

Перечень требований

Программный продукт: «Защита от несанкционированного привилегированного доступа (РАМ)» – программный продукт «Indeed Privileged Access Manager» версии, сертифицированной в Республике Беларусь, или аналог (далее – ПО) должен поставляться в комплекте с документацией в электронном или печатном виде на русском языке. Документация должна включать в себя правила установки и использования ПО (руководства администратора и пользователя).

Исполнитель должен передать Заказчику права на обновление и техническую поддержку (гарантийное сопровождение) ПО сроком 5 (пять) лет, провести обучение сотрудников Заказчика правилам эксплуатации системы РАМ.

ПО должно иметь действующий сертификат соответствия требованиям Технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY).

Наличие гарантийного письма от производителя, свидетельствующее о том что производитель ПО обязуется предоставлять доступ к обновлениям в течении 5 лет, а также гарантирующее не накладывать запрет на экспорт в Беларусь своего ПО в течении 5 лет, а в случае запрета экспорта или неокказание технической поддержки гарантирует возврат денежных средств затраченных на ПО.

Конфигурация ПО:

неисключительные права на программы для ЭВМ Indeed Access Manager и Indeed Privileged Access Manager;

неисключительные права на дополнительные функциональные возможности Модулей Windows Logon и NPS RADIUS Extension для программы Indeed Access Manager;

ПО для 75 пользователей с неограниченным количеством сессий.

Предложение должно быть представлено и детально описано в объеме, достаточном для понимания предлагаемого решения. Материалы должны быть представлены в таком виде и содержать информацию необходимую для понимания, что предложение соответствует настоящим требованиям.

Участник процедуры закупки обязан предоставить в электронном виде либо на электронном носителе информации копии имеющейся технической документации на компоненты системы в целом.

Требования к ПО

Система РАМ должна предоставлять возможность организации привилегированного доступа к целевым системам с использованием двухфакторной аутентификации, а также контроля и фиксации (записи и хранения сеансов удаленного доступа администрирующего персонала и внешних подрядчиков) активности сотрудников в режиме реального времени и возможностью управления доступом пользователей к информационным ресурсам в соответствии с действующими политиками безопасности с одновременным упрощением и повышением безопасности процедуры аутентификации.

Необходимо обеспечить удаленный доступ сотрудников с использованием современных методов строгой и многофакторной аутентификации. Дальнейшее подключение к целевым серверам системы РАМ осуществляется на основе жестко заданного списка доступных целевых узлов.

Система РАМ должна обеспечивать:

- инсталляцию как на Linux, так и Windows;
- обнаружение неконтролируемых локальных привилегированных учетных записей на целевых ресурсах и их импорт в хранилище РАМ;
- предотвращение попыток несанкционированных действий в отношении конфиденциальных сведений;
- снижение риска утечки данных;
- контролируемый доступ к инфраструктуре организации посредством единой точки входа для 75 привилегированных пользователей;
- анализ поведения пользователей в реальном режиме времени;
- предотвращение сбоев в информационных системах, которые могут произойти по вине привилегированных пользователей;
- непрерывное фиксирование событий безопасности и прочих артефактов привилегированных сессий, запись действий пользователей в централизованное хранилище, оповещение администраторов РАМ.

Система РАМ должна являться единой точкой доступа привилегированных пользователей к информационным ресурсам организации, осуществляющая следующие задачи защиты и контроля привилегированного доступа:

- непрерывная запись действий привилегированных пользователей в рамках рабочих сессий, сохранение данных для аудитов и расследований;
- фиксация логов и видео действий привилегированных пользователей (все либо что-то одно на выбор);

логирование событий безопасности и прочих артефактов привилегированных сессий в централизованном хранилище (на PostgreSQL или MSSQL);

фиксирование в журнале сессий попыток использования привилегированных учетных записей (идентификация сотрудника и конкретной учетной записи, к которой был получен доступ);

фиксация даты и времени получения доступа;

видео- и текстовая запись сессий привилегированного доступа, сохранение снимков экрана и передаваемых файлов на конечные ресурсы в журнале сессий;

возможность настройки разрыва сессий в случае неактивности пользователя;

возможность ограничения повышенных привилегий для SSH;

возможность прекращения сессии администратором с участием привилегированных пользователей при подозрении на несанкционированные действия;

обеспечение двухфакторной аутентификации сотрудников при доступе к привилегированным учетным записям (в качестве первого фактора используется логин и пароль учетной записи из каталога AD, в качестве второго фактора используется eToken Pass (портативное устройство строгой аутентификации с использованием одноразовых паролей, поставляется в комплекте с ПО и входит в его стоимость);

наличие подсистемы работы с собственными типами сервисных подключений (для создания кастомных подключений);

проксирование SQL сессий для PostgreSQL;

проверка ключей ресурса на ssh-проxy;

отправка событий журнала безопасности в систему мониторинга и корреляции событий безопасности по протоколу syslog;

отправка любого типа событий журнала на электронную почту администраторов РАМ;

управление настройками паролей пользователей на основании настроенных политик;

наличие Web Wizard (для установки обновления и настройки конфигурации РАМ).

Во время эксплуатации система РАМ должна быть защищена от воздействия на нее со стороны прочих систем.

Система РАМ должна поддерживать следующие типы учетных записей:

Microsoft Active Directory;

учетные записи ОС Windows;

учетные записи ОС Linux (пароли и SSH-ключи);

учетные записи для доступа к сетевому оборудованию.

Система РАМ должна поддерживать следующие протоколы доступа к целевым ресурсам:

RDP – для Windows серверов;

SSH – для серверов и оборудования, работающего на базе различных дистрибутивов Linux и Unix;

HTTP(s) – для целевых веб-приложений (например, для конфигурирования сетевого оборудования);

SCP, SFTP – протоколы, используемые для безопасной передачи файлов данных между хостами.

Требования по вводу системы РАМ в эксплуатацию

В ходе развертывания и эксплуатации компонентов системы не должно вноситься никаких изменений в схемы Заказчика.

В рамках поставки лицензий системы РАМ должны быть выполнены следующие работы:

Установка ПО системы РАМ;

Настройка системы РАМ, включая:

настройку ролевой модели доступа в систему РАМ (добавление пользователей и настройка ролей для них);

настройку контролируемых подключений к ресурсам (к сетевому оборудованию, серверам);

настройку передачи в соответствии с требованиями действующего законодательства РБ в SIEM-систему событий, имеющих свой уникальный идентификатор:

состоянии системы РАМ;

доступа администраторов и пользователей к системе РАМ;

изменения настроек системы РАМ;

удачного и неудачного доступа к информационным системам организации.

На этапе ввода системы в эксплуатацию по заявке Заказчика возможна настройка передачи на SIEM-систему дополнительных событий.

Исполнитель должен провести обучение сотрудников (пользователей и персонала сопровождения (администрирования)) правилам эксплуатации системы. Обучение проводится поэтапно, по мере необходимости и готовности системы. Предварительный график, программа и условия обучения сотрудников предоставляются Исполнителем и согласовываются с Заказчиком на этапе подготовки системы к внедрению.

Обучение сотрудников (пользователей по работе с инструментарием

системы (в разрезе их функций)) проводиться на площадях Заказчика. Количество обучаемых – не менее 4 человек. Продолжительность обучения – не менее 40 часов.

Обучение сотрудников производится в ходе осуществления работ по вводу в эксплуатацию.

Сотрудникам, прошедшим обучение, должен быть выдан документ, подтверждающий прохождение обучения.

Параметры технической поддержки (гарантийных обязательств)

Техническая поддержка (гарантийные обязательства) включают услуги, которые оказываются Заказчику на постоянной основе на весь срок действия технической поддержки (гарантийных обязательств) и направлены на:

- предоставление консультаций по вопросам эксплуатации, связанных с ошибками системы, некорректной работой функций системы;

- устранение ошибок функционирования системы и ее восстановление после критических ошибок;

- уведомление о выходе новых версий и исправлений (патчей);

- поставка исправлений (патчей);

- своевременное предоставление новых версий (обновлений);

- корректировка форм документов, отчетов, функций при изменении законодательных и/или отраслевых требований;

- предоставление информационной поддержки: оказание консультаций по функциональным возможностям системы, проведение вебинаров, тренингов (по предварительному согласованию), предоставление сопроводительной документации на систему.

Обновление системы или ее отдельных модулей (включая внедрение новых) должно производиться после процедуры тестирования. При этом, должна быть обеспечена сохранность дополнений и изменений, внесенных Заказчиком самостоятельно за период с предыдущего обновления.

Исполнитель должен обеспечить услуги по технической поддержке сроком не менее 5 (пяти) лет с момента ввода системы в эксплуатацию.

Исполнитель должен определить единый контактный центр для обращения в период оказания технической поддержки (гарантийных обязательств) по любым вопросам, связанным: с эксплуатацией системы, некорректной работой функций системы, заявленных в сопроводительной документации к системе.

Прием обращений в службу технической поддержки должен осуществляться по телефону в рабочие дни с 08:30 по 17:30 и в круглосуточном режиме по электронной почте или Web-портал Service

desk (автоматическая регистрация заявок, выделенный менеджер).

Процедура обслуживания заявок:

Открытие заявок осуществляется Заказчиком в режиме 24x7 (по телефону и/или через web-портал, и/или по электронной почте, и/или мессенджер).

Время оказания услуг считается со времени регистрации заявки до ее полного закрытия.

Оказание услуг осуществляется в соответствии с параметрами, указанными в таблице №1.

Таблица № 1

Приоритет	Время реакции	Продолжительность решения проблемы	Периодичность информирования заказчика о ходе решения проблемы
Приоритет 1. Критично	≤ 30 мин	не более 6 часов*	1 раз в час
Приоритет 2. Срочно	≤ 1 часа	не более 12 часов	1 раз в 3 часа
Приоритет 3. Некритично	≤ 4 рабочих часов	не более 3 рабочих дней	по запросу Заказчика и по факту решения проблемы
Приоритет 4. Консультация	Следующий рабочий день	не учитывается	по запросу Заказчика

*Время корректируется по итогам выбора исполнителя услуги, согласно предложениям участников.

Оценка приоритета осуществляется согласно таблице № 2.

Таблица № 2

Приоритет	Описание
Критично	Сбой непосредственно влияет на работу компании и несет экономические потери для компании
Срочно	Сбой непосредственно влияет на работу компании и/или может привести к экономическим и репутационным рискам.
Некритично/Консультация	Сбой, который влияет на работу компании, но не влияет на экономические или репутационные риски.

В случае аварийной ситуации со статусом «Критично» Исполнитель должен иметь возможность в нерабочее время оказать услуги Заказчику по телефону, на русском языке и/или на месте установки оборудования.

По запросу Исполнителя, Заказчик может предоставить дополнительную диагностическую информацию для локализации неисправности или причин некорректной работы программного

обеспечения.

По результатам обработки полученной информации Исполнитель по электронной почте направляет Заказчику заключение о характере сбоя.

При сбое, вызванном ошибкой в работе программного обеспечения, Исполнитель обязан предоставить Заказчику новую версию ПО (по мере выпуска производителем), устраняющую ошибку в работе или предложить Заказчику рекомендации по временному решению проблемы.

При не предоставлении Исполнителем Заказчику информации о ходе решения проблемы в течение периода, указанного в таблице № 1, заявка считается не выполненной.