МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ НАУЧНОЕ УЧРЕЖДЕНИЕ

«ФЕДЕРАЛЬНЫЙ НАУЧНЫЙ ЦЕНТР ИССЛЕДОВАНИЙ И РАЗРАБОТКИ ИММУНОБИОЛОГИЧЕСКИХ ПРЕПАРАТОВ ИМ. М.П. ЧУМАКОВА РАН» (ИНСТИТУТ ПОЛИОМИЕЛИТА)
(ФГАНУ «ФНЦИРИП им. М.П. Чумакова РАН» (Институт полиомиелита))

Адрес места нахождения: улица Кржижановского, дом 29, корпус 5, помещение I, комната № 6, город Москва, 117218

Почтовый адрес: поселение Московский, посёлок Института полиомиелита, дом 8, корпус 1, город Москва, 108819

Тел./факс (495) 841-90-02; (495) 549-67-60
E-mail: sue_polio@chumakovs.su; www.chumakovs.ru
ОКПО 01895045, ОГРН 1167746624847,
ИНН/КПП 7751023847/772701001

№ 23/3 от 23.01.2024г.

Исполнителям, заинтересованным в оказании Услуг
От:
Федеральное государственное автономное научное учреждение «Федеральный научный центр исследований и разработки иммунобиологических препаратов им. М.П. Чумакова РАН» (Институт полиомиелита) ФГАНУ «ФНЦИРИП им. М.П. Чумакова РАН» (Институт полиомиелита),
108819, г. Москва, поселение Московский, поселок Института полиомиелита, дом 8, корпус 1, umto@chumakovs.su, (495) 841-01-32

Запрос о предоставлении коммерческих предложений

ФГАНУ «ФНЦИРИП им. М.П. Чумакова РАН» (Институт полиомиелита) планирует проведение процедуры закупки на выполнение периодического технического контроля информационной системы персональных данных, в соответствии с Федеральным законом от 18 июля 2011 года № 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц».

Просим предоставить информацию о стоимости Услуг в соответствии с предлагаемой ниже информацией (Техническим заданием).

№ п/п	Оказываемая услуга	Ед. измерения	Количество	Срок выполнения услуг
1	Проведение периодического контроля уровня защиты информации на аттестованном объекте информатизации	Условная единица	1	60 рабочих дней с даты заключения договора
2	Установка и настройка средств защиты информации	Условная единица	1	
3	Предоставление прав на использование «Сканер-ВС», лицензия на 4 IP адреса на 1 год	Условная единица	1	
4	Предоставление программного продукта «SecretDoc»	Условная единица	1	

ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ

АРМ Автоматизированное рабочее место.
ИС Информационная система.
ИСПДн Информационная (-ых) система (-х) персональных данных.
ПДн Персональные данные.
ПО Программное обеспечение.
РФ Российская Федерация.
СЗИ Средство (-а) защиты информации.
СЗПДн Система защиты персональных данных.
ФСБ России Федеральная служба безопасности Российской Федерации.
ФСТЭК России Федеральная служба по техническому и экспортному контролю.

ЦЕЛЬ И ЗАДАЧИ ОКАЗАНИЯ УСЛУГ

Основной целью оказания услуг является обеспечение защиты ПДн от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных несанкционированных действий в отношении такой информации, обрабатываемой в

информационной системе персональных данных ФГАНУ «ФНЦИРИП им. М.П. Чумакова РАН» (Институт Полиомиелита) (далее – ИСПДн).

Оказываемые услуги должны включать в себя мероприятия по реализации организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн, необходимых для выполнения установленных требований к защите ПДн.

Задачи, подлежащие решению при оказании услуг:

– поставка, установка и настройка СЗИ (согласно требованиям, приведенным в приложении № 1 к настоящему Техническому заданию);

– проведение периодического технического контроля (испытания) ИСПДн на соответствие требованиям безопасности информации.

Срок оказания услуг: 60 рабочих дней с даты заключения договора.

ХАРАКТЕРИСТИКА ОБЪЕКТА ИНФОРМАТИЗАЦИИ

Обработка ПДн осуществляется в рамках ИСПДн.

Обработка, хранение и передача ПДн в ИСПДн происходит с использованием программных и технических средств.

Аппаратной платформой для программных средств обработки ПДн является автоматизированное рабочее место пользователей ИСПДн.

В состав ИСПДн входит 1 АРМ пользователей по адресу Заказчика.

ТРЕБОВАНИЯ К ОБЪЕМУ ОКАЗЫВАЕМЫХ УСЛУГ

Оказание услуг по выполнению периодического технического контроля ИСПДн включает в себя следующие мероприятия:

Обновление СЗПДн.

Исполнитель выполняет поставку, обновление, установку и настройку СЗИ на АРМ Заказчика (согласно требованиям, приведенным в Приложении 1 к настоящему Техническому заданию).

Установка и настройка СЗИ осуществляется Исполнителем в соответствии с требованиями нормативных документов ФСТЭК России, а также в соответствии с эксплуатационной документацией на СЗИ. Исполнитель предоставляет Заказчику акт установки СЗИ.

Заказчик предоставляет технические и программные средства для установки средств защиты информации. Состав программных и аппаратных средств, предоставляемых Заказчиком, должен соответствовать требованиям, указанным в формулярах на поставляемые СЗИ.

Исполнитель предоставляет ПО для автоматизации организационных мероприятий по обеспечению информационной безопасности (онлайн-сервис), поставляемого в рамках данного ТЗ (в соответствии с Приложением 1 настоящего ТЗ). Исполнитель проводит инструктаж пользователей Заказчика по использованию ПО для автоматизации организационных мероприятий по обеспечению информационной безопасности (онлайн-сервиса).

Проведение периодического технического контроля.

Исполнителем проводятся испытания ИСПДн на соответствие требованиям по безопасности информации. Испытания проводятся в соответствии с утвержденной Исполнителем и согласованной с Заказчиком «Программой и методиками аттестационных испытаний».

Проверка состояния технологического процесса автоматизированной обработки защищаемой информации, в том числе ПДн, включающая в себя:

– анализ обобщённой технологической схемы ИСПДн с существующими информационными потоками, возможностями доступа к обрабатываемой и передаваемой информации, в том числе ПДн;

– проверку соответствия описания технологического процесса обработки, хранения и передачи информации ограниченного доступа реальной практике на объекте;

– определение субъектов и объектов доступа и средств обработки и передачи информации;

– проверку данных ИСПДн, представленных в техническом паспорте;

– проверку наличия оформленных разрешений на допуск персонала к конфиденциальной информации, меток конфиденциальности на информационных носителях, соответствия технологических инструкций пользователей и администратора безопасности установленным требованиям;

– установление опасных факторов и угроз, критических мест ИСПДн, снижающих уровень защиты.

Проверка ИСПДн на соответствие организационно-техническим требованиям по защите информации, включающая в себя:

– проверку правильности классификации ИСПДн;

– проверку уровня подготовки кадров и распределения ответственности персонала;

– проверку комплектности и характеристик средств защиты, наличия сертификатов соответствия на средства вычислительной техники (СВТ) и средства защиты информации (СЗИ);

– проверку выполнения требований к помещениям, в которых производится обработка информации средствами ИСПДн.

По результатам испытаний ИСПДн Исполнителем оформляются Протокол аттестационных испытаний и Заключение с выводом о соответствии объекта информатизации требованиям по безопасности информации.

При выявлении несоответствия, в Заключении указываются выявленные недостатки с рекомендациями по их устранению.

ТРЕБОВАНИЯ К ПОСТАВЛЯЕМЫМ СЗИ

Исполнитель должен обеспечить:

– предпродажную подготовку СЗИ в соответствии с требованиями (приложение № 1 к настоящему Техническому заданию);

– работоспособность поставляемых СЗИ.

ПО поставляемых СЗИ должно иметь действующие сертификаты.

При оказании услуг должны соблюдаться все авторские и смежные с ними права разработчика СЗИ.

ТРЕБОВАНИЯ К ОРГАНИЗАЦИОННОМУ ОБЕСПЕЧЕНИЮ ПРИ ОКАЗАНИИ УСЛУГ

Исполнитель обязан использовать исправные и поверенные приборы, инструменты и средства измерений.

Исполнитель обязан оказывать услуги в соответствии с требованиями эксплуатационной документации на приборы, инструменты и средства измерений с соблюдением норм и правил техники безопасности.

Исполнитель устанавливает и настраивает СЗИ в соответствии с требованиями законодательства по защите информации, а также в соответствии с эксплуатационной документацией на СЗИ.

ПОРЯДОК ПРИЕМКИ РЕЗУЛЬТАТОВ РАБОТ

Исполнитель обязан своевременно предоставить отчетную документацию Заказчику в порядке, определенном Договором и в соответствии с разделом 4 «Требования к объему оказываемых услуг» настоящего ТЗ.

Исполнитель должен уведомить Заказчика о готовности к сдаче-приемки работ в срок, не превышающий 5 (пять) дней до даты окончания работ.

Документы должны быть представлены в бумажном виде, в 1 экземпляре, и в электронном виде в 1 экземпляре.

Документы, передаваемые в электронном виде, должны быть представлены в форматах MS Office (в формате *.doc/*docx для текстовых документов, *.xls/*xlsx для таблиц и расчетов и *.vsd/*vsdx для схем и чертежей). Все комплекты документов, передаваемых в бумажном виде, должны предоставляться в адрес Заказчика с сопроводительным письмом.

Экспертизу и приемку результатов работ осуществляет Заказчик. Заказчик имеет право для приемки работ привлекать внешнюю экспертизу.

В случае отсутствия замечаний, Заказчик в течение 5 (пяти) рабочих дней с момента завершения приемки подписывает два экземпляра Акта сдачи-приемки выполненных работ и возвращает 1 (один) экземпляр Исполнителю. В случае наличия замечаний, Заказчик направляет Исполнителю мотивированный отказ от приемки работ с перечнем необходимых доработок и указанием сроков их выполнения. Исполнитель должен устранить недостатки в указанные сроки и предъявить результаты Заказчику. Повторная приемка работ должна осуществляться в порядке, определенном настоящим разделом.

Оплата работ Заказчиком предусматривается в случае приемки работ на основании подписанного Исполнителем и Заказчиком Акта сдачи-приемки выполненных работ.

ГАРАНТИЙНЫЕ ОБЯЗАТЕЛЬСТВА

Исполнитель должен обеспечить гарантийное обслуживание поставленного (используемого) оборудования на следующих условиях:

– исполнитель гарантирует, что поставляемое (используемое) оборудование соответствует требованиям, приведенным в Приложении 1 настоящего Технического задания, а также свободно от дефектов материалов и изготовления;

– срок гарантии производителя на все поставленное оборудование должен составлять не менее 12 месяцев.

ТРЕБОВАНИЯ К ЛИЦЕНЗИРОВАНИЮ ИСПОЛНИТЕЛЯ

В соответствии с подпунктом 5 пункта 1 статьи 12 Федерального закона № 99-ФЗ «О лицензировании отдельных видов деятельности» от 04 мая 2011 года Исполнитель обязуется

предоставить документы, подтверждающие соответствие оказываемых услуг требованиям законодательства:

– копию действующей лицензии ФСТЭК России на осуществление деятельности по технической защите конфиденциальной информации.

ТРЕБОВАНИЯ К КАЧЕСТВУ УСЛУГ

Услуги должны оказываться с соблюдением требований Федерального закона № 152-ФЗ от 27 июля 2006 года «О персональных данных» и принятыми в соответствии с ним нормативно-методическими документами, устанавливающими требования к защите персональных данных.

Качество и комплектность СЗИ и ПО должны соответствовать требованиям, предъявляемым к техническим характеристикам товара в стране производителя, а также действующим в РФ стандартам и техническим условиям. Упаковка, в которой поставляется ПО, должна обеспечивать ее сохранность при транспортировке и хранении. Маркировка на упаковке должна соответствовать действующим стандартам.

ИСТОЧНИКИ РАЗРАБОТКИ

Исполнитель при оказании услуг должен обеспечивать соблюдение следующих федеральных законов, постановлений Правительства Российской Федерации и нормативных актов:

– Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

– Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Постановления Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– «Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности» (утверждены руководством 8 Центра ФСБ России 31 марта 2015 года № 149/7/2/6-432).

– Приказ Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. № 378 г. Москва «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»;

– ГОСТ 34.602-2020 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы».

ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ КОНФИДЕНЦИАЛЬНОСТИ

В период оказания услуг и после их окончания Исполнитель не должен разглашать и использовать конфиденциальную информацию, принадлежащую Заказчику, которая может стать ему известной в ходе оказания услуг. Исполнитель несет ответственность за соблюдение этого требования в соответствии с законодательством Российской Федерации.

Приложение 1 к Техническому заданию

Перечень поставляемых средств защиты информации

№ п/п	Наименование средств защиты информации	Функциональные характеристики средств защиты информации	Количество, шт.
1.	Средство анализа защищенности	**Требования к средствам анализа защищенности (САЗ):** ***1. Требования к механизмам сетевого аудита САЗ*** 1) САЗ должно обеспечивать инвентаризацию ресурсов сети, определение состояния TCP и UDP портов в диапазоне от 1 до 65535, идентификацию операционных систем и сетевых приложений, трассировку маршрутов следования данных для построения топологии сети. 2) САЗ должно обнаруживать уязвимости кода и конфигурации программного обеспечения. Для	1

№ п/п	Наименование средств защиты информации	Функциональные характеристики средств защиты информации	Количество, шт.
		выявления (поиска) уязвимостей САЗ должно использовать встроенную базу данных уязвимостей кода и уязвимостей конфигурации программного обеспечения. База данных уязвимостей САЗ должна содержать унифицированные описания уязвимостей, аналогичные содержащимся в следующих общедоступных источниках: банк данных угроз безопасности информации ФСТЭК России (http://www.bdu.fstec.ru), база данных «Common Vulnerabilities and Exposures (https://cve.mitre.org). САЗ должно осуществлять тестирование на проникновение путем эксплуатации уязвимостей, выявленных и содержащихся в базе данных уязвимостей. 3) САЗ должно осуществлять поиск уязвимостей автоматизировано или по расписанию, задаваемому оператором. 4) САЗ должно осуществлять обновление базы данных уязвимостей через сервис обновлений САЗ. 5) САЗ должно осуществлять подбор паролей по словарю для следующих сетевых сервисов: ftp, http, imap, mssql, mysql, oracle, pop3, postgres, rdp, redis, smb, smtp, snmp, ssh, telnet, vnc. 6) САЗ должно осуществлять аудит безопасности беспроводных сетей и имитацию атак на них. 7) САЗ должно осуществлять перехват, анализ и фильтрацию сетевых пакетов локальной и внешней сетей информационной системы и извлечение из сетевого трафика парольной информации (для протоколов ftp, pop3, http, https, telnet), а также, проверку возможности атак подмены MAC-адресов. 8) САЗ должно обеспечивать контроль за установкой обновлений ОС Microsoft Windows: 7, 8.1, 10, Server 2012, Server 2012-R2, Server 2016 9) САЗ должно обеспечивать контроль за настройками комплекса средств защиты ОС специального назначения «Astra Linux Special Edition». 10) САЗ должно обеспечивать формирование отчетов по результатам проверок в форматах: HTML, PDF, DOC, CSV. ***2. Требования к механизмам локального аудита САЗ*** 1. САЗ должно осуществлять поиск остаточной информации на различных носителях информации и гарантированное уничтожение информации путем записи случайной последовательности символов поверх стираемой информации, а также записи случайной последовательности символов в освободившееся пространство накопителей на жестких магнитных дисках, накопителей на основе флэш-памяти и съемных носителей информации.	

№ п/п	Наименование средств защиты информации	Функциональные характеристики средств защиты информации	Количество, шт.
		2. САЗ должно осуществлять локальный подбор паролей по словарю для учетных записей пользователей ОС Microsoft Windows:7, 8.1, 10. 3. САЗ должно обеспечивать контрольное суммирование заданных файлов, папок, подпапок, съемных носителей и накопителей на жестких магнитных дисках. Комплект поставки средства анализа защищенности включает в себя: - неисключительно право на ПО средства анализа защищенности, позволяющее одновременное сканирование не менее 4 IP адресов.	
2.	Программное обеспечение для автоматизации организационных мероприятий по обеспечению информационной безопасности	ПО должно представлять собой онлайн-сервис и позволять автоматизировать разработку и ведение организационно-распорядительной документации в сфере информационной безопасности. ПО должно обеспечивать работу с неограниченным числом организаций. Создание внутренней документации каждой организации должно быть доступно как вручную, так и с использованием готовых шаблонов. ПО должно обеспечивать выполнение следующих основных функций: – автоматизация и систематизация разработки и ведения организационно-распорядительной документации в области информационной безопасности: • создание внутренней документации организации в области информационной безопасности как вручную, так и с использованием готовых шаблонов; • поддержание созданной документации в актуальном состоянии; – выполнение требований надзорных органов в области использования средств криптографической защиты информации и средств защиты информации; – инвентаризационный учёт активов, обеспечивающих информационную безопасность организации; возможность автоматического учета технических средств на основе отчетов из сканера уязвимостей RedCheck; – организация проведения совместных закупок в области информационной безопасности и информационных технологий; – учёт и обработка инцидентов в области информационной безопасности, назначение ответственных и задач для обработки инцидентов; возможность автоматического учета инцидентов на основе отчетов из сканера уязвимостей RedCheck; – учет и контроль проведения мероприятий для подготовки организации к проведению проверок надзорным органом в области информационной	1

№ п/п	Наименование средств защиты информации	Функциональные характеристики средств защиты информации	Количество, шт.
		безопасности; возможность назначения и проведения видео-инструктажей для сотрудников организации; – информирование пользователей посредством SMS и Email-уведомлений о назначениях инцидентов, задач, а также изменениях в организационно-распорядительной документации; – ведение документооборота с системой согласования в том числе ведение юридически-значимых документооборота с подписанием усиленной квалифицированной электронной подписью; – предоставление доступа к данным системы посредством WEB-интерфейса и мобильного приложения. В рамках функционирования ПО должно осуществляться взаимодействие со следующими внешними системами: – система SMS-уведомлений; – система Email-уведомлений; – внешняя система юридически-значимого электронного документооборота. Взаимодействие с системой SMS-уведомлений должно осуществляться с использованием протоколов и механизмов, предоставляемых API-интерфейсом данной системы. Взаимодействие с системой Email-уведомлений должно осуществляться с использованием протоколов и механизмов, предоставляемых API-интерфейсом данной системы. Взаимодействие с внешней системой юридически-значимого электронного документооборота осуществляться с использованием протоколов и механизмов, предоставляемых API-интерфейсом системы ЭДО Русь-Телеком. ПО должно иметь клиент-серверную архитектуру и предусматривать WEB-интерфейс работы пользователя с базой данных и подсистемой ввода–вывода данных, в котором все операции бизнес-логики производятся на сервере. ПО должно поддерживать работу с использованием WEB-браузеров: Google Chrome 96.0 и выше, Mozilla Firefox 18.5 и выше, Opera 82.0 и выше, Яндекс.Браузер 21.11.4 и выше, Safari 15.1 и выше. ПО должно быть зарегистрировано в государственном реестре программ и баз данных в соответствии с действующим законодательством как самостоятельная программа для ЭВМ. Комплект поставки включает: – лицензия на неисключительное право использования ПО в электронном виде.	

Предполагаемые сроки проведения процедуры закупки: январь 2024 г.
Порядок оплаты: Оплата производится за фактически оказанные Услуги в течение 7 (семи) рабочих дней после подписания Акта оказанных Услуг и предоставления счета на оплату. Аванс не предусмотрен.

Особенности: Процедура закупки будет проводиться в соответствии с требованиями Федерального закона от 18 июля 2011 года № 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц».

Ответ должен содержать срок действия предлагаемой цены и расчет стоимости услуг, срок оказания услуг. В частности, из содержания предложения должны однозначно определяться цена за единицу услуги, описание услуг и общая цена договора на условиях, указанных в настоящем запросе.

Ответы должны быть поданы с «23» 01 2024 г. по «26» 01 2024 г. включительно по адресу: umto@chumakovs.su. Ответ должен иметь реквизиты Поставщика, печать и подпись.

Рекомендуем в теме письма указать номер запроса коммерческих предложений.

В коммерческом предложении обязательно должны быть реквизиты: номер и дата.

Проведение данной процедуры сбора информации не влечёт за собой возникновения каких-либо обязательств Заказчика.

При наличии технических ошибок и неточностей при описании Услуг просим сообщить Заказчику.

Если основные условия исполнения Договора отличаются от предложенных – просим сообщить Заказчику в Коммерческом предложении.

С уважением,

Первый заместитель
генерального директора А.Ю. Афонин