

## Техническое задание

Предмет закупки «Приобретение неисключительных прав на использование системы контроля доступа привилегированных пользователей»

Нижний Новгород  
2022 г.

## СОДЕРЖАНИЕ

РАЗДЕЛ 1. ПЕРЕЧЕНЬ И ОБЪЕМ ПЕРЕДАВАЕМЫХ НЕИСКЛЮЧИТЕЛЬНЫХ ПРАВ .....	3
<i>Подраздел 1.1. Состав (перечень) передаваемых неисключительных прав .....</i>	<i>3</i>
РАЗДЕЛ 2. ТРЕБОВАНИЯ ПО ПРАВИЛАМ СДАЧИ И ПРИЕМКИ .....	3
<i>Подраздел 2.1. Порядок сдачи и приемки .....</i>	<i>3</i>
<i>Подраздел 2.2. Требования по передаче лицензиату технических и иных документов при поставке товаров .....</i>	<i>3</i>
РАЗДЕЛ 3. ОБЩИЕ ТРЕБОВАНИЯ .....	4
<i>Подраздел 3.1. Назначение ПО .....</i>	<i>4</i>
<i>Подраздел 3.2. Структура ПО .....</i>	<i>4</i>
<i>Подраздел 3.3. Функциональные возможности .....</i>	<i>4</i>
<i>Подраздел 3.4. Масштабирование компонентов ПО .....</i>	<i>8</i>
<i>Подраздел 3.5. Общие требования к программному обеспечению .....</i>	<i>8</i>
РАЗДЕЛ 4. ТРЕБОВАНИЯ К КАЧЕСТВУ .....	8
РАЗДЕЛ 5. ТРЕБОВАНИЕ К ФОРМЕ ПРЕДСТАВЛЯЕМОЙ ИНФОРМАЦИИ .....	9
РАЗДЕЛ 6. ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ .....	9

## РАЗДЕЛ 1. ПЕРЕЧЕНЬ И ОБЪЕМ ПЕРЕДАВАЕМЫХ НЕИСКЛЮЧИТЕЛЬНЫХ ПРАВ

<i>Подраздел 1.1. Состав (перечень) передаваемых неисключительных прав</i>						
№ п/п	Наименование ПО	Вид носителя	Срок окончания использования ПО	Кол-во лицензий	Описание, количество рабочих мест/устройств/пользователей/ учетных записей	Срок (Дата) передачи Прав
1	Система контроля доступа привилегированных пользователей	CD/DVD/Flash	бессрочно	1	Лицензия данного ПО должна поддерживать работу с неограниченным количеством пользователей и конечных устройств не менее 9 конкурентных сессий одновременно.	24.11. 2022
<p>1. Порядок предоставления Лицензиату ключей, файлов электронных лицензий, паролей и т.п. (Ключей, ПО):</p> <ul style="list-style-type: none"> <li>• Ключи и ПО передаются Лицензиаром Лицензиату своими силами и за свой счет на не режимной территории на CD/DVD/Flash –диске по адресу: Россия, г.Нижний Новгород, Бурнаковский проезд, 15, с оформлением Сторонами Акта приема-передачи, подтверждающего фактическую передачу.</li> </ul> <p>2. Способы использования ПО: Право на использование программ для ЭВМ, предоставляемое Лицензиату в соответствии с проектом Договора, включает использование следующими способами:</p> <ul style="list-style-type: none"> <li>• Лицензиат имеет право на воспроизведение программ для ЭВМ, ограниченное правом инсталляции, копирования для целей резервного хранения, запуска программы для ЭВМ и использования в соответствии с ее функциональным назначением;</li> <li>• Лицензиат не имеет право производить декомпиляцию и модификацию ПО;</li> <li>• Лицензиат не имеет право передавать право пользования ПО третьим лицам;</li> <li>• Лицензиат имеет право изготовить копию Ключей при условии, что эта копия может использоваться для архивных целей и для замены Ключей, когда оригинал утерян или стал непригоден для использования.</li> </ul>						

## РАЗДЕЛ 2. ТРЕБОВАНИЯ ПО ПРАВИЛАМ СДАЧИ И ПРИЕМКИ

<i>Подраздел 2.1. Порядок сдачи и приемки</i>
В соответствии с разделом 2 проекта Договора.
<i>Подраздел 2.2. Требования по передаче лицензиату технических и иных документов при поставке товаров</i>
В соответствии с разделом 2 проекта Договора.

## РАЗДЕЛ 3. ОБЩИЕ ТРЕБОВАНИЯ

<i>Подраздел 3.1. Назначение ПО</i>
<p>Основное назначение системы контроля доступа привилегированных пользователей (далее – ПО) - решать задачи службы информационной безопасности и ИТ-подразделений организации, связанные с фиксацией и последующим разбором действий, совершенных персоналом с использованием административных учётных записей в информационных системах предприятия.</p> <p>ПО должно обеспечить доступ к серверам, коммутаторам и вести запись всех действий и инцидентов безопасности в журналах ПО для неограниченного количества системных администраторов.</p> <p>ПО должно обеспечивать хранение журналов и записанных сессий системных администраторов в течение не менее 6 месяцев.</p> <p>Лицензия ПО должна поддерживать работу с неограниченным количеством пользователей и конечных устройств (систем) не менее 9 (девяти) конкурентных сессий одновременно.</p>
<i>Подраздел 3.2. Структура ПО</i>
<p>ПО, непосредственно взаимодействующее с защищаемыми информационными системами, должно базироваться на основе сертифицированной отечественной ОС.</p> <p>ПО должно размещаться в функционально-замкнутой среде.</p> <p>ПО должно включать в себя систему контроля доступа. В подсистеме контроля доступа должна быть реализована встроенная система защиты информации, обеспечивающая разграничение доступа ко всем объектам подсистемы, в том числе к журналам сессий, хранящимся в ПО.</p> <p>ПО должно обеспечить защиту обрабатываемой информации от несанкционированного доступа. Защита должна быть реализована и на уровне операционной системы и на уровне программного обеспечения.</p> <p>ПО не понижает надежности смежных систем.</p> <p>ПО управляется из единой консоли.</p>
<i>Подраздел 3.3. Функциональные возможности</i>
<p>ПО должно обеспечивать выполнение следующих функций:</p> <ul style="list-style-type: none"> <li>- работу в режиме шлюза/прокси-сервера без установки агентов на сервера и APM;</li> <li>- поддержку протоколов SSH, RDP, TELNET, VNC, SCP/SFTP, RLOGIN, иметь функциональную возможность работы с консолью через последовательный порт RS-232 или RS-485;</li> <li>- возможность управления компонентами протоколов SSH, RDP, TELNET, VNC, SCP/SFTP, RLOGIN в зависимости от настраиваемых политик соединения;</li> <li>- поддержку клиент-серверных приложений (VMware ESXI, Oracle, MySQL, и т. д.);</li> </ul>

- поддержку административных веб-интерфейсов;
- обеспечение единой точки доступа к серверам (SSO) без добавления дополнительных промежуточных модулей, кроме самого шлюза доступа;
- оптическое распознавание символов в реальном режиме времени (OCR), в т.ч. английского и русского языка;
- анализ вводимой с клавиатуры информации по протоколу RDP;
- анализ передаваемых команд по протоколу SSH;
- режим доступа администратора с предварительным подтверждением от нескольких разных ответственных лиц (более одного подтверждающего, в том числе с распределением секторов ответственности);
- возможность запросить и разрешить доступ в рамках сессии администрирования;
- возможность получения доступа по расписанию;
- резервное сохранение полной конфигурации ПО с возможностью восстановления из резервной копии;
- обеспечение контроля следующих системных параметров ПО:
  1. количества установленных соединений;
  2. протоколов, по которым установлены соединения;
  3. использования оперативной памяти;
  4. использование дискового пространства;
  5. загрузки процессора.
- Использование следующих методов аутентификации:
  1. LDAP;
  2. Kerberos;
  3. RADIUS;
  4. LDAP-AD/LDAPS-AD;
  5. LDAP/LDAPS;
  6. Сертификаты x509;
  7. TACACS+.
- построение политик при помощи визуального интерфейса по протоколу HTTPS;
- отчетность ПО:
  1. История соединений (с возможностью наложения фильтров);
  2. История авторизации (с возможностью наложения фильтров);
  3. Журналы ПО.
- формирование отчетов по действиям привилегированных пользователей при работе с ИТ-инфраструктурой Заказчика с механизмами анализа поведенческой модели пользователей (опционально, возможность расширения системы до данных функций);
- создание ролей пользователей с различным набором прав доступа (не менее трех ролей: администратор, пользователь, аудитор);
- запись видео файлов, содержащих сессии системных

администраторов на серверах;

- формирование списка команд, диалогов и результатов выполнения, как вводимых администратором в рамках сессии, так и возвращаемых администратору от системы в рамках сессии администрирования, с возможностью поиска и сохранения для дальнейшего анализа;

- использование стандартных инструментов администрирования для создания подключения к серверу/сервису (rdp-client, putty, vnc-client);

- при использовании личной учетной записи пользователя должна обеспечиваться публикация готовой ссылки на парольный/беспарольный доступ к ресурсу, в том числе на базе механизма OTP (One-Time Password);

- оперативное оповещение администраторов ИБ о событиях безопасности по протоколу SMTP;

- возможность интеграции с SIEM-системой заказчика, с передачей ей событий о заголовках окон и вводимых команд, выполняемых и завершенных процессах, фактах использования механизма передачи файлов, фактах успешных и неуспешных авторизаций;

- загрузка учетных записей и прав пользователей с использованием протокола web API из других систем контроля доступа;

- возможность интеграции с программными решениями партнерских производителей «Лаборатории Касперского», «Positive Technologies» с помощью готовых плагинов;

- просмотр активных сессий пользователей в режиме реального времени с возможностью принудительного прерывания конкретной сессии пользователя;

- разрыв сессии привилегированного пользователя в автоматическом режиме или оповещение администратора при введении запрещенной команды из заранее созданного списка;

- запись сессий пользователей в журналы событий, как в формате видеозаписи (с контролем ввода с клавиатуры), так и в формате текстового файла с функцией показа ввода и вывода пользовательской команды;

- возможность интеграции с внешними системами средствами встроенного API;

- возможность интеграции с внешними системами для обеспечения доступа к целевым хостам через веб-браузер – SSH и RDP через HTTPs;

- работа как в прозрачном режиме (без ввода пароля на целевой системе), так и с аутентификацией на целевой системе;

- смена паролей на ключевых системах (с использованием парольной политики) без использования ПО третьих производителей;

- возможность предоставлять доступ к просмотру паролей учетных записей в соответствии с политикой;

- поддержка запуска разрешенного перечня приложений в изолированной среде (запуск только приложения, а не полноценной сессии);
- возможность оповещения пользователей системы после аутентификации о дате и времени предыдущего входа, а также о количестве зафиксированных неуспешных попыток с момента последнего успешного входа;
- завершение сеанса пользователя системы после превышения установленного времени бездействия;
- возможность оповещения уполномоченных пользователей системы при переполнении объема памяти, отведенного на хранение записей аудита событий безопасности и данных пользовательских сессий целевых систем, в масштабах времени, близком к реальному;
- запрет любых действий пользователей системы до прохождения ими процедур идентификации и аутентификации;
- возможность восстановления настроек системы и данных пользовательских сессий целевых систем;
- возможность управления сроком хранения записей аудита событий безопасности;
- возможность настройки парольной политики только уполномоченным пользователям;
- возможность управления учетными записями пользователей только уполномоченными пользователями;
- поддержка определенных ролей и их ассоциация с конкретными пользователями;
- возможность оповещения пользователей системы после аутентификации о необходимости соблюдения установленных ограничений на обработку информации;
- возможность оповещения пользователей системы после аутентификации о дате и времени предыдущего входа, а также о количестве зафиксированных неуспешных попыток с момента последнего успешного входа;
- завершение сеанса пользователя системы после превышения установленного времени бездействия;
- запрет любых действий пользователей системы до прохождения ими процедур идентификации и аутентификации;
- возможность расширенного просмотра записей аудита событий безопасности, относящихся к попыткам идентификации и аутентификации пользователей системы, с возможностью поиска, сортировки и фильтрации;
- контроль целостности компонентов системы по их контрольным суммам и возможность восстановления целостности системы при

<p>возникновении нештатных ситуаций;</p> <ul style="list-style-type: none"> <li>- поддержка преобразования групп учетных записей из Microsoft AD на профили доступа в рамках ПО.</li> </ul>
<p><i>Подраздел 3.4. Масштабирование компонентов ПО</i></p>
<ul style="list-style-type: none"> <li>- Возможность реализации отказоустойчивого решения (кластер) средствами ПО API;</li> <li>- Возможность объединения серверов в кластеры;</li> <li>- Поддержка масштабирования системы (вертикальное и горизонтальное масштабирование);</li> <li>- Возможность шифрования записанных сессий на внешних хранилищах;</li> <li>- Возможность хранения записей аудита событий безопасности и данных пользовательских сессий целевых систем в выделенном хранилище;</li> <li>- Поддержка взаимодействия с брокером фермы RDP-серверов Windows версий 2012 и выше;</li> <li>- Возможность длительного хранения записей на подключаемых по сети хранилищах данных по протоколам NFS и CIFS;</li> <li>- Возможность опционального расширения функциональности ПО за счет установки его дополнительных модулей.</li> </ul>
<p><i>Подраздел 3.5. Общие требования к программному обеспечению</i></p>
<p>Предлагаемое к использованию программное обеспечение должно быть включено в реестр Минкомсвязи "Единый реестр российских программ для электронных вычислительных машин и баз данных".</p> <p>Компоненты ПО непосредственно взаимодействующие с защищаемыми информационными системами ИТ-инфраструктуры Заказчика должны иметь сертификат в соответствии с «Требованиями по безопасности информации, устанавливающими уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России) не ниже 4 уровня доверия.</p>

## РАЗДЕЛ 4. ТРЕБОВАНИЯ К КАЧЕСТВУ

<p>Выполнение программным обеспечением функций, согласно сопроводительной документации производителя.</p>
---

## РАЗДЕЛ 5. ТРЕБОВАНИЕ К ФОРМЕ ПРЕДСТАВЛЯЕМОЙ ИНФОРМАЦИИ

<p>Требования к отчетной документации – согласно разделу 3 проекта Договора.</p>
--



## РАЗДЕЛ 6. ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ

№ п/п	Сокращение	Расшифровка сокращения
1.	AD	Active Directory, централизованная стандартная система
2.	LDAP	Протокол доступа к каталогам
3.	RDP	Remote Desktop Protocol- протокол удалённого рабочего стола
4.	SIEM-система	Система мониторинга событий информационной безопасности, предназначенная для анализа информации
5.	SSH	Secure Shell Protocol - это протокол удаленного управления
6.	SSO	Single Sign-One, технология единого входа
7.	APM	Автоматизированное рабочее место
8.	ИБ	Информационная безопасность
9.	ИТ	Информационные технологии
10.	ПО	Программное обеспечение
11.	ЭВМ	Электронно-вычислительная машина

Начальник подразделения 65

Смышляев П.В.