень событий, при	Документ имеется в наличии

	наступлении которых необходимо совершить определенное действие и т.п.)	
40.	Проверка наличия документа, регламентирующего порядок и периодичность проведения контроля состояния защиты информации	Документ имеется в наличии

Приложение 7

Типовая форма протокола проведения приемочных испытаний внешнего сегмента при подключении к государственной информационной системы автоматизации процесса управления государственными закупками Ульяновской области «АЦК-Госзаказ»

УТВЕРЖДАЮ	УТВЕРЖДАЮ
Руководитель Абонента	Ответственное лицо Оператора ГИС
_____ ФИО	_____ ФИО
«___» _____ 20__ г.	«___» _____ 20__г.

Внешний сегмент, проходящий проверку соответствия сегменту государственной информационной системы автоматизации процесса управления государственными закупками Ульяновской области «АЦК-Госзаказ», в отношении которого уже произведены аттестационные испытания

Наименование Абонента

Протокол проведения приемочных испытаний

Листов

АННОТАЦИЯ

Настоящий протокол составлен по результатам приемочных испытаний сегмента Абонента (далее - АРМ), предназначенногодля подключения к государственной информационной системе автоматизации процесса управления государственными закупками Ульяновской области «АЦК-Госзаказ» через веб- интерфейс, выполненных в соответствии с «Программой и методикой приемочных испытаний внешних сегментов государственной информационной системы автоматизации процесса управления государственными закупками Ульяновской области «АЦК-Госзаказ» от_. .2024 уч. №_(далее по тексту «ПиМ»).

1. Общие положения

Объект испытаний:

Сегмент, предназначенный для подключения к государственной информационной системы автоматизации процесса управления государственными закупками Ульяновской области «АЦК-Госзаказ» (далее — сегмент).

Тип сегмента: «Внешний пользователь (вариант подключения №1)» или «Внешний пользователь (вариант подключения №2)»

Место испытаний:

— *адрес*

Дата и время испытаний:

- *дата начала испытаний*
- *дата окончания испытаний*

Состав комиссии по проведению испытаний

Члены комиссии		
	должность	*организация*
	должность	*организация*
	должность	*организация*
	должность	*организация*
	должность	*организация*
	должность	*организация*

2. Проверка классификации сегмента и оценка актуальных угроз безопасности информации сегмента

Классификация сегмента Абонента произведена, присутствует акт классификации, в котором уровень защищенности персональных данных, обрабатываемых в сегменте соответствует 4 (УЗ 4). Класс защищенности – К3.

Перечень актуальных угроз безопасности информации сегмента Абонента соответствует перечню актуальных угроз безопасности информации внешнего аттестованного сегмента ГИС.

3. Результаты испытаний

3.1 Проверка отсутствия известных уязвимостей в сегменте

№ п/п	СЗИ	Результат анализа
1	Сетевой сканер безопасности XSpider или RedCheck (выбрать нужное_	Содержится в Приложении 1 кнастоящему документу

3.2 Проверка готовности пользователей и администраторов к эксплуатации СЗИ

№ п/п	Проверка	Результат
1	Проверка готовности администраторов сегмента	
1.a	Знание описания технологического процесса обработки информации на объекте информатизации	
1.b		
1.c		
2	Проверка готовности пользователей сегмента	
2.a		
2.b		

3.3 Проверка выполненных настроек СрЗИ сегмента Абонента.

№ п/п	**Наименование проверки**	**Выполняемые действия**	**Критерий оценки успешности прохождения проверки**

1			
…			
13			

3.4 Проверки полноты и качества разработанной организационно-распорядительной документации по защите информации внешних сегментов ГИС.

№ п/п	Наименование проверки	Выполняемые действия	Критерий оценки успешности прохождения проверки
1			
…			
28			

3.5 Проверки соответствия системы защиты информации сегмента аттестованному ранее сегменту информационной системы

№ п/п	Наименование проверки	Критерий оценки успешности прохождения проверки
1		
…		
42		

4. Сведения об отказах, сбоях и аварийных ситуациях

Отказов, сбоев и аварийных ситуаций во время испытаний не обнаруживалось

5. Сведения о корректировках параметров объекта испытаний и технической документации

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

6. Заключение комиссии

Результаты испытаний:

В ходе проведения приемочных испытаний сегмента, была обеспечена проверка выполнения ее функций во всех режимах функционирования, устаwовленных в ПиМ.
Комиссия пришла к выводv о:

- *соответствии класса защищенности и уровня защищенности персональных данных, обрабатываемых в сегменте заказчика внешнему сегменту ГИС;*
- *отсутствии известных уязвимостей в программном обеспечении сегмента;*
- *готовности пользователей и администраторов к эксплуатации сегмента;*
- *выполненных настройках системы защиты;*
- *соответствии полноты и качества разработанной организационно-распорядительной документации по защите информации;*
- *соответствии системы защиты информации сегмента аттестованному ранее сегменту информационной системы.*

Выводы:

По результатам проведения приемочных испытаний может быть составлен акт о соответствии сегмента Абонента, сегменту государственной информационной системе автоматизации процесса управления государственными закупками Ульяновской области «АЦК-Госзаказ», прошедшему аттестационные испытания, о готовности к подключению к государственной информационной системе и готовности приемки в постоянную эксплуатацию.