ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ

по закупке № 204648

способом «Открытый тендер на понижение»

Лот № 561296

Заказчик: Акционерное общество "Национальная атомная компания "Казатомпром"

Организатор: Акционерное общество "Национальная атомная компания "Казатомпром"

1. **Краткое описание ТРУ**

Наименование	**Значение**
Номер строки	39-1 Р
Наименование и краткая характеристика	Комплексные работы в сфере информационных технологий «под ключ», Комплексные работы в сфере информационных технологий «под ключ», включающая: поставку программного обеспечения, консалтинговые услуги по внедрению информационной системы и поставку оборудования (при необходимости)
Дополнительная характеристика	Система «Центр контроля информационной безопасности Р-Вижн: комплекс «SGRC»
Количество	1
Цена за единицу	29 087 293.75
Единица измерения	-
Сумма, без НДС	29 087 293.75
Место поставки	КАЗАХСТАН, г.Астана, г. Астана ул. Кунаева 10
Условия поставки	-
Срок поставки	С даты подписания договора в течение 120 рабочих дней
Условия оплаты	Окончательный платеж - 100%, Промежуточный платеж - 0%, Предоплата - 0%

2. **Описание и требуемые функциональные, технические, качественные и эксплуатационные характеристики**

Техническая спецификация

1.Перечень и место проведения работ.

Наименование: Лицензия на право использования программного обеспечения, включая техническую поддержку от вендора сроком 12 месяцев, кол-во -1 шт.;

Наименование: Внедрение системы «Центр контроля информационной безопасности», кол-во -1 работа;

Наименование: Обучение пользователей, кол-во -1 работа;

Место проведения работ г. Астана.

2.Требования к Подрядчику.

Подрядчик должен предоставить авторизационное письмо от производителя программного обеспечения или официального представителя на территории Республики Казахстан.

Срок гарантии: 12 месяцев с даты подписания договора.

3.Назначение и цели создания системы

3.1.Назначение системы

Центр контроля информационной безопасности (далее Система) предназначена для автоматизации процесса менеджмента ИБ в соответствии с бизнес-целями Общества, обеспечения интегрированного целостного подхода к управлению информационной безопасностью (Governance), управлению рисками ИБ (Risk Management) и контролю соответствия отраслевым и законодательным требованиям (Compliance) через взаимосвязь стратегии, процессов, технологий и человеческих ресурсов.

3.2.Цели и задачи выполнения работ

Целями создания Системы является:

снижение уровня финансовых рисков, связанных с ИБ, путем их идентификации, оценки и обработки, в том числе за счет принятия адекватных защитных мер;

планирование расходов на информационную безопасность;

повышение общей эффективности ИБ в организации за счет достижения комплексности, взаимосвязанности и прозрачности всех мер ИБ;

контроль состояния ИБ в Обществе.

В результате внедрения Системы должны быть решены следующие задачи:

мониторинг и отслеживание изменений ИТ-инфраструктуры, выявление оборудования и сбор данных о его характеристиках;

инвентаризация компонентов информационных систем;

учет материальных и нематериальных активов и их взаимосвязей;

контроль структуры и состава компонентов ИТ-инфраструктуры;

формирование перечня критических активов и проведение оценки их ценности;

организация совместной работы различных групп специалистов и экспертов, участвующих в процессе оценки рисков ИБ, проведения аудитов, хранение всей информации в единой базе данных;

оценка степени вероятности реализации угроз ИБ и тяжести последствий с прогнозированием возможного ущерба;

формирование модели угроз и модели нарушителя ИБ;

проведение оценки рисков информационной безопасности;

составление плана мероприятий по обработке рисков, исходя из имеющегося бюджета на информационную безопасность;

подготовка документов, фиксирующих результаты оценки рисков ИБ;

оценка соответствия корпоративным, отраслевым и международным стандартам;

обеспечение учета реализованных и запланированных мероприятий по информационной безопасности, разработанных нормативных документов, актуальных замечаний по системе защиты и проводимых аудитов ИБ;

автоматизированная оценка выполнения различных нормативных и законодательных требований и хранение истории проведенных оценок для отслеживания изменений;

управление операционными задачами персонала с возможностью автоматического создания и оперативного уведомления об инцидентах ИБ;

формирование пакета отчетных документов по состоянию системы информационной безопасности, реализованным мероприятиям, а также по результатам проводимых периодических оценок рисков ИБ и аудитов ИБ.

4.Требования к архитектуре системы

2.1.Архитектура решения

В состав Системы должны входить следующие компоненты:

сервер – виртуальное устройство, которое обеспечивает централизованное управление компонентами Системы, обеспечивает взаимодействие с пользователями Системы, осуществляет сбор, хранение и предоставление информации в различных форматах;

коллектор – виртуальное устройство, которое обеспечивает инвентаризацию (сбор сведений) по отдельным сегментам ИТ-инфраструктуры с последующей передачей данных на сервер;

АРМ пользователя – АРМ, с которого посредством веб-консоли осуществляется доступ пользователей и администраторов к Системе.

Система должна поставляться в виде преднастроенного образа виртуальной машины,

функционирующего в следующих средах виртуализации: VMWare.

Допускается совмещение сервера и коллектора в едином виртуальном устройстве.

Состав компонентов, расположение мест установки компонентов Системы может быть уточнен на этапе технического проектирования Системы.При масштабировании Система не должна предполагать использования дополнительного коммерческого ПО.

Компоненты Системы должны функционировать на базе ОС Linux, в том числе Ubuntu 14.04 LTS, Ubuntu 16.04 LTS, CentOS 7, RHEL 7;

В качестве СУБД Системы должна использоваться PostgreSQL v.10 и выше.

Требования к вычислительной части (при размещении БД и коллектора на той же виртуальной машине, в которой функционирует сервер):

Характеристика: Процессор: 8vCPU, 2 ГГц; Память: 16 Гб; Дисковое пространство: 500 ГБ

2.2.Состав и краткое описание модулей системы

В состав Системы должны входить следующие функциональны блоки:

Блок сопряжения с внешними системами.

Блок управления активами.

Блок управления рисками ИБ.

Блок управления инцидентами ИБ.

Блок управления аудитами ИБ.

Блок управления задачами.

Блок управления документами ИБ.

Блок визуализации.

Блок отчётности.

Блок централизованного управления.

Блок сопряжения с внешними системами должен обеспечивать интеграцию Системы с внешними системами: сетевыми средствами защиты; с почтовыми серверами Microsoft Exchange; системами идентификации и аутентификации, сканерами защищенности, поставщиками инвентаризационной информации об ИТ-инфраструктуре (ITSM/CMDB-системами), Центром управления McAfee ePO, SIEM системой McAfee ESM, средствами антивирусной защиты и др. системами.Блок управления активами должен обеспечивать проведение инвентаризации сети с целью обнаружения устройств, контроля состояния ИТ-инфраструктуры, управления жизненным циклом активов и их взаимосвязями.Блок управления уязвимостями должен обеспечивать централизованный сбор и учет сведений по обнаруженным уязвимостям, а также управление задачами по устранению уязвимостей на объектах ИТ-инфраструктуры.

Блок управления рисками ИБ должен обеспечивать возможность формирования перечня актуальных рисков и плана их обработки. Блок управления аудитами ИБ должен обеспечивать автоматизацию контроля и оценки соответствия организации требованиям различных нормативных правовых актов и стандартов в области информационной безопасности.Блок управления задачами должен обеспечивать управление задачами, проводимыми в рамках деятельности по управлению ИБ и иметь средства контроля их исполнения.

Блок визуализации должен обеспечивать визуализацию информации в различных форматах представления данных, включая графики, интерактивные схемы. Блок централизованного управления должен обеспечивать настройку параметров работы составных компонентов Системы.

Блок управления документами должен обеспечивать хранение документов, обеспечивать контроль срока действия документов и разграничивать доступ пользователей Системы к документам.

Система должна содержать инструкции и руководства пользователя на русском языке с возможностью осуществления поиска.

Взаимодействие пользователей с Системой должно осуществляться посредством визуального графического интерфейса на основе веб-технологий.

Блок управления отчётностью должен обеспечивать возможность формирования различной отчётности.

2.3.Требования к способам и средствам связи для информационного обмена между компонентами Системы

Система должна поддерживать применение защищенных протоколов передачи данных между составными компонентами.

При взаимодействии с контролируемыми узлами должны применяться следующие протоколы, указанные ниже:
Перечень протоколов взаимодействия между компонентами Системы и смежными системами. Наименование объекта: WMI;
Протокол взаимодействия: DCE/RCP;
Сетевые порты: 135, >1024;
Характеристики объекта: Номера портов RPC присваиваются автоматически.

Наименование объекта: NetBIOS;
Протокол взаимодействия: CIFS/SMB;
Сетевые порты: 445 TCP/UDP;
Характеристики объекта: Поддерживаются устаревшие клиенты (137-139 TCP/UDP)

Наименование объекта: LDAP;
Протокол взаимодействия: LDAP;
Сетевые порты: 389,636 TCP
Характеристики объекта:

Наименование объекта: SSH;
Протокол взаимодействия: SSH;
Сетевые порты: 22 TCP;
Характеристики объекта: Стандартный порт. Может быть изменен;

Наименование объекта: Telnet;
Протокол взаимодействия: Telnet;
Сетевые порты: 23 TCP;
Характеристики объекта: Стандартный порт. Может быть изменен.

Наименование объекта: SMTP;
Протокол взаимодействия: SMTP;
Сетевые порты: 25 TCP;
Характеристики объекта: Стандартный порт. Может быть изменен.

Наименование объекта: MS SQL;
Протокол взаимодействия: Microsoft SQL, Server SMB;
Сетевые порты: 1433 TCP, 445 TCP;
Характеристики объекта: Зависит от настоек сервера

Наименование объекта: Компоненты системы;

Протокол взаимодействия: SSL;

Сетевые порты: 80 TCP, 3001 TCP;

Характеристики объекта: Стандартный порт. Может быть изменен.

2.4.Требования к функциональному блоку управления Активами

Блок управления активами должен обеспечивать реализацию следующих функций:

Сбор, регистрация, обогащение и агрегация информации по активам с различных источников в единой системе.

Ведение и учет карточек активов, включающих общие сведения об активе, список ответственных лиц, связанные активы и документы из общей базы (с возможным комментарием), а также другую информацию, связанную с активами.

Учет материальных и нематериальных активов и их взаимосвязей (процессы, информация, информационные системы, сети, оборудование, пользователи, группы ИТ-активов).

Управление жизненным циклом ИТ-активов.

Возможность автоматически помечать и удалять из системы устаревшее оборудование/персонал. Параметр устаревания позволяет определить оборудование и учетные записи пользователей, сведения о которых не обновлялись при сканировании в течение заданного периода времени. Также в системе наглядно отображается статистика по количеству устаревших учетных записей пользователей и оборудования.

Возможность настраивать собственные поля для описания активов.

Возможность назначения тегов в поля карточки описании актива.

Наличие предустановленных справочников, описывающих активы, с возможностью их редактирования (типы оборудования, бизнес-процессы, группы ПО, теги, статусы оборудования, атрибуты безопасности, локации, типы подразделений).

Наличие в карточке описании актива поля, отображающего статус инвентаризации, содержащего описание ошибки инвентаризации или статус ее успешного прохождения.

Возможность привязки актива к населенному пункту, содержащему географические координаты («Локация»).

Автоматическое заполнение поля «Локация» для группы ИТ-активов и сетей на основе информации от входящих в их состав узлов.

Возможность добавления в базу данных документов, относящихся к активам, и возможность добавления к активам документов из общей базы.

Возможность настройки отображаемой информации в списках активов, в том числе включение/отключение отображения иерархической структуры для Бизнес-процессов и Групп ИТ-активов.

Возможность группировки выявленных ИТ-активов и ПО.

Возможность учета сроков действия лицензий для ПО.

Возможность присвоения инвентарных номеров оборудованию по шаблону.

Инвентаризация (сканирование) ИТ-инфраструктуры без применения агентов.

Поддержка сканирования следующих Операционных систем (далее – ОС): Windows, Linux/Unix, Mac OS, сетевого оборудования Cisco, Juniper, HP функционирующих на базе ОС H3C Comware - средствами самой Системы.

Возможность создания многоуровневых элементов для описания организационной структуры организации и места размещения компонентов ИТ-инфраструктуры (характеристики помещения).

Возможность группового запуска скриптов автоматизации.

Наличие функционала, позволяющего работать с привилегиями пользователей. Возможность автоматически выявлять привилегии пользователей, используя данные учетных записей Active Directory. Выявление пользователей с правами администраторов на оборудовании, пользователей, обладающих излишними правами, а также учет привилегий, определяемых пользователем вручную.

Инвентаризация узлов с ОС Windows с использованием VBS-скриптов.

Сбор сведений по сканируемым узлам: IP-адрес, тип ОС, основные технические параметры оборудования (данные о процессоре, объеме ОЗУ, дисковой подсистеме и их использование на сканируемом хосте), перечень установленного программного обеспечения, перечень пользователей, параметры безопасности (для Windows систем статусы включен/выключен: персональный МЭ, USB-порт; система автоматического обновления ОС, встроенное САЗ).

Возможность отображения статуса работы хостового агента стороннего средства защиты (при интеграции с СЗИ).

Возможность одновременного выбора и запуска сканирования нескольких сетей.

Поддержка сканирования по расписанию.

Возможность группового ручного запуска сетей на сканирование с разными коллекторами и параллельное сканирование сетей разными коллекторами в рамках политики сканирования.

Обеспечение контроля структуры и состава компонентов ИТ-инфраструктуры (появление новых устройств, установка или удаление программного обеспечения, изменение параметров безопасности, появление новых пользователей).

Сканирование ИТ-инфраструктуры должно выполняться в соответствии со следующим алгоритмом:

1.пользователь вносит в Систему сведения об учетных записях (Windows, SSH, MAC), используемых для сбора данных в процессе сканирования, и добавляет в Систему сети или отдельные узлы, для которых необходимо собрать данные по инфраструктуре;

2.после получения команды на проведение сканирования Система осуществляет первоначальное обнаружение оборудования и сканирование портов;

3.после обнаружения оборудования производится попытка доступа к узлам и сбор необходимых сведений за счет таких инструментов, как WMI и доступ к реестру (для Windows систем), сбор данных путем запуска системных команд по протоколу SSH (для Linux/Unix-систем, Mac OS, сетевого оборудования Cisco, Juniper, HP);

4.в случае обнаружения на оборудовании дополнительных сетевых интерфейсов, подключенных к сетям, сведения о которых еще не внесены в перечень в базе Системы, сведения о дополнительных сетях записываются в базу и отображаются пользователю с целью принятия решения о необходимости их инвентаризации. Таким образом, должна быть возможность поэтапного обнаружения компонентов сетевой инфраструктуры, а также обнаружения несанкционированных сетей и сетевых сегментов;

5.последующая инвентаризация должна проводиться либо путем ручного запуска сканирования, либо путем настройки соответствующих политик сканирования, позволяющих выполнять автоматическую инвентаризацию в соответствии с заданным расписанием.

Возможность отправки по электронной почте уведомлений пользователям о зафиксированных изменениях в активах (нахождение нового оборудования, нового ПО или пользователя, новых уязвимостей, новых сетей, устранения уязвимостей, в случае, если закончились инвентарные номера для присвоения оборудованию, уведомление об исчезновении оборудования (удалено оборудование)). При этом для уведомления пользователей должна обеспечиваться возможность их автоматической настройки.

Возможность сокрытия некоторых групп пользователей в Системе: заблокированных, системных и нераспознанных учётных записей.

Возможность группового удаления подсетей.

Возможность группового редактирования дополнительных полей активов.

Отображение критичности в виде цветовой схемы в разделах Бизнес-процессы, Информация и Группы ИТ-активов.

Возможность просматривать карты сетей (схемы, отображающие оборудование и сети, входящие в состав группы ИТ-активов) и схемы взаимосвязей (схемы, отображающая связанные объекты) для групп ИТ-активов.

Возможность автоматического включения ПО в группы по настроенным правилам.

Возможность настройки исключений для Групп ПО для более точной настройки правил привязки ПО к Группам ПО.

Возможность поиска ПО в заданных директориях, а также в профилях индивидуальных пользователей.

Возможность отображения таблицы найденного ПО в виде дерева. ПО должно группироваться по версиям, должна быть возможность редактировать сразу все элементы группы.

Отображение в истории актива источника добавления актива.

Возможность автоматического включения найденного оборудования в группы ИТ-активов по настроенным правилам. В качестве критерия включения должны быть следующие характеристики: структурное подразделение, найденное ПО на данном оборудовании, домен, рабочая группа, пользователи данного оборудования, помещение, к которому прикреплено данное оборудование, тег, тип оборудования, принадлежность к определенной сети.

Автоматическое удаление политик назначения групп ИТ-активов с оборудования, если условие назначения перестало выполняться.

Возможность удаленного подключения по протоколу RDP к проинвентаризированным Системой узлам Windows.

Возможность удаленного доступа по протоколу SSH к проинвентаризированным Системой Linux-узлам и оборудованию.

Обеспечение автоматического назначения владельцев, администраторов и аудиторов безопасности группы ИТ-активов тому оборудованию, которое входит в эту группу.

Автоматическая привязка сетей к группам ИТ-активов, в которые входят узлы из этой группы.

Автоматическая привязка Группы ИТ-активов к элементам организационной структуры при связывании оборудования из Группы с этим элементом.

Автоматическое удаление политик назначения групп ИТ-активов с оборудования, если условие назначения

перестало выполняться.

Возможность при получении данных через интеграции обновлять информацию по существующему узлу без создания нового узла при наличии дубликатов узлов во внешней системе.

Автоматическая привязка администраторов безопасности сети к входящему в нее оборудованию.

Возможность интеграции с внешними системами – поставщиками инвентаризационной информации (ITSM/CMDB – системы, сканеры защищенности, средства антивирусной защиты, средства защиты от НСД и др.).

Возможность импорта из Excel данных по сетям и оборудованию. При этом должна осуществляться проверка на дублирование сетей и оборудования.

Возможность формирования необходимых отчетных документов (паспортов сетей, систем и помещений, перечней активов, сводных отчетов) и выгрузка в docx, pdf или графический формат для схем.

Возможность экспорта в Excel данных по активам с учетом текущей настройки столбцов, их фильтров и сортировки.

Наличие журнала по активам. Запись источника добавления актива в журнал актива.

Возможность разграничения доступа к Активам на основании роли пользователя.

Возможность сортировки и фильтрации списка активов по различным полям. Возможность индивидуальной настройки списка активов для каждого заданного пользователем фильтра.

Возможность сохранить фильтры в функциональном блоке «Активы» для каждой учетной записи в Системе.

2.5.Требования к функциональному блоку управления рисками

Блок управления рисками ИБ должен обеспечивать реализацию следующих функций:

Возможность проведения оценки рисков информационной безопасности разного масштаба (для отдельных проектов, активов, прикладных систем, бизнес-процессов).

Наличие гибкой и настраиваемой схемы оценки рисков, которая может быть адаптирована под конкретную модель, используемую в Организации. Должна быть возможность задавать математический алгоритм оценки. Параметры алгоритма должны быть качественными (с возможностью проставлять их вручную, выбирать из списка или определять, исходя из заполненной таблицы) или количественными (с возможностью проставлять их вручную, выбирать из списка или рассчитывать согласно математической формуле).

Возможность настройки каталогов угроз. Должна быть возможность добавлять в базу данных системы источники угроз, предпосылки к их реализации и защитные меры.

Возможность связать угрозу с нарушаемыми атрибутами безопасности актива, а также с источниками угроз (потенциал источника для каждой угрозы может настраиваться), предпосылками к реализации (достаточность предпосылок для реализации каждой угрозы может настраиваться) и защитными мерами (потенциал защитных мер для каждой угрозы может настраиваться).

Возможность копировать существующие в системе каталоги угроз.

Составление перечня активов, входящих в область оценки рисков, и определение их ценности.

Возможность указывать эффективность мероприятия в свойствах риска.

Наличие предустановленных справочников: содержащих источники угроз, предпосылки к их реализации и защитные меры с возможностью добавления в базу данных Системы собственных.

Возможность оценки степени вероятности реализации угроз ИБ и тяжести последствий с прогнозированием возможного ущерба.

Возможность выбора одной из предустановленных в Системе методик оценки рисков и возможность адаптации под конкретную модель, используемую в организации.

Учет производных рисков (в случае, если ценность одного актива влияет на ценность другого актива).

Наличие в Системе различных баз угроз (ISO и др.), возможность формирования модели угроз и модели нарушителя.

Возможность формирования плана обработки рисков на определенный период и его сопоставление с имеющимся бюджетом на информационную безопасность.

Возможность фиксирования создаваемой оценки рисков ИБ для обеспечения анализа изменений отдельных рисков.

Возможность оценивать необходимость и целесообразность применения организационных и технических мер для обработки недопустимых рисков на основе анализа рисков ИБ.

Возможность связи различных атрибутов безопасности и активов (при нарушении свойств какого-либо атрибута (атрибутов) одного актива нарушаются атрибут (ы) другого).

Возможность настройки фильтров в реестре рисков.

Возможность привлечения экспертов для оценки отдельных назначенных им рисков;

Автоматический пересчет параметров риска при удалении всех назначенных на него экспертов.

Возможность прикреплять документы и оставлять комментарии к мероприятиям по обработке рисков (внутри оценки и в общем плане).

Визуальное представление информации по текущим рискам информационной безопасности и схемам обработки рисков (графики).

Учет всех мероприятий по управлению рисками (журналирование).

Подготовка документов, фиксирующих результаты оценки рисков (сводный реестр рисков, план обработки рисков и т.д.).

Возможность учета сведений о реализованных защитных мерах при оценке рисков.

Возможность ведения базы защитных мер с возможностью их привязки к группам ИТ-активов, на которых они реализованы.

Автоматический пересчет параметров риска при удалении всех назначенных на него экспертов.

2.6.Требования к функциональному блоку управления инцидентами

Блок управления инцидентами должен обеспечивать реализацию следующих функций:

Блок управления инцидентами должен обеспечивать реализацию следующих функций:

Сбор, регистрация, обогащение и агрегация информации по всем инцидентам ИБ с различных источников в единой системе.

Ведение и учет карточек-описаний инцидентов, содержащих сведения по инцидентам, свидетельства и другую информацию.

Возможность реализации полного цикла обработки инцидентов в соответствии с заданными в организации процедурами.

Формирование карточек инцидентов как в автоматическом, так и ручном режиме и их хранение.

Управление жизненным циклом инцидентов: регистрация, классификация, приоритезация инцидентов по степени критичности в автоматическом или ручном режиме.

Возможность конструирования формы описания инцидента (карточки инцидента) с возможностью добавления следующих типов полей: числовое поле, текстовое поле, несколько текстовых строк, выпадающий список, числовое поле с денежным символом, дата, время, чек-бокс.

Возможность назначения тегов в поля карточки инцидента. Теги должны быть доступны для использования при интеграции с внешними системами для сбора событий и инцидентов ИБ.

Наличие в карточке-описании инцидента поля, фиксирующего дату и время последнего изменения в инциденте.

Наличие в карточке-описании инцидента поля, в качестве значения которого указывается ответственный пользователь ПО.

Возможность производить индивидуальную настройку состава и свойств полей карточки инцидента для каждой категории инцидентов:

1.обязательность заполнения поля (без заполнения указанного поля ПО не должно позволять закрыть инцидент).

2.возможность ограничения доступа к полю;

3.отображение поля в составе основных или дополнительных полей.

Возможность гранулярного разграничения доступа вплоть до полей в карточке инцидента.

Наличие логической составляющей привязки полей к типам инцидента.

Наличие предустановленных справочников с возможностью их редактирования, содержащих как минимум следующую информацию по инцидентам ИБ: типы инцидентов, способы реализации, причины возникновения, последствия инцидента, действия по инциденту, шаблоны инцидентов, уровни критичности, уровни ущерба, источник инцидента, степень преднамеренности, статус реализации, вероятность повторного возникновения, приоритет, статус инцидента.

Возможность добавления и хранения комментариев (командный чат) и подгружаемой информации по инцидентам в единой базе данных.

Автоматическое обновление раздела комментариев к инциденту при добавлении нового комментария одним из пользователей.

Возможность прикреплять к инциденту или событию ИБ свидетельства, содержащие дополнительные сведения (материалы расследования, файлы) и автоматический расчет контрольной суммы этих файлов (MD5, SHA-1).

Возможность скачивать сразу все свидетельства, прикреплённые к инциденту, в виде архива.

Присвоение каждому инциденту индивидуальной ссылки, обеспечивающей возможность перехода на определенный инцидент из рассылаемых пользователям уведомлений, а также других интерфейсных элементов ПО.

Возможность сортировки и фильтрации списка инцидентов по различным полям. Возможность индивидуальной

настройки списка инцидентов для каждого заданного пользователем фильтра.

Возможность сохранить фильтры для каждой учетной записи (для каждого пользователя ПО).

Возможность создания нескольких циклов обработки инцидентов для разных категорий инцидентов для повышения гибкости настройки порядка реагирования на инциденты.

Возможность создавать новые инциденты путем копирования уже существующих.

Возможность создания инцидентов на основании предзаполненных шаблонов.

Регистрация инцидентов и заполнение карточки инцидента вручную оператором (пользователем) ПО через веб-интерфейс.

Возможность автоматической регистрации и обработки инцидентов ИБ посредством разбора syslog-файла, содержащего информацию по инцидентам.

Автоматическая регистрация и обработка инцидентов ИБ, поступающих с SIEM-систем через API-интерфейс, поддержка двухстороннего обмена данными - синхронизация статуса инцидента (нарушения) в SIEM при его закрытии в подсистеме управления инцидентами.

Автоматическая регистрация и обработка инцидентов ИБ посредством интеграции с почтовым сервером путем парсинга почтовых сообщений с указанного ящика электронной почты по тегам или регулярным выражениям.

Возможность использования регулярных выражений JavaScript для парсинга писем от сторонних систем.

Наличие встроенного обработчика электронной почты и возможность приема почтовых сообщений по протоколу SMTP с последующим парсингом сообщений по тегам или регулярным выражениям.

Возможность настройки правил авто заполнения полей карточки инцидента. В качестве критериев для настройки правила должно фигурировать значение определённого поля или логического условия.

Возможность автоматического выставления даты/времени выявления инцидента при его создании.

Возможность присвоения категории и типа инцидента по почтовому адресу отправителя письма при интеграции с почтовой системой.

Возможность отображения поля инцидента только, если в нем есть данные.

Возможность фильтровать список инцидентов по отсутствию каких-либо значений в свойствах инцидента.

Автоматизация реагирования на инциденты, выполнение следующих действий:

1.уведомление пользователей;

2.назначение ответственных лиц;

3.модификация инцидента (модификация полей карточки инцидента);

4.определение действий по инциденту (автоматическое создание задач при назначении действий по реагированию на инциденты);

5.установка сроков по задачам;

6.решение (предложение различных вариантов решения задачи пользователю).

7.запрос информации. ПО подсистемы управления инцидентами #1 должно поддерживать возможность отправки и получения информации с целью получения дополнительных данных по инциденту у пользователей и других сотрудников на основе запроса по электронной почте.

Автоматическое назначение пользователей на инциденты ИБ по заданным критериям. В качестве критерия для

настройки правила реагирования на инцидент должно выбираться значение определённого поля.

Автоматическое уведомление пользователей Системы по заданным критериям. В качестве критерия для настройки правила реагирования на инцидент должно выбираться значение определенного поля.

Автоматическое уведомление ответственного по инциденту об истечении срока, установленного для обработки инцидента.

Возможность выполнения пользователем следующих действий: Уведомление, Действие персонала и возможность настройки цепочки действий в свойствах самого инцидента.

Возможность определять действия по инцидентам в соответствии с заданными критериями, а также назначать исполнителей и плановые сроки реализации действия.

Возможность использования логических выражений при настройке критериев выполнения правила реагирования.

Наличие конструктора сценариев реагирования, возможность задания в сценарии реагирования последовательности выполнения действий.

Возможность создания различных сценариев реагирования для разных типов инцидентов.

Возможность определения любой последовательности выполнения действий в сценариях реагирования.

Возможность выставлять таймаут при выполнении последовательных действий (отложенный запуск).

Возможность указания критериев в правилах реагирования, на основе которых выполняются сценарии. В качестве критериев должно выступать значение поля из карточки инцидента.

Поддержка динамических сценариев. Возможность создания сценария реагирования, в котором последующее действие учитывает результат предыдущего действия.

Визуализация сценариев реагирования.

Возможность запускать сценарии реагирования напрямую из свойств инцидентов.

Возможность настраивать темы и содержание уведомлений, отправляемых при исполнении сценариев реагирования.

Возможность указывать в качестве исполнителей действий по инцидентам пользователей, ответственных за инцидент.

Возможность учета уровня ущерба от реализации инцидентов информационной безопасности.

Возможность обмена информацией по инцидентам ИБ с другой, внешней аналогичной подсистемой.

Возможность изменения категории инцидентов, полученных из внешних систем.

Возможность экспорта/импорта данных об инцидентах в файл в формате *.xlsx.

Возможность выбора полей при экспорте данных по инцидентам.

Возможность импортировать данные и действия в уже существующие инциденты с помощью функционала тегов.

Возможность экспорта настроенных правил в файл в формате *.xlsx.

Возможность расширения функционала по реагированию на инциденты, поддержка скриптов реагирования для реализации превентивных или активных мер, включая получение свидетельств по инцидентам в автоматическом режиме.

2.7.Требования к функциональному блоку управления аудитами

Блок управления аудитами должен обеспечивать реализацию следующих функций:

Организация единой системы оценки состояния информационной безопасности на всех объектах организации.

Ведение базы внутренней документации по информационной безопасности с возможностью создания списков доступа пользователей к документам.

обеспечение совместной работы различных групп специалистов (ответственных за информационную безопасность на объектах, аудиторов, руководителей по информационной безопасности).

Обеспечение контроля системы защиты организации, в том числе на предмет выполнения законодательных, отраслевых и корпоративных требований.

Обеспечение учета всех мероприятий по информационной безопасности, нормативных документов, замечаний, проводимых аудитов безопасности.

Наличие предустановленных нормативно-правовых актов и стандартов в области обеспечения ИБ: (стандарт ISO 27001, PCI DSS, SWIFT Customer Security Programme Controls), а также возможность создания собственных стандартов безопасности или требований по безопасности и возможность контроля по заданным требованиям.

Наличие предустановленной базы, содержащей защитные меры с возможностью их привязки к группам ИТ-активов, на которых они реализованы и возможность ее дополнения;

Возможность оценки выполнения требований по информационной безопасности по предустановленным шкалам.

Возможность устанавливать собственные коэффициенты значимости для отдельных требований для пользовательских стандартов.

Возможность отслеживания для защитных мер связанных с ними контрольных проверок.

Возможность связать документ с теми активами, на которые распространяется область его действия.

Наличие механизма контрольных проверок, обеспечивающего:

овозможность создавать собственные контрольные проверки, позволяющие оценивать выполнение связанных требований по информационной безопасности и возможность создания аудитов с автоматической оценкой соблюдения требований на основании данных о степени выполнения контрольных проверок;

овозможность импорта описаний контрольных проверок из Excel-файлов;

овозможность настройки шкал для оценки контрольных проверок;

овозможность настройки рабочей группы (ответственные/аудиторы) для контрольных проверок;

овозможность настройки периодичности осуществления контроля для контрольных проверок;

овозможность выставления комментариев участниками рабочей группы для контрольных проверок;

овозможность подтверждения текущей оценки для контрольной проверки.

овозможность фильтровать журнал изменений по контрольным проверкам с помощью текстового поиска.

Возможность организации выборочной проверки конкретных настраиваемых требований.

Возможность копирования существующей оценки соответствия для проведения повторной оценки на основании скопированной.

Возможность прикреплять документы к создаваемым аудитам (например, отчет аудиторов по итогам внешнего аудита).

Возможность аудитору вносить замечания к каждому показателю безопасности системы защиты. Все замечания аудитора должны отображаться в интерфейсе Системы с возможностью контроля выполнения замечаний.

Возможность автоматического добавления задач при добавлении аудиторских замечаний.

Возможность внесения обоснования при выставлении оценки каждому показателю с возможностью прикрепления свидетельств и документов.

Фиксация создаваемых оценок с возможностью хранения истории предыдущих оценок для отслеживания изменений.

Блокирование изменений в результатах проведенных аудитов.

Возможность импортировать результаты оценки аудита из Excel-файлов.

Формирование пакета отчетных документов отчетных документов по состоянию системы информационной безопасности, а также по результатам проводимых оценок соответствия и аудитов информационной безопасности (сводные и детализированные отчеты, отчеты по установленным формам, Перечень свидетельств оценки и др., в том числе отчеты, содержащие комментарии участников рабочей группы в рамках аудита, и отчет, позволяющий оценить изменения в оценке показателей для нескольких выбранных аудитов).

2.8.Требования к функциональному блоку управления задачами

Блок управления задачами должен обеспечивать реализацию следующих функций:

Обеспечение единого рабочего пространства для всех сотрудников службы ИБ и других задействованных лиц в рамках задач по управлению активами, уязвимостями, аудитами и оценке рисков ИБ.

Отражение задач в зависимости от роли пользователя в Системе.

Визуализация состояния задач, индикация важности (критичности) задач, а также задач с просроченным сроком исполнения.

Регистрация действий пользователей по задачам.

Учет и просмотр истории выполнения задач.

Индикация просроченных задач.

Наличие чата для обмена сообщениями между участниками группы пользователей, привлеченных к задаче.

Отображение задач, назначенных исполнителям автоматически или в ручном режиме из функциональных блоков: управления уязвимостями, управления активами.

Хранение и учет документов, связанных как с постановкой задачи, так и результатов исполнения.

Возможность заведения субзадач вручную с привязкой к основной задаче, выбор пользователя, установка срока исполнения, критичности (важности), описание задачи, вложение файла с постановкой задачи.

Возможность фильтрации перечня задач по различным критериям (полям).

Возможность экспорта сведений по задачам в файл в формате Exel.

2.9.Требования к функциональному блоку визуализации данных

Блок визуализации данных должен обеспечивать реализацию следующих функций:

Наличие настраиваемых панелей визуализации (dashboard), отображающих различные метрики ИБ.

Возможность отображения разных панелей визуализации для разных групп пользователей.

Возможность индивидуальной настройки панелей визуализации для разных пользователей одной группы.

Возможность создания вкладок, содержащих разные панели, с отображением карт, сетей, планов помещений и схем визуализации активов, и возможность быстрого переключения между панелями.

Возможность сохранения настроенного отображения карты/сети/других элементов для каждого пользователя.

Визуализация информации в виде диаграмм, графиков и интерактивных схем.

Визуализация активов на геокарте (карте мира). Возможность просмотра групп ИТ-активов в виде короткого списка с возможностью просмотра всех групп в отдельном окне.

Визуализация активов на сетевой схеме L3 модели OSI.

Возможность перехода с геокарты в схему L3 (интерактивность).

Отображение активов на планах помещения, возможность загрузки планов помещений в Систему в графическом формате.

Отображение в списках оборудования, групп ИТ-активов, персонала, информации, бизнес-процессов, связанных с данным активом.

Отображение ресурсно-сервисной модели представления данных, отображение взаимосвязей между физическими и информационными активами;

Индикация на схеме L3 и плане помещения активов, на которых обнаружены уязвимости с учетом их статуса критичности (подсветка разным цветом в зависимости от критичности).

Возможность группировки объектов, назначение на группу иконки из преднастроенного справочника с изображениями иконок.

Возможность рисования на схеме графических элементов (линии, круги, прямоугольники);

Возможность интерактивной работы с элементами на панелях визуализации: отображение дополнительной информации об узлах, их группировка, фильтрация на картах сетей, добавление связанных элементов на схемах, возможность перехода к соответствующему разделу по щелчку на графиках и диаграммах (drill down).

Возможность отображения дополнительной информации по активу на схеме сети или ресурсно-сервисной схеме (схеме связей между информационными и физическими активами) при двойном щелчке на нем. Должна отображаться как минимум следующая информация: (имя устройства, тип ОС, домен, IP-адрес, перечень пользователей ОС с отображением информации о дате последнего входа в ОС, перечень установленного ПО, параметры безопасности ОС, сведения об уязвимостях).

Возможность построения графиков на основе данных из функционального блока управления активами, соответствующих критериям пользовательского фильтра.

2.10.Требования к функциональному блоку централизованного управления

Блок централизованного управления должен обеспечивать реализацию следующих функций:

Централизованное управление настройками составных компонентов ПО.

Централизованное обновление составных компонентов ПО.

Наличие ролевой модели доступа, возможность разграничения доступа пользователей ПО к определенным функциональным блокам, а также к документам в соответствии с определёнными ролями пользователей.

Возможность регистрации пользователей в самом ПО, а также возможность импорта пользователей из Active Directory.

Возможность создания групп пользователей.

Возможность настройки ролей, позволяющая пользователю ПО создавать, редактировать и удалять системные роли.

Поддержка двух цветовых схем в интерфейсе ПО – темной и светлой.

Возможность назначения системных ролей группам пользователей.

Наличие в ПО ролей по умолчанию, которые позволят сохранить настройки прав, созданные до обновления.

Управление обновлениями ПО, возможность локального обновления ПО без обращения в сеть Интернет.

Поддержка защищённых протоколов передачи данных для доступа к ПО (без применения дополнительных средств криптографической защиты).

Ведение журнала событий с возможностью его просмотра.

2.11.Требования к функциональному блоку отчетности

Блок отчетности должен обеспечивать реализацию следующих функций:

Наличие предустановленных отчетов, соответствующих основным функциям Системы.

Формирование отчетов вручную и автоматически согласно заданному расписанию.

Автоматическая рассылка сформированных отчетов заданным группам пользователей системы с использованием электронной почты.

Генерация и просмотр отчетов на основе исторических данных, накапливаемых в Системе;

Экспорт отчетов в файлы различных форматов: .docx, .pdf.

Экспорт карт, планов помещений в графическом формате.

В Системе должны присутствовать следующие отчеты:

сводка по группе ИТ-активов – отчет должен включать в себя сводку по оборудованию, сетям, пользователям и программному обеспечению в составе выбранной группы ИТ-активов;

сводка по сети – отчет должен содержать сводку по оборудованию, пользователям и программному обеспечению, обнаруженному в выбранной сети;

перечень программного обеспечения – отчет должен содержать сводку по всему программному обеспечению, либо программному обеспечению из определенной группы ПО;

перечень информационных активов – отчет, должен содержать сводку информационных активов (информации), а также отражать их взаимосвязь с бизнес-процессами и группами ИТ-активов;

перечень бизнес-процессов – отчет должен содержать список бизнес-процессов с указанием их взаимосвязи с информацией и группами ИТ-активов;

отчет по уязвимостям для группы ИТ-активов – отчет должен содержать перечень обнаруженных сканером

защищенности уязвимостей для определенной группы ИТ-активов;

отчет по уязвимостям для сети – отчет должен содержать перечень обнаруженных сканером уязвимостей для определенной сети;

отчет по уязвимостям для хоста – отчет должен содержать обнаруженные сканером безопасности уязвимости для определенного узла;

отчет по помещению – отчет должен содержать сводку по оборудованию, пользователям и программному обеспечению, размещенным в выбранном помещении;

отчет по хосту – отчет должен содержать сводку по конкретному хосту и включать в себя информацию об установленном ПО, развернутых средствах защиты информации, пользователях, связанных документах и имеющихся уязвимостях (при подключении сканера анализа защищённости);

сводка по задачам – отчет должен содержать детализированный перечень сведений по задачам включая отражение их статуса;

сводный реестр рисков – отчет должен представлять собой обобщенный список выявленных рисков информационной безопасности;

план обработки рисков – отчет должен содержать перечень запланированных мероприятий по обработке рисков;

детализированный реестр рисков – отчет должен содержать детализированный перечень выявленных рисков информационной безопасности, включающий в себя описание всех параметров по каждому из рисков (способы реализации, источники, предпосылки, активы, подвергающиеся риску, защитные меры и проч.);

сводный отчет по соответствию – отчет должен содержать обобщенные результаты оценки выполнений требований по защите информации, с указанием области оценки и уровня соответствия ему;

детализированный отчет по соответствию – отчет должен содержать детализированную информацию по результатам проведённой оценки соответствия требованиям по информационной безопасности с указанием степени выполнения каждого требования;

положение о применимости контролей – документ должен определять цели и меры управления, соответствующие и применимые к системе менеджмента ИБ организации (в соответствии с требованиями ISO 27001:2013);

детализированный отчет по аудиту (с комментариями) – отчет должен содержать подробную информацию о результатах проведённой оценки соответствия требованиям по информационной безопасности и включать в себя комментарии рабочей группы по аудиту.

2.12.Требования к функциональному модулю интеграции с внешними системами

Модуль интеграции с внешними системами должен обеспечивать реализацию следующих функций:

Автоматический сбор сведений по ИТ-инфраструктуре, активам и их свойствам, уязвимостям с внешних систем и импорт данных в Систему с помощью механизма коннекторов к смежным системам.

Возможность двухстороннего обмена данными со смежными системами.

Наличие интеграции с Active Directory (импорт сведений о пользователях, зарегистрированных в AD, о структурных элементах - данных о бизнес-подразделениях из профиля пользователя).

Импорт имени домена из интеграции с Active Directory в форматах FQDN и NETBIOS.

Наличие интеграции с Microsoft Exchange Server (отправка уведомлений пользователям).

Возможность указания дополнительных типов данных, получаемых через интеграции.

Получение сведений об уязвимостях с публичного сервиса Vulners.com.

Наличие коннектора к McAfee ePO (импорт сведений по хосту).

Наличие коннектора к McAfee ESM (импорт инцидентов).

4.Требование к обучению

Поставщик должен обучить не менее 3-х специалистов Заказчика пользованию Системой.

Допустимо проведение удалённого обучения. (вебинар)

Программа обучения должна включать следующие темы (модули):

•Модуль 1. Теоретические основы управления активами организации;

•Модуль 2. Управления активами с использованием R-Vision SGRC;

•Модуль 3. Теоретические основы управления инцидентами информационной безопасности;

•Модуль 4. Практика управления инцидентами ИБ с использованием R-Vision SGRC;

•Модуль 5. Основные методики и подходы к управлению рисками информационной безопасности;

•Модуль 6. Практика управления рисками ИБ с использованием R-Vision SGRC;

•Модуль 7. Основные подходы к организации аудита и контроля состояния информационной безопасности организации;

•Модуль 8. Практика проведения оценки соответствия требованиям ИБ с использованием R-Vision SGRC.

ИБРАЕВ АЛМАТ АЙТБАЕВИЧ

Дата подписания: 14.11.2018