**Техническая спецификация**

**«Услуги по обеспечению информационной безопасности»**

**(код по ЕНС ТР**[**У**](https://enstru.kz/code_new.jsp?&t=%D1%83%D1%81%D0%BB%D1%83%D0%B3%D0%B8%20%D0%BF%D0%BE%20%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%BE%D1%81%D1%82%D1%80%D0%B0%D0%BD%D0%B5%D0%BD%D0%B8%D1%8E%20%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%20%D0%BF%D0%BE%20%D0%BA%D0%B0%D0%B1%D0%B5%D0%BB%D1%8C%D0%BD%D0%BE%D0%B9%20%D0%B8%D0%BD%D1%84%D1%80%D0%B0%D1%81%D1%82%D1%80%D1%83%D0%BA%D1%82%D1%83%D1%80%D0%B5%20%D1%83%D1%81%D0%BB%D1%83%D0%B3%D0%B8%20%D0%BF%D0%BE%20%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%BE%D1%81%D1%82%D1%80%D0%B0%D0%BD%D0%B5%D0%BD%D0%B8%D1%8E%20%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%20%D0%BF%D0%BE%20%D0%BA%D0%B0%D0%B1%D0%B5%D0%BB%D1%8C%D0%BD%D0%BE%D0%B9%20%D0%B8%D0%BD%D1%84%D1%80%D0%B0%D1%81%D1%82%D1%80%D1%83%D0%BA%D1%82%D1%83%D1%80%D0%B5%20%D1%83%D1%81%D0%BB%D1%83%D0%B3%D0%B8%20%D1%81%D0%B2%D1%8F%D0%B7%D0%B8%20(%D1%82%D0%B5%D0%BB%D0%B5%D0%BA%D0%BE%D0%BC%D0%BC%D1%83%D0%BD%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D1%8B%D0%B5%20%D1%83%D1%81%D0%BB%D1%83%D0%B3%D0%B8)&s=common&p=10&n=0&S=611053%2E000&N=%D0%A3%D1%81%D0%BB%D1%83%D0%B3%D0%B8%20%D0%BF%D0%BE%20%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%BE%D1%81%D1%82%D1%80%D0%B0%D0%BD%D0%B5%D0%BD%D0%B8%D1%8E%20%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%20%D0%BF%D0%BE%20%D0%BA%D0%B0%D0%B1%D0%B5%D0%BB%D1%8C%D0%BD%D0%BE%D0%B9%20%D0%B8%D0%BD%D1%84%D1%80%D0%B0%D1%81%D1%82%D1%80%D1%83%D0%BA%D1%82%D1%83%D1%80%D0%B5&fc=1&fg=0&new=611053.000.000000) **801019.000.000010)**

|  |  |
| --- | --- |
| **№ п/п** | **Требования** |
| 1 | 2 |
| 1 | **Описание закупаемых товаров, работ и услуг** |
|  | Оказание услуги системы управления информационной безопасностью (далее – СУИБ) осуществляется оперативным центром информационной безопасности (ОЦИБ), осуществляющим свою деятельность на основании лицензии на оказание услуг по выявлению технических каналов утечки информации и специальных технических средств, предназначенных для оперативно-розыскных мероприятий в соответствии с законодательством Республики Казахстан в области информатизации.  Основными целями и задачами являются:   * Внедрение современных механизмов защиты для выявления и предотвращения целевых атак; * Улучшение механизмов выявления и предотвращения утечек, данных; * Повышение доступности ИТ-инфраструктуры и сервисов; * Повышение уровня информационной безопасности АО «НК «ҚТЖ»; * Снижение рисков ИБ и уменьшение числа актуальных угроз; * Повышение зрелости процессов ИБ, интеграция и централизация средств ИБ; * Создание ситуационного центра ИБ, для осуществления централизованного контроля над системами ИБ, мониторинга процессов и управления безопасностью. |
| 2 | **Требуемые функциональные, технические, качественные, эксплуатационные характеристики закупаемых товаров, работ и услуг.** |
|  | В рамках оказание услуги управления информационной безопасностью Исполнитель обязуется:  1. Произвести установку и активацию лицензий на право использования программных/программно-аппаратных сервисов по внедряемым услугам в течении 5 рабочих дней со дня подписания договора, с предоставлением Заказчику прав по использованию программного и аппаратного обеспечения.  2. Обеспечивать обновление и актуализацию баз данных угроз оборудования и программного обеспечения согласно предоставленным лицензиям, используемого для оказания услуги СУИБ;  3. Осуществлять настройку и интеграцию внедряемой услуги с существующими и внедряемыми системами АО «НК «ҚТЖ»;  4. По запросу от работников службы информационной безопасности АО «НК «ҚТЖ» вносить изменения в настройки и политики безопасности услуги СУИБ в соответствии с утвержденными сервисными регламентами с согласованием с работниками службы корпоративной безопасности АО «НК «ҚТЖ», а также по запросу от них;  5. Уведомлять ответственных работников АО «НК «ҚТЖ» о выявленных уязвимостях, представляющих угрозу безопасности ИТ-инфраструктуры АО «НК «ҚТЖ»;  6. Выделить технических специалистов, в количестве необходимом для оказания услуги в полном объеме в режиме 24\*7 (не менее 2-х сотрудников первой линии в круглосуточном режиме 24\*7).  7. В рамках услуги СУИБ использовать специализированные системы и предоставлять услуги, приведенные в таблице 1 для выполнения целей и задач услуги СУИБ с предоставлением необходимого аппаратного и программного обеспечения:  **Таблица 1:** Перечень обязательных систем и услуг, используемых при оказании услуги СУИБ.   |  |  |  |  | | --- | --- | --- | --- | | **Наименование системы** | **Показатель критичности (1-5), 1- макс.** | **Количественные показатели** | **Минимальное количество часов для обучения работников Заказчика с системой в год** | | Услуга ситуационного центра (SOC) | 1 | 1 услуга |  | | Система сбора и анализа событий (SIEM) | 1 | 30000 событий в секунду (EPS), максимальное значение | 80 | | Система управления активами и инцидентами | 1 | 1 услуга, для 12 000 активов | 80 | | Система защиты сетевого периметра и контроля доступа между сетевыми сегментами (Firewall and network security) | 1 | 2 площадки:  А) Периметровая: подключение к сети интернет, с организацией горячего резерва (серверный сегмент, клиентский сегмент, DMZ);  Б) Внутренняя: с организацией горячего резерва (серверный сегмент, клиентский сегмент).  VPN – не менее 5000 подключений с применением 2-х факторной аутентификации. | 160 | | Двухфакторная аутентификация | 1 | 1 услуга (не менее 5000 подключений) |  | | Антивирусная система контроля конечных рабочих станций (Endpoint malware protection) | 1 | 18000 защищаемых объектов, включая 1500 объектов с системой embedded | 160 | | Система защиты от таргетированных атак (APT defense) | 1 | 1 услуга | 160 | | Система выявления и предотвращения утечек данных (DLP); | 3 | 11000 защищаемых объектов | 80 | | Системы анализа трафика сети и каналов связи | 2 | 1 услуга, для корпоративного центра и 12 регионов | 80 | | Система фильтрации почтового трафика (Mail gateway) | 2 | 18000 защищаемых объектов | 80 | | Система сканирования на уязвимости (Vulnerability scanner) | 4 | 1 услуга | 80 | | Система анализа исходного кода (Source code analyzer) | 4 | 1 услуга | 80 | | Система управления и мониторинга привилегированного доступа (PAM - Privileged Acccess Management) | 1 | 1000 ресурсов без ограничения пользователей | 160 | | Проведение тестирования на проникновение (Penetration testing, pentest) | 5 | 1 раз в год |  | | Услуги повышения осведомлённости пользователей | 5 | 1 услуга |  | | Услуги компьютерной криминалистики (форензика) | 4 | 1 услуга |  | | Услуги консалтинга | 5 | 1 услуга |  | | Система очистки атак типа «Отказ в обслуживании» (Anti-DDOS) | 1 | Не менее 5 информационных ресурсов  Мощность очистки трафика не менее 5 Гбит/c | 80 | | Система фильтрации трафика веб-приложений (WAF) | 1 | 1 услуга, не менее 5 информационных ресурсов | 80 |   Примечание: предоставление ко всем системам необходимых вычислительных мощностей достаточных для эффективного предоставления услуг производится Исполнителем, также размещение центров управления и серверов перечисленных систем должно быть обеспечено в пределах локальной сети Заказчика.  8. Предоставить работникам АО «НК «ҚТЖ» доступ к интерфейсу систем управления сервисными услугами для просмотра текущего состояния сервиса и отчетности, а также для выполнения самостоятельной настройки правил и политик:   * Система сбора и анализа событий; * Система управления активами и инцидентами; * Система защиты сетевого периметра и контроля доступа между сетевыми сегментами; * Система контроля конечных рабочих станций (антивирусная защита); * Система защиты от таргетированных атак; * Система выявления и предотвращения утечек данных; * Системы анализа трафика сети и каналов связи; * Система фильтрации почтового трафика; * Система сканирования на уязвимости; * Система анализа исходного кода; * Система управления и мониторинга привилегированного доступа; * Система обмена информации о подозрительных событиях и инцидентах ИБ.   9. Для оперативного реагирования и выезда на объект Заказчика в аварийных случаях, служба технической поддержки Исполнителя должна находиться в городе Астана.  **2.3 Общие требования**  10. Исполнитель должен соответствовать единым требованиям, утверждённым постановлением Правительства Республики Казахстан от 20 декабря 2016 года № 832, а также требованиям Закона Республики Казахстан «Об информатизации» от 24.11.2015 г.  11. Исполнитель должен иметь действующую лицензию на оказание услуг по выявлению технических каналов утечки информации и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий в соответствии со статьёй 7–2 Закона Республики Казахстан об информатизации.  12. Наличие методики оказания услуг по выявлению технических каналов утечки информации оперативным центром информационной безопасности.  13. Предоставление ежемесячного/ежеквартального электронного отчета по оказанным услугам по выявлению технических каналов утечки информации и СТС оперативным центром информационной безопасности.  14. Возможность самостоятельного разграничения доступа к работающим в нем информационным системам.   * 1. **Требованию к уровню SLA**   15. Услуга предоставляется Заказчику в полном объеме в течение 24 часов в сутки, без перерывов за исключением времени проведения плановых регламентных работ, заблаговременно (не менее 2 рабочих дней) согласованных с Заказчиком.  16. Недоступность услуги Исполнителя может быть вызвана или связана с:   * Аварийной ситуацией. * Плановыми регламентными работами с суммарной продолжительностью не более 8 (восемь) часов в месяц, согласованными с Заказчиком нее менее чем за 48 (сорок восемь) часов до начала перерыва. * Срочными работами, согласованными с Заказчиком.   17. Заявки и запросы на обслуживание в случае предоставлении услуги в неполном объеме (Инцидент) направляются Заказчиком в Службу поддержки Исполнителя (ServiceDesk) одним из перечисленных способов:   * Электронные заявки через систему учета запросов; * По телефону на выделенный номер; * По электронной почте.   Запрос должен содержать информацию, необходимую для его корректной регистрации и выполнения:   * Ф.И.О. Инициатора запроса; * Номер телефона и адрес корпоративной электронной почты Инициатора запроса; * Описание возникшей неисправности или описание требований к выполнению в случае запроса на обслуживание или изменение;   При поступлении запроса сотрудники службы ServiceDesk обязуются:   * Зарегистрировать запрос в системе учета запросов; * Назначить каждому запросу на поддержку уникальный номер для упрощения обмена информацией; * Установить приоритет запроса; * Приступить к выполнению запроса.   При недостаточности и (или) неточности регистрационной информации специалисты Службы ServiceDesk имеют право:   * Обратиться к Инициатору запроса за дополнительной информацией. * Отклонить запрос, если Инициатор отказывается предоставить информацию, необходимую для регистрации Запроса.   Сроки обработки запросов и время работ по запросам Заказчика зависят от типа и определяются согласно **таблице 2.**  **Таблица 2.** Классификция запросов по уровню приоритетности и время реагирования   |  |  |  |  |  | | --- | --- | --- | --- | --- | | **Уровень критичности** | **Показатель критичности системы** | **Описание проблемы** | **Время начала работ по устранению** | **Время устранения** | | Уровень-1 (Критическая ошибка) | 1 | Инциденты, которые могут привести к серьезным нарушениям функциональности услуги - инфраструктура, в том числе в результате которых бизнес-процессы Заказчика оказываются неработоспособными | До 30 минут | До 1 часа | | Уровень-2 (Значительная ошибка) | 1-2 | Инциденты, при которых бизнес-процессы клиента функционируют, но их работа сильно затруднена или имеет высокий риск информационной безопасности. Данного рода инциденты оказывают значительное негативное влияние на бизнес-процесс клиента в целом | До 1 часа | До 4 часов | | Уровень 3 (Незначительная ошибка) | 1-3 | Инциденты, которые ведут к частичной потере функциональности бизнес-процессов. Проблема мешает работе лишь частично, в целом бизнес-процесс продолжает работать корректно; | До 3 часов | До 12 часов | | Уровень 4 (Консультации) | 1-4 | Любые запросы на обслуживание Заказчика по сбору и анализу информации. | До 6 часов | До 1 рабочего дня | | Уровень 5 (Изменения и доработки) | 1-5 | Любые запросы на обслуживание Заказчика по изменению конфигураций | До 24 часов | По согласованию с Заказчиком |   В таблице указаны крайние сроки решения проблемы. Персонал, занимающийся решением проблемы, обязан как можно раньше предоставить решение.  18. Исполнитель обязан выполнить анализ причин нарушения и выработать корректирующие мероприятия в случае нарушения SLA, позволяющие исключить повторение нарушения SLA.  19. Исполнитель обязан предоставлять Заказчику, в течение 3 (трех) рабочих дней, после устранения аварийной ситуации, акт выполненных работ и отчет по выполненным мероприятиям в ходе устранения аварийной ситуации.  20. Все компенсации Заказчику за недоступность услуг и/или превышение сроков оказания Технической поддержки в соответствующем Отчетном периоде предоставляются Заказчику исключительно в виде вычета из стоимости предоставления услуг за Отчётный период. При этом под «Отчетным периодом» Стороны договорились понимать как месяц предоставления услуги, под «началом срока недоступности Услуг» получения Заявки (письма, уведомления или иного документа) от Заказчика, в которой указывается время начала недоступности Услуг, под «окончанием срока недоступности Услуги» Стороны договорились понимать время выполнения Заявки Исполнителем (Статус Заявки - Выполнена), а под «превышением сроков оказания Технической поддержки» — нарушение Исполнителем сроков реакции или решения, предусмотренных выбранным Заказчиком уровнем технической поддержки настоящего Соглашения.  21. Исполнитель обязуется компенсировать случаи нарушения SLA Заказчику согласно **таблице 3.**  **Таблица 3.** Виды и размер компенсации:   |  |  |  | | --- | --- | --- | | **Превышение времени реакции** | **Превышение времени выполнения** | **Размер компенсации** | | От 1 минуты до 2 часов | От 1 минуты до 4 часов | 1% от суммы отчетного периода | | От 2 часов 1 минуты до 4 часов | От 4 часов 1 минуты до 8 часов | 3% от суммы отчетного периода | | От 4 часов 1 минуты до 6 часов | От 8 часов 1 минуты до 12 часов | 5% от суммы отчетного периода | | От 6 часов 1 минуты до 9 часов | От 12 часов 1 минуты до 18 часов | 7% от суммы отчетного периода | | От 9 часов 1 минуты и более | От 18 часов 1 минуты и более | 10% от суммы отчетного периода |   22. Заказчик не требует компенсации и не выставляет штрафные санкции Исполнителю за недоступность услуг и/или превышение сроков оказания технической поддержки, вызванные изменениями настроек или конфигураций самим Заказчиком без согласования с Исполнителем.  23. Заказчик не требует компенсации и не выставляет штрафные санкции Исполнителю за недоступность услуг и/или превышение сроков оказания технической поддержки, вызванные обстоятельствами непреодолимой силы. Функциональные требования к оказываемым услугамУслуга ситуационного центра (SOC) Услуга ситуационного центра осуществляется через имеющиеся у Исполнителя программно-аппаратные комплексы по мониторингу ИБ.  Услуга ситуационного центра должна обеспечивать следующий функционал:   * Круглосуточный мониторинг событий ИБ, зафиксированных в системах, предоставляемых в рамках данного договора; * Круглосуточный мониторинг событий ИБ, зафиксированных на серверном, клиентском и сетевом оборудовании, операционных системах, информационных системах и программном обеспечении Заказчика, подключенных к SIEM-системе Исполнителя (далее – Зона мониторинга); * Исключение ложных срабатываний и дубликатов подозрительных событий (далее ПС); * Обогащение информации о ПС дополнительными данными из систем, предоставляемых в рамках услуги или внешних источников в режиме 24/7; * Проведение технического анализа инцидента, включая анализ вредоносного программного обеспечения и цифровых артефактов, предоставление рекомендаций и участие в реагировании на инцидент дистанционно, а в случае необходимости на площадке заказчика; * Выявление инцидентов ИБ, произошедших в Зоне мониторинга; * Предоставление экспертной поддержки в процессе реагирования на инциденты; * Предоставление руководства и программного обеспечения для сбора артефактов; * Предоставление информации о критических уязвимостях и угрозах; * Предоставление ресурса, принадлежащего Исполнителю для передачи артефактов, собранных в рамках расследования инцидентов; * Осуществление консультаций при проведении расследования инцидентов ИБ; * Предоставление информации о выявленных критических уязвимостях с детальными рекомендациями по их устранению на корпоративные адреса электронной почты работников Заказчика; * Разработка не менее 10 уникальных сценариев выявления атак для Заказчика; * Осуществление подключения без ограничений типовых источников событий Заказчика и не менее 5 в год не типовых (в случае их наличия); * Проведение анализа объектов информатизации Заказчика на соответствие требованиям законодательства РК в области информационной безопасности; * Предоставление консультационной помощи, рекомендаций и инструкций по подключению источников Заказчика к системе сбора и анализа событий; * В случае если в Зоне мониторинга будет выявлено подозрительное событие, касающееся систем, не входящих в Зону мониторинга, – о данном событии уведомляется Заказчик. Дальнейшее расследование Заказчик осуществляет самостоятельно, Исполнитель при необходимости оказывает консультации для определения степени критичности и дополнительного анализа, с целью выявления источника проблемы и помощи в устранении инцидента специалистами Заказчика; * Взаимодействие с НКЦИБ в соответствии с требованиями законодательства Республики Казахстан; * Направление данных о произошедших инцидентах информационной безопасности в централизованный ОЦИБ группы компаний АО «Самрук-Қазына», при согласовании формата данных; * Разработка новых сценариев и соответствующих правил и сигнатур обнаружения атак:   + на основе собственной аналитики техник, тактик и процедур (TTP) атакующих, в том числе с применением методов Purple Teaming;   + на основе сбора и анализа Cyber Threat Intelligence – CTI (сбор, обработка и анализ отчетов по CTI и отчетов об атаках, а также новостей в области кибербезопасности, включающих новые угрозы, уязвимости и исследования);   + по запросу Заказчика; * Внедрение ложных целей – внутренних и внешних «кибер-ловушек»:   + создание и мониторинг стандартных и специфичных «кибер-ловушек» – цифровых клонов сервисов Заказчика;   + использование «кибер-ловушек» для обнаружения и реагирования на активности злоумышленников;   + автоматическая блокировка на периметровых устройствах доступа злоумышленников к защищаемым активам; * Threat Intelligence:   + интеграция с внешними источниками индикаторов компрометации (IoC);   + выявление в режиме реального времени индикаторов компрометации (IoC) по результатам анализа атак на инфраструктуру киберловушек;   + анализ журналов событий на наличие индикаторов компрометации (IoC) в режиме реального времени;   + периодический ретроспективный анализ журналов событий на наличие индикаторов компрометации (IoC);   + возможность подключения к коммерческим источникам TI (фиды, отчеты и т.п.) (по отдельной тарификации); * Threat Hunting – поиск следов компрометации в ИТ-инфраструктуре Заказчика, не обнаруженных превентивными средствами защиты и механизмами обнаружения в режиме реального времени:   + аналитиками Исполнителя в ручном режиме;   + с использованием автоматизированной ретроспективной корреляции событий безопасности;   + с использованием визуальной реконструкции сложных цепочек взаимосвязанных событий для упрощения процесса обнаружения атак и проведения специализированной экспертизы; * Администрирование технологической платформы SOC Исполнителя (серверов SIEM, систем сбора и хранения событий, системы обмена информацией о подозрительных событиях/инцидентах ИБ, киберловушек). * Направление Заказчику информации о выявленных инцидентах и методах реагирования на них и предоставления рекомендаций по их приостановлению распространения, устранению и предупреждению инцидентов ИБ в сроки определенные SLA (Раздел 2.5.1.1). * В случае отказа Заказчика от использования услуг ОЦИБ или по окончании действия Договора, Исполнитель должен в течение 14 календарных дней архивировать все накопленные данные (события, сетевые потоки), находящиеся на ресурсах Исполнителя. Заказчику должна предоставляться возможность скачивания архива данных по защищённому каналу или копирования на собственные съёмные носители. Передача данных должна фиксироваться актом приема-передачи. Заказчик обязан хранить переданные данные в течение 3 (трех) лет. Исполнитель обязуется после расторжения Договора в течение 30 (тридцать) календарных дней хранить на своих ресурсах данные Заказчика, безвозмездно. При хранении данных свыше 30 (тридцати) календарных дней, Заказчик оплачивает стоимость услуг Исполнителя в течение срока хранения информации Заказчика на ресурсах Исполнителя по согласованным тарифам. * В случае не востребованности, накопленные данные, включая архивные, будут удалены не позднее 45 (сорок пять) календарных дней с предварительным уведомлением и возможным участием Заказчика.   + - 1. **Целевые показатели уровня предоставления услуги ситуационного центра(SOC)** * Целевые показатели уровня предоставления услуги ситуационного центра распространяется только на события, поступающие с источников Заказчика и определяются согласно таблице 4.   Таблица 4   | **№** | **Показатель** | **Уровень критичности** | **Время реагирования Исполнителя** | **Табель** | **Время реагирования Заказчика** | | --- | --- | --- | --- | --- | --- | |  | Время информирования Исполнителем Заказчика о ПС/инциденте ИБ с момента его фиксации в SIEM, после проведения первичного анализа, проверки на признак ложной сработки, категорирования, с предоставлением рекомендаций по первичному реагированию. | 4 – Критический | 30 минут | 24x7 | Не применимо | | 3 – Высокий | 45 минут | 24x7 | Не применимо | | 2 – Средний | 2 часа | 24x7 | Не применимо | | 1 – Низкий | 6 часов | 24x7 | Не применимо | |  | Выдача рекомендаций по противодействию инциденту ИБ с момента подтверждения инцидента ИБ Заказчиком | 4 – Критический | 1 час | 24x7 | Не применимо | | 3 – Высокий | 2 часа | 24x7 | Не применимо | | 2 – Средний | 4 часа | 24x7 | Не применимо | | 1 – Низкий | 18 часов | 24x7 | Не применимо |  * Уровень критичности ПС/инцидента определяется согласно таблице 5.   **Таблица 5. Уровни критичности ПС/инцидента ИБ**   | **Уровень критичности** | **Описание** | | --- | --- | | |  | | 4  (Critical - Критический) | Инцидент, связанный с критическим ресурсом, в результате которого бизнес-процессы Заказчика оказываются неработоспособными или нанесен существенный ущерб для Заказчика связанный с компрометацией системы/систем | | 3  (High - Высокий) | ПС или инцидент, связанный с критическим ресурсом, который может привести или привел к компрометации системы/систем или ущербу для Заказчика. Бизнес-процессы клиента функционируют, но их работа сильно затруднена или имеет высокий риск информационной безопасности. Данного рода инциденты оказывают значительное негативное влияние на бизнес-процесс клиента в целом. | | 2  (Medium - Средний) | ПС или инцидент, связанный с некритическим ресурсом, который может привести или привел к компрометации системы/систем или ограниченному ущербу для Заказчика. Проблема мешает работе лишь частично, в целом бизнес-процесс продолжает работать корректно. | | 1  (Low - Низкий) | ПС, свидетельствующее о неуспешной попытке атаки, атаки, остановленной средствами защиты, либо этап разведки инфраструктуры Заказчика. |  * Учет времени реагирования на ПС приостанавливается, когда обстоятельства, влияющие на это время, находятся вне зоны ответственности Исполнителя, например, сбои на каналах связи, сбои серверов систем доставки событий, контролируемых Заказчиком и т.п. * Заказчик информирует Исполнителя о статусе реагирования на ПС/ инцидент в сроки, указанные в Таблице 5. * Заказчик информирует Исполнителя об окончательном результате реагирования на ПС/ инцидент в течение 5 рабочих дней, после чего Исполнитель имеет право автоматически закрыть ПС на своей стороне (если от Заказчика в течение 5 рабочих дней не поступает мотивированный запрос на продление срока реагирования). * SLA не распространяется на сценарий «Threat Hunting» (в связи с тем, что сам принцип проведения Threat Hunting подразумевает полуавтоматический и ручной поиск следов компрометации в ИТ-инфраструктуре Заказчика, не обнаруженных превентивными средствами защиты и механизмами обнаружения в режиме реального времени).   + - 1. **Расчет уровня выполнения SLA в рамках услуги мониторинга.** * В целях общей оценки качества выполнения SLA Исполнителем ежегодно производится расчёт показателя «Уровень выполнения SLA». * Исполнитель не несет ответственность за любые сбои программного обеспечения и оборудования Заказчика, в том числе произошедшие при настройке Заказчиком источников, входящих в Зону мониторинга, а также возникшие в процессе оказания Услуги, за исключением случаев, когда Исполнитель самостоятельно производил работы на ИС Заказчика силами своих специалистов (например, при настройке и администрировании брокеров). При этом Исполнитель приложит максимальные зависящие от него усилия по оказанию консультационной помощи для обеспечения корректной работы платформы мониторинга и программного обеспечения, рекомендованного Исполнителем для сбора журналов событий с источников. * При оказании Услуги Исполнитель несёт ответственность исключительно в рамках показателей, зафиксированных в таблице 4. Непосредственные работы по реагированию на инцидент и восстановлению работоспособности ИС производятся Заказчиком и любой сбой или простой ИС Заказчика никак не влияет на расчёт SLA. * Расчет услуги круглосуточного мониторинга событий ИБ производится по следующей формуле:   Уровень выполнения услуги круглосуточного мониторинга = ((R-S)/R)\*100%  , где   * R – количество обнаруженных посредством круглосуточного мониторинга подозрительных событий критичного и высокого приоритета, * S – количество подозрительных событий критичного и высокого приоритета, не обработанных в заявленные сроки согласно таблице 5. Пороговым оценочным показателем является– 100 %. * В случае снижения уровня обслуживания ниже заявленного 99.5%, Заказчик в праве применить штрафные санкции согласно таблице 6.   **Таблица 6**   |  |  | | --- | --- | | **Значение SLA %** | **Уровень налагаемого штрафа в процентах от суммы платежа за период действия SLA** | | 98-99,(4) % | До 0.3% | | 95-97,(9)% | До 0.5% | | менее 95% | До 1% |    Система сбора и анализа событий Обеспечение надежного и оперативного управления событиями информационной безопасности в организации, с целью предотвращения угроз, обнаружения инцидентов и реагирования на них в реальном времени.  Задачи:  Обеспечение централизованного сбора и анализа данных о событиях безопасности.  Автоматическое обнаружение и классификация инцидентов безопасности.  Реализация автоматизированных процессов реагирования на инциденты.  Обеспечение требований регуляторов и стандартов в области кибербезопасности.  Основные функциональные требования  - Сбор, обработка и корреляция событий информационной безопасности, должны выполняться посредством системы управления событиями информационной безопасности (SIEM), развёрнутой у Заказчика.  - Система должна обеспечивать централизованное управление всеми ее компонентами и функционалом через единый веб-интерфейс без необходимости запуска сторонних приложений, дополнительных интерфейсов, окон или скриптов;  - Система должна обеспечивать автоматический импорт данных: Готовые интеграции с другими продуктами. Возможность автоматического импорта данных из различных источников в течение нескольких минут.  - Поддержка различных форматов данных: Не структурированные данные любого типа.  - Система должна поддерживать возможность разделения dashboards через пользовательский интерфейс для использования во внедрениях SOC (Security Operations Center) и NOC (Network Operations Center);  - Система должна обеспечивать гибкий процесс управления учетными записями пользователей и их ролями;  - Система должна иметь возможность шифровать коммуникации между компонентами;  - Система должна обеспечивать автоматическое обновление конфигураций без дополнительных временных затрат со стороны пользователя системы путем автоматической загрузки их с сервера обновлений, что может находиться в сети интернет, или в локальной сети организации. Например, обновление модулей нормализации и коннекторов по отдельным Системам и устройствам сторонних производителей;  - Система должна поддерживать возможность реализации отказоустойчивой архитектуры;  - Система должна гарантировать работу отдельных компонентов системы, при выходе из строя любой части системы. (Например, центральная консоль выходит из строя, но лог коллекторы продолжают функционировать);  - Система должна иметь автоматический процесс резервного копирования конфигурации (Backup) и возможность восстановления (Recovery) конфигурации с графического интерфейса пользователя;  - Система должна иметь встроенный процесс анализа своего состояния и оповещать пользователя при возникновении проблем;  - Система должна предоставлять возможность развернуть при необходимости подсистему для координации и автоматизации процессов реагирования и расследования инцидентов от производителя Системы;  - Система должна легко масштабироваться и расширять функционал (при добавлении новых устройств, офисов, приложений в сети заказчика) для соответствия требованиям организации;  - Система должна иметь возможность гибкого долгосрочного хранения данных с разделением на горячие, тёплые и холодные данные для уменьшения издержек, с сохранением возможности поиска и расследования инцидентов.  - Система должна иметь возможность хранения и поиска данных как отдельно на on-prem серверах, публичных облаках, так и в гибридном исполнении  - Система должна развертываться с запасом производительности и работать при кратковременных пиках нагрузки, превышающие расчетные нагрузки для данной системы;  - Система должна обеспечивать целостность собранной информации;  - Система должна поддерживать разнесённую модель для корреляции со всех коллекторов. (Например, для 25 неудачных попыток аутентификации, когда 25 событий приходят не на 1 коллектор, а на несколько);  - Система должна поддерживать расширенную таксономию пользователей для событий и полей. Пользователь должен иметь возможность присваивать событиям любые имена;  - Система должна предоставлять возможность изменения поведения автоматической пометкой событий по важности в соответствии с пожеланиями пользователя;  - Система должна иметь функционал SOAR.  - Система должна предоставлять прозрачное получение, агрегирование, сортировку, фильтрацию и аналитику данных по всем разнесенным компонентам системы;  - Система должна поддерживать хранение журналов событий на внешних хранилищах без необходимости приобретения дополнительных лицензий для активации этих возможностей;  - Система должна поддерживать стандартные методы сбора журналов событий (например, syslog, WMI, JDBC, SNMP, Checkpoint LEA, и др.);  - Система должна поддерживать безагентный сбор журналов событий везде, где это возможно;  - Система должна иметь возможность распределять хранение журналов событий и их обработку по всей архитектуре Системы;  - Система должна предоставлять доступ ко всей информации о событиях на протяжении длительного периода времени (например, 12 месяцев) для дальнейших расследований;  - Система должна нормализовать стандартные поля событий (имена пользователей, IP адреса, имена хостов, устройства-источники событий) с различных устройств мультивендорной сети. Нормализация должна проводиться без дополнительных настроек (out of the box);  - Система должна предоставлять стандартную категоризацию событий без предварительных дополнительных настроек;  - Система должна иметь возможность сохранять информацию о событиях, как в исходном виде, так и в нормализованном виде для использования в дальнейших расследованиях;  - Система должна иметь возможность обрабатывать и нормализовать данные с полей, которые не поддерживаются изначально и не предоставляются с настройками out of the box;  - Система должна обеспечивать анализ событий в режиме реального времени;  - Система должна обеспечивать анализ событий в течение определенного периода времени;  - Система должна предоставлять возможность собирать и анализировать события по установленным пользователем фильтрам;  - Система должна предоставлять возможность получения дополнительной информации о событиях при необходимости (drill down);  - Система должна обеспечивать фильтрацию, а также показывать через интерфейс события в режиме реального времени, где пользователь может сразу же применять политики и фильтры;  - Система должна предоставлять отчетность по всем событиям, отчетность должна быть доступна через веб-интерфейс для пользователей решения;  - Система должна давать возможность самостоятельной настройки отчетности и создание собственных отчетов пользователем;  - Система должна иметь возможность расширения функционала за счет установки приложений/интеграций, которые должны быть проверены производителем системы;  - Система должна предоставлять поддержку языка запросов ES|QL;  - Система должна иметь возможность расширения количества корреляционных правил (например, для выявления новых угроз), отчетов и встроенных поисков за счет установки приложений/интеграций, которые должны быть проверены производителем системы;  - Система должна поддерживать мультиарендность (multitenancy) с возможностью разграничения доступа и обфускации (маскированием) данных для заданных пользователей;  - Система должна иметь возможность увеличения количества полей, нормализуемых системой за счет установки приложений/интеграций, которые должны быть проверены производителем системы;  - Система должна предоставлять предустановленные правила обнаружения: Наличие предустановленных правил обнаружения не менее 800 шт., основанных на MITRE ATT&CK  - Система должна предоставлять возможность пользователю оценивать уровень покрытия правилам обнаружения угроз известных тактик и техник по MITRE ATT & CK Framework;  - Система должна предоставлять возможность создания своих правил обнаружения без использования «кода»  - Система должна иметь возможность подключать сторонние каналы обнаружения угроз (Threat Intelligence). Использовать их для обнаружения атак, в том числе в историческом контексте  - Система должна предоставлять возможность ручной загрузки событий через Веб-интерфейс для дальнейшего анализа корреляционными правилами с целью выявления потенциальных угроз;  - Система должна предоставлять возможность установки неограниченного количества компонентов, которые не требуют дополнительных затрат на лицензирование для обеспечения сбора событий с удаленных сетей с использованием безопасных протоколов передачи данных с возможностью подключения через публичные сети;  - Система должна предоставлять возможность графического анализа и визуализации в виде схемы взаимодействия корреляционных правил, групп корреляционных правил и динамических списков для упрощения процесса построения сложных моделей и алгоритмов обнаружения угроз;  - Система должна поддерживать использование алгоритмов машинного обучения для выявления аномалий и неизвестных угроз;  - Система должна поддерживать возможность использования пользователем собственных моделей машинного обучения;  - Система должна предоставлять функционал поведенческого анализа активности пользователей (UBA);  - Модуль поведенческого анализа должен использовать модели машинного обучения и не нуждаться в дополнительном лицензировании;  - Модуль поведенческого анализа не должен содержать ограничений по количеству учетных записей и пользователей активность которых поддается анализу;  - Система должна поддерживать возможность подключения сторонних ИИ.  - Система должна давать рекомендации по установлению дополнительных приложений/интеграций на основании информации о подключенных источниках событий;  - Система должна предоставлять возможность выявления угроз на уровне DNS (использование алгоритмов генерации доменных имен (DGA), передача данных через DNS запросы (DNS Tunneling), выявления попыток доступа к запасных доменных имен (DNS Squatting)) на основании данных от DNS серверов, прокси серверов или других систем, поддерживающих технологию BIND;  - Система должна обеспечивать централизованное управление всеми вышеперечисленными компонентами и их функционалом через единый веб-интерфейс;  - Система должна гарантировать актуальность данных, собираемых и обрабатываемых в единой базе данных - обеспечивать обработку и корреляцию данных из журналов событий (logs) с задержкой не более 1 секунды после получения данных системой от источника событий;  - Все вышеперечисленные компоненты Системы должны иметь единую базу данных для хранения и обработки информации.  Требования к интеграции  - Интеграция с источниками данных: сетевыми устройствами (маршрутизаторы, коммутаторы, межсетевые экраны); серверами и рабочими станциями (в т.ч. под управлением ОС Microsoft, Linux/Unix и др.;), а также поддержка Агентов Linux / Windows; приложениями и базами данных (в т.ч. SAP, Web, Oracle, MySQL и др.); другими системами безопасности (IPS, IDS, DLP и т.д.); поддержка стандартных протоколов для интеграции (LDAP, Netflow, J-Flow, S-Flow Syslog, SNMP, API, WMI, JDBC, Checkpoint LEA, и т.д.); возможность создания собственных парсеров для нестандартных форматов логов.  Требования к обучению и поддержке  - Обучение персонала по работе с системой: базовое и продвинутое.  - Техническая поддержка в течение эксплуатации системы.  - Поставка обновлений и патчей безопасности для системы.  Требования к лицензированию  - Модель лицензирования (по объему данных или количеству источников или количеству событий в секунду позволяющих фиксировать и обрабатывать количество EPS указанных в таблице 1).  - Возможность масштабирования и расширения функционала системы без замены основного продукта, в т.ч. путем развертывания дополнительных коллекторов.   * + 1. **Система управления активами и инцидентами**   В состав системы должны входить следующие компоненты:  - Сервер центрального управления информационной безопасностью;  - Сервер баз данных;  - Коллектор(ы).  Сервер центрального управления системой должен обеспечивать реализацию основных функций Системы, включая работу с активами, уязвимостями, инцидентами ИБ, рисками, аудитами, визуализацию и формирование отчетов, а также взаимодействие с другими модулями Системы.  Коллектор Системы должен обеспечивать инвентаризацию отдельных сегментов ИТ-инфраструктуры, в том числе сканирование с целью поиска уязвимостей ПО, и передачу информации на основной сервер(ы), интеграцию с различными смежными ИС и СЗИ, а также поддерживать возможность реализации функций технического реагирования,  Системы не должны предполагать использования и приобретения дополнительного стороннего коммерческого ПО, включая СУБД.  Архитектура Системы должна предусматривать возможность размещения своих компонентов на нескольких площадках/вычислительных ресурсах и осуществлять интеграцию с оборудованием, расположенным в различных сегментах сети Заказчика.  В качестве АРМ Пользователя и АРМ администратора должны использоваться эксплуатируемые АРМ Заказчика.  Требования к функциям  Требования к подсистеме центрального управления информационной безопасностью  Требования к способам и средствам управления подсистемой, а также информационного обмена между модулями подсистемы  Должна быть обеспечена совместимость между компонентами подсистемы, а также ее совместимость с взаимосвязанными телекоммуникационными и автоматизированными системами, находящимися в эксплуатации у Заказчика и доступными для интеграции.  Взаимодействие пользователей подсистемы должно осуществляться посредством графического веб-интерфейса.  ПО должно поддерживать применение защищенных протоколов передачи данных между компонентами.  Подсистема должна предоставлять возможность локального обновления компонентов подсистемы без обращения в сеть Интернет.  Требования по диагностированию подсистемы  Диагностирование Системы должно выполняться посредством записей в журналы аудита информации по служебным событиям и сбоям. Записи в журналах должны содержать информацию, достаточную для установления причины неисправности. Должна поддерживаться возможность отправки журналов компонентов системы по протоколу syslog на сервер мониторинга.  Масштабирование подсистемы  Подсистема должна предусматривать масштабирование по производительности и объему обрабатываемой информации путем добавления дополнительных компонентов используемого аппаратного комплекса технических средств и расширения лицензии. При масштабировании подсистема не должна предполагать использования дополнительного стороннего коммерческого ПО, включая коммерческие СУБД.  Требования к защите информации от несанкционированного доступа  Подсистема должна поддерживать следующий функционал:  • Обеспечение авторизации и аутентификации пользователей.  • Аутентификационные данные, используемые для подключения подсистем к смежным ИС или СЗИ, должны храниться в подсистеме в зашифрованном виде.  • Наличие ролевой модели доступа, возможность разграничения доступа пользователей подсистемы к определенным функциональным блокам.  • Авторизация пользователя по токену для работы через API подсистемы. С помощью токена пользователь может работать через API подсистемы с правами, заданными в его учетной записи.  Требования к модулю управления активами подсистемы центрального управления  Требования к функционалу инвентаризации  • Возможность инвентаризации узлов с ОС Windows с использованием инструментария WMI, WinRM, SMB или с использованием VBS-скриптов, выполняемых на конечных узлах.  • Возможность инвентаризации узлов с ОС Linux посредством подключения по SSH, по протоколу SNMP или с использованием bash-скриптов, выполняемых на конечных узлах.  • Возможность инвентаризации сетевого оборудования посредством подключения через SSH или по протоколу SNMP (инвентаризируется оборудование, поддерживающее OID MIB-II).  • Сбор базовой инвентаризационной информации, включая технические параметры оборудования и параметры безопасности.  • Возможность формирования политик инвентаризации с настройкой периодичности инвентаризации объектов, включающих следующий функционал:  o сканирование произвольных диапазонов IP адресов/сетей/имен устройств;  o сканирование хостов и Групп ИТ-активов по именам устройств;  o исключение из сканирования IP адресов/сетей/имен устройств;  o возможность задать область сканирования - все оборудование или только новые объекты;  o возможность задать перечень учетных записей для каждой политики;  o режим “Обнаружение” для сканирования без учетной записи;  o возможность настройки параметров сканирования;  o просмотр истории и статуса сканирования в интерфейсе.  o сбор информации об открытых портах по заданному диапазону TCP/UDP портов.  Требования к интеграции с внешними системами  • Интеграция с системами антивирусной защиты:  o Импорт инвентаризационной информации об узлах.  • Интеграция с другими системами:  o наличие интеграции с Active Directory. Импорт сведений о пользователях, зарегистрированных в AD, оборудованию, сведений о структурных элементах – о бизнес-подразделениях, или группах ИТ-активов из Organization Unit AD или атрибута пользователя/оборудования. Настраиваемый перечень импортируемых дополнительных атрибутов оборудования или пользователей AD в систему;  o возможность создания универсальной интеграции с файлами для импорта данных об активах. Поддержка импорта сведений из файлов формата xlsx, csv, json, xml. Возможность привязки оборудования к домену при импорте из файлов Excel: система проверяет наличие домена в базе данных: если такой домен существует, система автоматически привязывает оборудование к этому домену, если домена нет в базе данных, система добавляет новый домен и привязывает оборудование к нему;  o наличие универсальной интеграции с базами данных: Microsoft SQL Server, Oracle, PostgreSQL, MySQL. Импорт следующих типов активов: оборудование, организация, бизнес-процессы, информация, группы ИТ-активов, cети, персонал, помещение, а также пользовательских типов активов. При импорте оборудования из внешних БД должна импортироваться в Систему связанная с ними информация по установленному на оборудовании ПО.  • Наличие конструктора интеграций, поддерживающего следующий функционал:  o создание произвольной интеграции, которая в свою очередь может импортировать любые активы с использованием языка программирования Python;  o возможность использования шаблонов интеграции для настройки основных параметров;  o возможность настроить виртуальное окружение для запуска скрипта интеграции при необходимости загрузить библиотеки, не включенные в стандартное виртуальное окружение по умолчанию.  • Возможность задания расписания интеграции с внешними системами.  • Возможность штатной интеграции Системы с другой инсталляцией Системы по модели «система донор» - «система реципиент». В рамках интеграции синхронизируются данные:  o справочников из раздела Активы: Теги, Пользовательские справочники, Поля описания активов, Статусы оборудования, Типы оборудования, Группы ПО;  o справочника из раздела Общие: Локации;  o для типов активов: Группы ИТ-активов, Оборудованиe, Персонал, Сети, Бизнес-подразделения, Бизнес-процессы, Помещения;  o по категоризации групп ИТ-активов.  Требования к учету активов  • Учет материальных и нематериальных активов и их взаимосвязей (бизнес-процессы, информация, сети, оборудование, помещения, персонал, подразделения, группы ИТ-активов, пользовательские активы).  • Нормализация и дедупликация данных об активах при интеграции с несколькими внешними источниками.  • Ведение карточек активов, включающих общие сведения об активе, список ответственных лиц и связанные активы, связанные инциденты и дополнительную информацию, а также возможность просмотреть карточку любого связанного с ним актива в отдельном окне.  • Возможность связывания актива с другими объектами системы (вручную или автоматически):  o активами других типов (бизнес-процессы, информация, группы ИТ-активов, оборудование, бизнес-подразделения, персонал, программное обеспечение, пользовательские активы и иными типами активов), настроенными в системе;  o активами того же типа по принципу простой связи или иерархической (для активов типа группы ИТ-активов, оборудование и пользовательские активы);  o задачами (для активов типа бизнес-процессы, группы ИТ-активов, оборудование, бизнес-подразделения, пользовательские активы);  o инцидентами (для активов типа бизнес-процессы, информация, группы ИТ-активов, оборудование, бизнес-подразделения, персонал, ПО);  o уязвимостями (для активов типа оборудование и Группы ИТ-активов с возможностью отображения статистики по уязвимостям и фильтрации по уровню критичности, по типу оборудования, по наличию эксплойта, по портам, по вектору достижимости);  o требованиями (для активов типа бизнес-процессы, группы ИТ-активов, оборудование, бизнес-подразделения, помещения);  o аудитами (для активов типа бизнес-процессы, группы ИТ-активов, оборудование, бизнес-подразделения, помещения);  o документами (для активов типа бизнес-процессы, группы ИТ-активов, оборудование, бизнес-подразделения, помещения, информация, ПО, сети, персонал, пользовательские активы).  • Возможность вести каждый тип активов в отдельной вкладке (оборудование, персонал, программное обеспечение, помещения и т. д.).  • Возможности работы со списком активов:  o поиск по таблицам со списками оборудования и персонала;  o сортировка списка по любому полю для каждого типа актива;  o фильтрация списка по одному или нескольким полям для каждого типа актива;  o сохранение пользователем фильтра списка;  o настройка выводимых полей для списка активов;  o создание нескольких режимов отображения активов по заданному фильтру и быстрого переключения между ними (для каждого локального пользователя Системы).  o вывод списков активов (подразделения, помещения, бизнес-процессы, группы ИТ-активов, ПО, сети) как в виде линейного списка, так и в виде иерархической структуры, с возможностью быстрой идентификации родительских и дочерних активов;  o групповое удаление активов.  • Возможность создавать собственные (пользовательские) типы активов с индивидуальными полями карточек и выбирать для таких активов иконку отображения. Возможность устанавливать связи пользовательских активов между собой и с другими типами активов.  • Возможность автоматизированного учета оборудования в сетях с одинаковой адресацией. Возможность создания требуемого количества адресных пространств и распределения по ним всех дублирующихся сетей.  • Автоматическое определение типа узла с помощью настраиваемых правил.  • Автоматическая привязка сетей к группам ИТ-активов, в которые входят узлы из этой группы.  • Возможность автоматического включения ПО в группы по настроенным правилам. Возможность настройки исключений для групп ПО. ПО должно группироваться по наименованию, должна быть возможность редактирования нескольких элементов одной группы.  • Отображение степени критичности активов в виде цветовой схемы.  • Возможность управления категоризацией групп ИТ-активов с заполнением соответствующих полей описания (АСУТП, ГИС, КИИ, ИСПДн и пр.). Возможность создавать собственные категории групп ИТ-активов с индивидуальным набором полей.  • Ведение истории по действиям с активами (добавление, изменение, удаление) в пользовательском интерфейсе независимо от источника изменений (пользователь, интеграции).  • Возможность уведомлений пользователей по электронной почте или во всплывающем окне на панели уведомлений о зафиксированных изменениях в активах (нахождение нового оборудования, нахождение нового открытого порта оборудования, нового ПО или пользователя, новых уязвимостей, новых сетей, устранение уязвимостей, уведомление об исчезновении оборудования (удаление оборудования), обнаружение новой группы ИТ-активов, создание/изменение/удаление пользовательского актива, изменение статуса инвентаризации узла).  • Возможность ручного импорта данных по сетям, оборудованию, группам ИТ-активов, подразделениям, помещениям, персоналу, бизнес-процессам и пользовательским активам из файлов формата excel по шаблону. Должна осуществляться проверка системой заполненности обязательных полей при импорте активов из файла.  • Возможность экспорта в таблицу .xlsx данных по активам с учетом текущей настройки столбцов, примененных фильтров и сортировок.  • Возможность проводить первоначальную оценку ценности актива (для активов типа группы ИТ-активов, бизнес-процессы, информация) по параметрам конфиденциальности, целостности и доступности, а также их редактирования.  Требование к полям и карточкам активов  • Возможность конструировать карточки активов для каждого типа актива отдельно с возможностью добавления следующих типов полей: выпадающий список, дата, несколько текстовых строк, текстовое поле, чек-бокс, числовое поле, числовое поле с денежным символом, выбор пользователя (возможность выбора пользователя из списка пользователей системы), IP-адрес/адрес сети. Конструктор должен позволять настраивать набор и порядок следования полей в карточке для заданного типа актива.  • Возможность настроить валидацию по регулярному выражению для текстовых полей и полей типа IP-адрес/адрес сети  • Возможность контролировать истечение даты любых полей типа «Дата» с индикацией в интерфейсе и отправкой уведомлений: как почтовых, так и в панель уведомлений.  • Возможность группового редактирования полей активов.  • Наличие в карточке оборудования поля, отображающего статус инвентаризации, содержащего описание ошибки инвентаризации или статус ее успешного прохождения.  • Наличие поля в карточке актива для указания локации с возможностью привязки актива к населенному пункту или объекту из справочника локаций, применяемому для вывода информации по активам и связанных с ним инцидентов и уязвимостей на географическую карту.  Требования к жизненному циклу  • Возможность реализации статусной модели актива в соответствии с заданными в организации процедурами.  • Возможность автоматически помечать и удалять из системы оборудование и активы типа персонал, сведения по которым не обновлялись в течение заданного периода времени.  • Визуализация в виде диаграмм количества активов типа оборудование или персонал, сведения по которым не обновлялись определенный период времени.  Требования к автоматизации  • Возможность создания правил, по которым осуществляется автозаполнение полей активов.  • Автоматическое заполнение поля «Локация» для группы ИТ-активов и сетей на основе информации от входящих в их состав узлов.  • Возможность расчета состояния активов:  o автоматизированное построение ресурсно-сервисной модели бизнес-процессов в виде схемы;  o автоматический расчет состояния активов ресурсно-сервисной модели на основе связанных с ними инцидентов;  o опция автоматического обновления схемы взаимосвязей в соответствии с актуальной информацией в базе данных;  o переход из схемы расчета состояния актива к связанным активам или инцидентам;  o расчет влияния активов друг на друга и на состояние бизнес-процесса с учетом статусов активов, объединения оборудования в кластер, с возможностью указать коэффициент влияния, а также ограничить порог влияния инцидентов на состояние актива;  o возможность задать прямое влияние инцидента на бизнес-процесс;  o наличие режима тестирования схемы взаимосвязей активов, позволяющей добавлять к активам "виртуальные инциденты" и выполнять расчет состояния от точки изменения;  o наличие режима редактирования схемы, который позволяет одновременно только одному пользователю изменять данные, а также отображает индикатор пользователя, редактирующего схему взаимосвязей;  o возможность загружать на схему все связи выбранного актива на один уровень и сворачивать цепочку активов до выбранного;  o возможность отправлять уведомления при изменении схемы взаимосвязей указанного бизнес-процесса;  o просмотр истории изменений схемы взаимосвязей активов.  • Возможность выполнения скриптов автоматизации на проинвентаризированных системой хостах.  • Наличие не менее 50 готовых различных скриптов автоматизации, сгруппированных по типу.  • Возможность добавления собственных скриптов автоматизации написанных на python, java, powershell, bash (при установке на хост соответствующего ПО).  Требования к модулю управления инцидентами подсистемы центрального управления  Требования к интеграции с внешними системами  В части получения инцидентов из внешних источников  • Интеграция с модулем управления событиями для получения инцидентов по результатам формирования оповещений с обратной синхронизацией статуса.  • Наличие универсальной интеграции с базами данных: Microsoft SQL Server, Oracle, PostgreSQL.  • Создание инцидентов из сообщений электронной почты с возможностью автоматического заполнения заданных полей.  • Создание инцидентов через интерфейс API:  o возможность заполнения заданных полей инцидента выбранными данными из внешней системы;  o возможность двухстороннего обмена данными – синхронизация статуса инцидента.  • Возможность задания расписания интеграции с внешними системами.  В части отправки инцидентов во внешние системы:  • Возможность отправки информации по инцидентам по электронной почте (протоколам IMAP, SMTP).  • Возможность передачи данных инцидентов в произвольные внешние системы путем взаимодействия с их REST API.  Требования к учету инцидентов  • Сбор, регистрация и обогащение информации по всем инцидентам ИБ из различных источников в единой системе.  • Ведение карточек инцидентов, содержащих сведения по инцидентам, прикрепленные файлы и дополнительную информацию.  • Возможность создавать инцидент как автоматически из внешних источников, так и вручную (в том числе с использованием предзаполненных шаблонов).  • Классификация инцидентов по категориям и типам с возможностью изменения категорий и типов любых инцидентов.  • Возможность назначения на инцидент уровня критичности в соответствии с настраиваемым справочником уровней критичности.  • Автоматическая фиксация даты и времени создания инцидента.  • Возможность прикрепления к инциденту файлов (с автоматическим расчетом контрольной суммы этих файлов (MD5, SHA-1)) и добавления метаданных к ним, возможность скачивания всех файлов по инциденту в виде архива. Для прикрепления файлов должен поддерживаться инструмент перемещения файла в рабочую область карточку (drag-and-drop).  • Возможность связывания инцидента с другими объектами системы (вручную или автоматически):  o активами (бизнес-процессы, информация, группы ИТ-активов, оборудование, бизнес-подразделения, персонал, пользовательские активы и иными типами активов, настроенными в системе);  o задачами;  o другими инцидентами.  • Контроль времени работы над инцидентом:  o добавление в карточку инцидента конфигурируемых счетчиков времени;  o назначение для счетчика лимита времени;  o индикация превышения лимита времени;  o управление счетчиком на уровне сценариев реагирования: остановка, запуск, назначение лимита;  o возможность вывода сводной информации по настроенным в инцидентах счетчикам времени на графиках в дашбордах.  • Возможность работы со списком инцидентов:  o поиск по списку;  o сортировка и фильтрация списка по одному или нескольким полям;  o сохранение пользователем фильтра списка для повторного использования;  o настройка перечня отображаемых полей в общем списке;  o создание нескольких режимов отображения инцидентов по заданному фильтру и возможность быстрого переключения между ними.  • Изменения, вносимые в карточку инцидента, должны журналироваться, независимо от источника изменений (пользователь, сценарий) и интерфейса, через который они внесены (UI, API)  • Возможность экспорта/импорта данных об инцидентах в файл в формате \*.xlsx. Возможность выбора полей при экспорте данных по инцидентам.  • Возможность уведомления пользователей при изменении в инцидентах, попадающих под заданные критерии. Возможность уведомления пользователя при добавлении в инцидент нового комментария.  • Возможность присвоения категории и типа инцидента по почтовому адресу отправителя письма при интеграции с почтовой системой.  • Возможность учета уровня ущерба от реализации инцидентов информационной безопасности.  Требования к полям и карточкам инцидентов  • Возможность производить индивидуальную настройку карточки инцидента для каждой категории (типа) инцидентов.  • Возможность добавления в карточку настраиваемых полей следующих типов: числовое поле, текстовое поле, многострочное текстовое поле, выпадающий список, числовое поле с денежным символом, дата и время, счетчик времени, чек-бокс, выбор пользователя.  • Возможность добавления в карточку таблиц, где колонками выступают поля перечисленных типов: текстовое поле, числовое поле, несколько текстовых строк, выпадающий список, числовое поле с денежным символом, дата, чек-бокс, выбор пользователя.  • Создание и редактирование собственных справочников для полей типа "выпадающий список".  • Настройка валидации для вводимых в текстовые поля значений. Возможность использования для валидации регулярных выражений, заранее преднастроенных и вынесенных в отдельный справочник.  • Возможность установки правила валидации вводимого значения для полей типа дата: разрешить ввод только будущих или только прошедших дат.  • Настройка предустановленных значений для полей.  • Настройка подсказок для полей.  • Отображение текстовых полей в виде гиперссылок с настраиваемым адресом ссылки и выводимым тестом.  • Возможность добавления в карточку инцидента кнопки для запуска выбранного сценария.  • Наличие конструктора представлений карточки инцидента, поддерживающего следующий функционал:  o настройка разного отображения карточки инцидента в зависимости от критериев, заданных в отношении значений произвольных полей, роли пользователя или сочетания данных критериев;  o настройка полей: скрыть, показать, запретить редактирование, скрыть пустое, сделать поле обязательным для заполнения, задать предустановленное значение, настроить справочник для полей типа "выпадающий список", сделав заданные значения полей недоступными для выбора.  o возможность объединения полей в именованные группы для логической организации полей инцидента, поддержка управления отображением группы по умолчанию - в свернутом или развернутом виде.  o возможность скрыть или показать разделы карточки инцидента;  o возможность назначить представление по умолчанию, которое будет применяться к карточке, если не было назначено никакое другое представление.  o возможность настройки зависимостей внутри представлений, позволяющих отображать значение одного поля в зависимости от значения другого.  • Возможность создать представление облегченной страницы Системы для отправки сообщений об инцидентах для определенных ролей пользователей без доступа ко всем вкладкам в интерфейсе продукта.  Требования к жизненному циклу инцидента  • Возможность реализации статусной модели инцидента в соответствии с заданными в организации процедурами.  • Гибкая настройка жизненного цикла инцидента:  o добавление в жизненный цикл произвольных статусов;  o настройка произвольных переходов между статусами жизненного цикла;  o настройка прав на осуществление перехода для отдельных пользователей и групп пользователей;  o настройка полей инцидента, заполнение которых в пользовательском интерфейсе является обязательным для осуществления перехода из одного статуса в другой;  o настройка разных жизненных циклов для разных категорий инцидентов.  Требования к функционалу совместной работы над инцидентами  • Разграничение доступа к инцидентам на основании:  o ролевой модели;  o дискреционных прав доступа;  o значений полей инцидента.  • Возможность настраивать отдельные права на создание, удаление, чтение и изменение инцидентов.  • Возможность задавать ограничение категорий (типов) инцидентов, которые может создавать пользователь.  • Назначение на инцидент ответственного пользователя:  o настройка автоматического назначения ответственного на основании критериев, заданных в полях инцидента;  o настройка автоматического назначения ответственного из заданной группы локальных пользователей на основании текущей загрузки.  • Возможность вести коммуникацию по каждому инциденту в отдельном встроенном чате:  o возможность упоминания в текстовом сообщении пользователя системы с его последующим уведомлением;  o отображение статуса работы пользователя в системе в системе реального времени: «активен», «не активен».  • Возможность вести почтовую переписку по инциденту в карточке, в рамках которой пользователи системы должны иметь возможность отправлять сообщения по электронной почте и получать ответы, при этом все письма должны храниться в системе и быть доступными для просмотра из карточки инцидента.  Требования к макрокорреляции и группировке  • Группировка инцидентов:  o объединение инцидентов в группы, где один инцидент является родительским, а остальные - дочерними;  o возможность как добавления инцидента в существующую группу, так и вывода инцидента из группы;  o вывод группы инцидентов в пользовательский интерфейс с возможностью свернуть/развернуть список инцидентов, входящих в группу;  o создание именованных типов групп. Настраиваемое для типа группы наследование полей внутри группы от родительского инцидента к дочернему и заполнение полей родительского из полей дочерних.  • Поиск похожих инцидентов по критерию совпадения значений полей.  • Возможность связывания найденных инцидентов с текущим и объединения их в группу.  Функциональные требования к автоматизации  Наличие возможности добавлять конфигурируемые сценарии (плейбуки), применяемые к инциденту.  • Сценарий должен состоять из действий, запускаемых в заданном порядке.  • Сценарий должен иметь возможность "ветвления" (параллельное выполнение разных последовательностей действий) и слияния "веток" (выполнение действия после завершения двух или более веток - всех или любой), в том числе в зависимости от действий пользователей, результатов предыдущих действий или значения переменных (значение поля в карточке инцидента).  • В сценарии должна присутствовать возможность использования условных операторов вида "if-else" и "case".  • Из одного сценария должна быть возможность инициировать запуск другого сценария.  • Для действий в сценарии должна присутствовать возможность отложенного запуска.  • Действия в сценарии должны работать со значениями полей инцидента на момент запуска действия (то есть в режиме реального времени).  • Поставляемые в составе системы действия должны обеспечивать возможность:  - автоматической отправки сообщений электронной почты с настраиваемым содержимым, в том числе с использованием значений из полей инцидента: с возможностью ожидания ответа и сохранения его содержимого; с возможностью автоматической генерации и прикрепления к письму отчета по инциденту; с возможностью сохранять все отправленные и полученные в рамках инцидента письма в соответствующем разделе карточки; с возможностью настраивать условия автоматического завершения действия - после отправки письма или после получения ответа от получателя; перед отправкой сообщения должна производится проверка статуса учетной записи пользователя в системе;  - автоматического создания в системе задачи с заданным содержимым с возможностью указывать в качестве исполнителей задач по инцидентам пользователей, ответственных за инцидент;  - автоматического назначения или изменения ответственного и назначение дискреционных прав доступа по инциденту;  - автоматической модификации полей инцидента (в том числе с возможностью записи в текстовые поля содержимого других полей), в том числе с возможностью указать текущую дату на момент выполнения действия или смещение от текущей даты в качестве значения поля типа "дата";  - запуска сканирования связанного с инцидентом оборудования;  - запуска скриптов и коннекторов к внешним системам, сконструированных пользователем (см. функциональные требования к механизмам оркестрации), в том числе с возможностью запуска в цикле до достижения заданного критерия остановки;  • Запуск сценария вручную.  • Запуск сценария автоматически при создании или изменении инцидента при совпадении критериев, заданных в отношении значений произвольных полей инцидента.  • Запуск сценария и выполнение действий в рамках него должны журналироваться.  • Должна присутствовать возможность приостановить выполнения сценария. После приостановки сценария должна присутствовать возможность его возобновления.  • Должна присутствовать возможность прервать выполнение как единичного действия в сценарии, так и сценария целиком.  • Для сценария должна настраиваться возможность его применения к инциденту - однократное применение, либо многократное.  • Возможность запуска вручную действий по отправке уведомления или запросу информации по email (в том числе с возможностью ожидания ответа), запуску скриптов и коннекторов, сканированию связанного оборудования, постановки задач непосредственно из карточки инцидента без необходимости создания для этого сценария.  • Возможность создавать переменные, значение которых будет содержать информацию из полей инцидента или пользовательскую информацию в текстовом формате, и использовать их в действиях по реагированию, в том числе в коннекторах.  Функциональные требования к механизмам оркестрации  • Возможность в графическом режиме конструировать коннекторы для взаимодействия с произвольными внешними системами.  • Возможность установки и запуска новых коннекторов без остановки Системы.  • Коннекторы должны поддерживать технологии: Powershell и cmd.exe; SSH; REST API; LDAP; MS SQL; MySQL; PostgreSQL; SNMP; SOAP.  • Возможность использования значения полей инцидента в теле коннектора.  • Возможность проверки подключения к внешней системе на этапе настройки коннектора.  • Возможность отладки коннектора в процессе его настройки с отправкой запроса и выводом его результата.  • Возможность копирования существующего коннектора в рамках работы с конструктором коннекторов.  • Возможность просмотра связанных объектов (сценариев и других коннекторов), на которые может повлиять изменение коннектора.  • Возможность работы REST-коннекторов через прокси-серверы.  • Возможность направления во внешние системы бинарных файлов через коннектор REST API.  • Возможность настройки выполнения коннектора на отдельно вынесенном коллекторе.  • Возможность настроить повторное выполнение действия "Запуск коннектора" с заданным тайм-аутом, приостановить или прервать выполнение сценария, если при первичном выполнении возникла ошибка.  • Возможность обработки результатов работы коннектора с использованием регулярных выражений и записи результатов обработки в одно или несколько полей инцидента.  • Возможность проверки подлинности SSL-сертификата для коннекторов типа REST и SOAP.  Требования к работе со сценариями в пользовательском интерфейсе  • Создание и редактирование сценариев в графическом режиме.  • Отображение сценариев, запущенных на инциденте, в графическом виде с возможностью просмотра как всех сценариев сразу, так и выбранного сценария.  • Отображение сценариев, запущенных на инциденте, в виде таймлайна с привязкой к временным меткам их запуска.  • Возможность просмотра действий "вложенного" сценария и обратная возможность свернуть их в компактный блок при запуске одного сценария из другого.  • Индикация действий при просмотре запущенного сценария: выполненных, выполняющихся в данный момент, запланированных и действий, выполнившихся с ошибкой, для которых должна быть возможность просмотреть текст ошибки, которая привела к его некорректному завершению.  • Возможность сохранения диаграммы выполнившихся на инциденте сценариев как изображения.  Требования к модулю управления уязвимостями подсистемы центрального управления  Требования к интеграции с внешними системами  • Импорт сведений по уязвимостям, уязвимом ПО.  • Возможность задания расписания интеграции со сканерами уязвимостей.  Требования к учету уязвимостей  • Учет и отображение результатов сканирования на основе сведений, полученных от сканеров уязвимостей, и (или) сервисов, предоставляющих сведения по уязвимостям, а также встроенного функционала сканирования.  • Отображение статистики по уязвимостям, зарегистрированным в системе, с возможностью фильтрации по уровню критичности, по типу оборудования, по наличию эксплойта, по портам, по вектору достижимости.  • Возможности работы со списком уязвимостей:  o поиск по списку уязвимостей;  o сортировка и фильтрация списка по одному или нескольким полям;  o сохранение пользователем фильтра списка уязвимостей;  o настройка перечня отображаемых полей в общем списке уязвимостей;  o создание нескольких режимов отображения уязвимостей по заданному фильтру и возможность быстрого переключения между ними (для каждого пользователя Системы).  • Возможность создания уязвимости вручную и настройки связи с уязвимым оборудованием, а также редактирования таких уязвимостей.  • Возможность экспорта данных об уязвимостях в файл в формате \*.xlsx.  • Наличие списка уникальных уязвимостей с отображением:  o количества связей уникальной уязвимости с уязвимым оборудованием;  o суммарного рейтинга открытых уязвимостей на оборудовании;  o распределения открытых уязвимостей на оборудовании по уровням критичности.  • Возможности работы со списком уникальных уязвимостей:  o поиск по списку уязвимостей;  o сортировка списка;  o настройка перечня отображаемых полей в общем списке уязвимостей;  o переход к списку уязвимостей с предварительной фильтрацией по уровню критичности и статусу.  Требование к полям и карточкам уязвимостей  • Отображение общей информации по каждой уязвимости в карточке.  • Отображение уровня критичности уязвимостей в зависимости от рейтинга уязвимости, возможность менять диапазоны значений рейтинга для уровней.  • Возможность писать комментарии к уязвимостям в разделе Уязвимости.  • Возможность добавления в карточку настраиваемых полей следующих типов: числовое поле, текстовое поле, многострочное текстовое поле, выпадающий список. Возможность редактирования пользовательских полей.  • Создание и редактирование собственных справочников для полей типа "выпадающий список".  Требования к жизненному циклу  • Учет следующих статусов для уязвимостей: открыта, закрыта, риск принят и ложное срабатывание, а также поддержка смены статусов вручную.  • Возможность создания собственных статусов жизненного цикла уязвимостей.  • Возможность смены статуса по выбранной уязвимости с указанием даты истечения статуса.  • Возможность группового изменения статуса уязвимостей.  Требования к автоматизации  • Автоматизированное управление уязвимостями: создание задач или инцидентов, изменение статуса, удаление уязвимостей по заданным критериям (атрибуты уязвимости, атрибуты уязвимого устройства, критичность группы ИТ активов или уязвимого устройства).  • Возможность указывать критерии-исключения, при которых политика не должна применяться.  • Приоритизация уязвимостей на основе настраиваемого рейтинга уязвимости. Для расчета рейтинга должна быть возможность использовать атрибуты самой уязвимости, оборудования и связанной с оборудованием группы ИТ-активов. Рейтинг должен пересчитываться автоматически не реже чем один раз в сутки.  • Возможность применения политик управления уязвимостями к уже существующим уязвимостям в базе системы.  Требования к модулю управления рисками подсистемы центрального управления  Требования к встроенным справочникам  • Наличие предустановленных каталогов угроз (собственная типовая база).  • Наличие предустановленного каталога защитных мер (собственная типовая база).  • Наличие предустановленных схем оценки рисков.  Требования к возможностям пользовательской настройки  • Возможность гибкой настройки схемы оценки рисков, которая может быть адаптирована под конкретную методику, используемую в организации. Возможность создания количественных параметров расчета (заполняемых вручную, вычисляемых по формуле или на основе значений взаимосвязанного параметра) и качественных (с заполнением значения вручную, из списка или на основе таблицы).  • Возможность настройки каталогов угроз, описывающих возможный перечень угроз безопасности, а также связанные с ними источники, предпосылки к реализации, защитные меры и затрагиваемые атрибуты безопасности.  • Возможность настройки потенциалов источников угроз, достаточности предпосылок реализации и эффективности защитных мер в отношении каждой угрозы каталога.  • Возможность копирования существующих в системе каталогов угроз.  • Возможность настройки критериев и уровней оценки ценности актива.  • Возможность ведения базы каталогов защитных мер, поддерживающей создание каталогов вручную или посредством импорта из excel.  • Возможность ведения базы внедренных защитных мер с возможностью их привязки к группам ИТ-активов, информационным активам и бизнес-процессам, в отношении которых они реализованы.  Требования к проведению оценки рисков  • Составление перечня активов, входящих в область оценки рисков, определение их ценности по параметрам конфиденциальности, целостности и доступности, а также их редактирования. Определение риск-аппетита активов.  • Возможность указывать влияние связанных активов друг на друга в контексте потенциального нарушения атрибутов безопасности одного из них.  • Возможность проведения оценки рисков информационной безопасности для групп ИТ-активов, а также связанных с ними бизнес-процессов и обрабатываемой информации.  • Возможность автоматического поиска рисков из каталога, актуальных в отношении заданной области оценки, на основе заполнения опросников об актуальных источниках и предпосылках.  • Автоматический расчет уровня риска на основе вероятности, ущерба и/или других параметров в соответствии с заданной схемой (методикой) оценки.  • Возможность учета ценности актива, потенциала нарушителей, сведений о реализованных защитных мерах и их эффективности при оценке рисков.  • Возможность просмотра перечня инцидентов, связанных с риском, которые были выявлены в организации.  • Визуальная маркировка рисков, превысивших установленный для актива допустимый уровень.  • Учет производных рисков (в случае, если ценность одного актива влияет на ценность другого актива).  Требования к обработке рисков  • Возможность формирования плана обработки рисков на определенный период и его сопоставление с имеющимся бюджетом на информационную безопасность.  • Возможность включения в план обработки мероприятий по внедрению защитных мер из каталога организации.  • Автоматический пересчет целевого уровня риска по мере формирования плана обработки с целью сравнения его с изначальным (текущим) уровнем риска для оценки эффективности мероприятий.  • Возможность сравнения различных сценариев по обработке рисков.  • Возможность прикрепления документов и формирования комментариев к мероприятиям по обработке рисков (внутри оценки и в общем плане обработки рисков).  Требования к работе с результатами оценки рисков  • Возможность фиксации оценки рисков ИБ для утверждения сформированной карты рисков и плана их обработки, а также для обеспечения анализа изменений отдельных рисков с течением времени.  • Возможность просмотра сводной информации по рискам - списка всех рисков (включая источники угроз и предпосылки), выявленных при проведении оценок.  • Подготовка документов, фиксирующих результаты оценки рисков (сводный реестр рисков, план обработки рисков и т. д.).  • Возможности для анализа рисков, включенных в карту рисков организации: наличие перечня факторов риска, ставших причиной его возникновения; перечня защитных мер, уже реализованных в отношении риска; перечня запланированных мероприятий по обработке; перечня произошедших инцидентов, связанных с риском; возможность отслеживания изменения уровня риска на основе исторических оценок.  • Наличие единого плана обработки рисков, включающего мероприятия по всем рискам, актуальным для активов организации, с возможностью отслеживания их статуса и сроков исполнения.  • Возможность ведения архива реализованных мероприятий по обработке рисков.  • Учет результатов предыдущей оценки рисков актива при создании новой: автоматическое включение уже идентифицированных рисков из Карты рисков организации, предзаполнение опросников по факторам риска, включение незавершенных мероприятий по обработке рисков.  • Визуальное представление информации по текущим рискам информационной безопасности и схемам обработки рисков (графики).  Требования к совместной работе  • Возможность назначить рабочую группу для проведения оценки с указанием ролей участников Участник или Наблюдатель.  • Возможность привлечения экспертов для оценки отдельных, назначенных им, рисков.  • Возможность настройки принципа обработки оценки параметров риска от нескольких экспертов.  Требования к модулю управления аудитами подсистемы центрального управления  Требования к встроенным справочникам  • Наличие предустановленных нормативно-правовых актов и стандартов в области обеспечения ИБ:  o ISO 27001:2013  o ISO 27001:2022  o ISO/IEC 27001:2013/DAM 1:2022  o ISO/IEC 27002:2022  Требования к работе с аудитами  • Возможность проведения аудитов в отношении групп ИТ-активов, бизнес-процессов, подразделений, помещений и оборудования.  • Возможность проведения комплексных проверок (сводных аудитов), объединяющих в себе несколько аудитов: в отношении разных активов и/или по разным стандартам. Возможность управления простыми аудитами из интерфейса сводок: смена статуса, редактирование рабочей группы, оценка требований. Возможность просмотра карточек активов, входящих в область оценки аудитов, из карточки аудита. Возможность анализа результата входящих проверок с помощью встроенного дашборда, включающего: информацию о расчетах уровня соответствия, созданных отчетах, статистику выявленных нарушений и данные по их обработке.  • Наличие в системе динамического плана проверок, позволяющего осуществлять мониторинг сроков, статусов и прогресса проведения аудитов, а также сравнивать плановые и фактические даты проведения.  • Возможность работы с реестром проверок: сортировка и фильтрация списка по одному или нескольким полям, настройка перечня отображаемых полей в общем списке проверок, сохранение пользователем фильтра для повторного использования, создание нескольких режимов отображения реестра по заданному фильтру и возможность быстрого переключения между ними.  • Возможность ведения в свойствах активов перечня действующих в их отношении нормативно-правовых документов, в т.ч. автоматически на основе атрибутов актива.  • Возможность формирования динамического плана проверок из реестра активов: наличие в карточке актива информации, необходимой для планирования (перечень уже запланированных проверок, даты их проведения и статус, выявленные ранее замечания, запланированные работы); режим быстрого создания аудита из свойств актива; возможность автоматического включения в комплексную проверку аудитов по связанным активам с учетом действующих в их отношении документов (проверки по дочерним системам, входящему оборудованию и т.д.).  • Возможность отправки уведомлений о создании новых аудитов, приближении запланированных проверок, нарушении плановых дат проведения проверок, а также об изменении статуса аудита.  • Возможность копирования существующей оценки соответствия для проведения повторной оценки на основании скопированной.  • Возможность выставления аудитором оценки требований посредством выбора ответа по шкале с последующим автоматическим перерасчетом уровня соответствия актива документу.  • Возможность маркировки требований, неприменимых в отношении актива, с последующим исключением их из расчета уровня соответствия.  • Возможность импорта результатов оценки аудита из Excel-файлов.  • Возможность прикрепления свидетельств проверки к оцениваемым требованиям нормативного документа.  • Возможность выгрузки всех свидетельств, прикрепленных к требованиям внутри аудита, в один клик с автоматическим разбиением файлов на папки, соответствующие вопросам аудита.  • Формирование пакета 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).  • Возможность прикреплять отчеты и другие документы к аудитам информационной безопасности (например, отчет аудиторов по итогам внешнего аудита).  • Блокировка любых изменений внутри проверки после её перевода в статус «Завершено».  Требования к работе с замечаниями  • Возможность заведения замечаний в отношении не выполняющихся требований с указанием критичности, ответственных и сроков для отслеживания прогресса по их устранению.  • Автоматическая связь новых замечаний с проверяемым активом, автором замечания, нарушаемым требованием и аудитом.  • Возможность просмотра исторических замечаний, заведенных в рамках предыдущих проверок, для анализа успешности их устранения и выявления повторяющихся замечаний.  • Возможность формирования плана по устранению замечаний аудита, включая автоматическое создание задач на основе плана для передачи исполнителям.  • Возможность заведения замечаний и мероприятий по их устранению с использованием шаблонов с целью систематизации данных и сбора статистики.  • Автоматический поиск покрываемых мероприятием замечаний при заведении мероприятия по шаблону на основе имеющейся связи с требованием.  • Возможность декомпозиции мероприятий из плана по устранению на подзадачи, включая возможность быстрого создания отдельных подзадач для всех затрагиваемых активов.  • Автоматическое закрытие замечаний по мере завершения задач, включенных в план по их устранению.  • Возможность импорта замечаний из файлов в формате Excel.  • Возможность работы с реестром замечаний и планом их обработки: сортировка и фильтрация списка по одному или нескольким полям, настройка перечня отображаемых полей в общем списке проверок, сохранение пользователем фильтра для повторного использования, создание нескольких режимов отображения реестра по заданному фильтру и возможность быстрого переключения между ними.  Требования к совместной работе  • Возможность указания сразу нескольких пользователей менеджерами (ответственными) аудита, а также возможность назначения разных менеджеров на комплексную проверку и входящие в неё аудиты.  • Гибкое формирование рабочих групп: возможность предоставления экспертам доступа к отдельным частям опросного листа проверки, касающихся зоны их компетенций; возможность предоставления экспертам доступа лишь на определенных этапах проведения проверок.  Требования к функционалу контрольных проверок  • Возможность отслеживания связи между схожими требованиями различных нормативных документов.  • Возможность создания собственных комплексов контрольных проверок и настройки их связей с объединяемыми ими требованиями – вручную или посредством импорта через excel.  • Возможность настройки шкал для оценки контрольных проверок.  • Автоматическое формирование перечня контрольных проверок для активов на основании действующих в их отношении нормативно-правовых документов.  • Возможность регулярной оценки соответствия актива назначенным ему контрольным проверкам и настройки периодичности осуществляемого контроля.  • Возможность настройки рабочей группы (ответственные/аудиторы) для контрольных проверок.  • Автоматическое уведомление участников рабочей группы о приближающемся сроке проверки.  • Обязательная фиксация обоснования выставленных оценок участниками рабочей группы.  • Возможность прикрепления документов, подтверждающих выставленную оценку.  • Возможность просмотра замечаний, выявленных в ходе аудитов по требованиям, покрываемым контрольной проверкой.  • Возможность просмотра истории ранее выставленных оценок, включая: дату оценки, список подтверждающих документов и автоматическая индикация прогресса (ухудшение или улучшение по сравнению с предыдущей оценкой).  • Возможность автоматического переноса результатов оценки контрольных проверок в аудиты для быстрой оценки схожих требований, встречающихся в различных нормативных документах.  • Учет коэффициентов требований, различий в их шкалах оценки и количества полей для оценки аудитором при автоматическом переносе оценок контрольных проверок.  • Возможность просмотра замечаний по схожим требованиям, выявленным в ходе других проверок.  Требования к модулю управления задачами подсистемы центрального управления  Требования к возможностям пользовательской настройки  • Возможность настройки состава и порядка полей для разных типов задач.  • Возможность настройки полей, обязательных для создания задачи, а также полей, обязательных для заполнения при переходе из одного статуса в другой  Требования к работе с задачами  • Возможность работы с реестром задач: сортировка и фильтрация списка задач по одному или нескольким полям, сохранение пользователем фильтра списка задач для повторного использования, настройка перечня отображаемых полей в реестре задач, сохранение пользователем и повторное использование заданного условия фильтрации реестра, создание нескольких режимов отображения реестра задач по заданному фильтру и быстрого переключения между ними.  • Наличие связи задач с активами, инцидентами, уязвимостями, документами. Возможность просмотреть существующие связи между этими сущностями и создать новые.  • Возможность перехода из карточки задачи к связанным с ней сущностям (активы, инциденты и уязвимости).  • Контроль сроков исполнения задач. Возможность настроить уведомления по задачам с истекающим сроком исполнения и по задачам, срок исполнения которых истек.  • Визуализация состояния задач, индикация важности (критичности) задач, а также задач с просроченным сроком исполнения.  • Учет и просмотр истории выполнения задач.  • Хранение и учет документов, связанных как с постановкой задачи, так и с результатами её исполнения.  • Возможность заведения подзадач вручную с привязкой к основной задаче, которые будут автоматически влиять на её статус.  • Возможность создания задач вручную из карточек различных объектов системы (пользовательские активы, документы, мероприятия по устранению замечаний, инциденты)  • Возможность создать задачу по нескольким активам типа ПО или по нескольким пользовательским активам из контекстного меню при групповом выделении активов.  • Возможность импорта задач из файлов в формате Excel.  • Возможность экспорта сведений по задачам в файл в формате Microsoft Excel.  • Наличие индикатора, отражающего прогресс устранения уязвимостей (прогресс-бар), для типа задач, связанных с устранением уязвимостей.  • Возможность отображения иерархии и пользовательских полей для задач, связанных с инцидентом.  Требования к совместной работе  • Отображение задач в зависимости от роли пользователя.  • Наличие чата для обмена сообщениями между участниками группы пользователей, привлеченных к задаче.  Требования к модулю управления документами подсистемы центрального управления  Требования к возможностям пользовательской настройки  • Возможность создания различных типов документов (приказы, инструкции, политики и пр.) и индивидуальной настройки состава полей для каждого типа документа.  Требования к учету документов  • Возможность ведения документации по информационной безопасности в едином хранилище.  • Возможности работы со списком документов: настройки столбцов, отображаемых пользователю при работе с реестром документов, поиска по списку документов, сортировки и фильтрации списка по одному или нескольким полям, сохранения пользователем и повторного использования заданного условия фильтрации реестра, создания вкладок с заданным условием фильтрации.  • Возможность создания документов вручную или с помощью импорта из excel.  • Возможность загрузки вложений в любом формате к карточке документа (с автоматическим расчетом контрольной суммы для загруженного файла).  • Возможность скачивать вложения из карточки документа как по одному файлу, так и все вложения одним архивом.  • Возможность управления жизненным циклом документа. Указание срока действия документа, а также возможность автоматического уведомления ответственных пользователей при наступлении установленной даты пересмотра документа.  • Возможность привязки документов к активам разных типов (группы ИТ-активов, информация, бизнес-процессы, подразделения).  • Возможность прикрепления документов из общей базы к активам, инцидентам, мерам защиты, задачам, оценкам рисков, аудитам, замечаниям, мероприятиям по устранению замечаний.  • Возможность группового редактирования связей документа(ов) с активами.  • Отображение в карточке документа требований, в которых он используется в качестве свидетельств.  • Возможность просмотра истории ранее внесенных изменений в карточку документа.  Требования к совместной работе с документами  • Возможность настройки рабочей группы пользователей, ответственных за документ. Для каждого участника должна быть обеспечена возможность настройки уровня доступа (чтение, изменение).  • Возможность быстрого предоставления доступа к документу на чтение всем сотрудникам организации.  Требования к модулю визуализации и представления данных подсистемы центрального управления  Требования к работе с дашбордами  • Возможность создания вкладок, содержащих разные панели, с отображением карт, сетей, планов помещений и схем визуализации активов, статистики по инцидентам и возможность быстрого переключения между панелями.  • Визуализация информации в виде диаграмм, графиков и интерактивных схем. Возможность настраивать количество, размер и расположение графиков на дашборде.  • Автоматическое и ручное обновление пользовательских графиков на дашбордах с возможностью просмотра времени последнего обновления.  • Визуализация активов и инцидентов 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 ресурсно-сервисной модели представления данных, отображение взаимосвязей между физическими и информационными активами, их автоматическая отрисовка на схемах на основе существующих в системе связей.  • Возможность просматривать карты сетей (схемы, отображающие оборудование и сети, входящие в состав группы ИТ-активов) и схемы взаимосвязей (схемы, отображающие связанные активы) для групп ИТ-активов.  • Возможность визуализации инцидентов ИБ на схемах, позволяющих отображать их связи с различными элементами Системы (например, ИТ-активами), а также представления значения отдельных полей.  • Индикация на схеме L3 и плане помещения активов, на которых обнаружены уязвимости, активов, на которых зарегистрированы инциденты 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 инцидентах, сведения об уязвимостях).  • Возможность создавать группы для логической группировки графиков. В Системе должен быть доступен поиск, краткое описание и предварительный просмотр графиков.  Требования к предустановленным шаблонам графиков  В Системе должен быть предустановлен следующий перечень графиков:  • общий график состояния бизнес-процессов организации.  • защищенность персонала по подразделениям;  • история оборудования (по группе ИТ-активов);  • история открытых уязвимостей (по группе ИТ-активов);  • количество открытых уязвимостей (по группам активов, сетям);  • количество открытых уязвимостей по сетям;  • статистика количества инсталляций по группам ПО;  • статистика количества оборудования по группам активов;  • статистика количества оборудования по сетям;  • статистика по операционным системам;  • статистика по типам оборудования;  • статистика количества пользователей по привилегиям;  • инциденты в работе;  • инциденты по статусам обработки;  • инциденты по ответственным (с указанием уровня критичности/статуса);  • инциденты по типам;  • инциденты по объектам инфраструктуры;  • инциденты по подразделениям;  • история инцидентов;  • доля инцидентов с соблюдением срока реагирования;  • предотвращенный ущерб от инцидентов;  • среднее время реагирования на инциденты;  • ущерб от реализации инцидентов.  • распределение рисков для актива (качественная/количественная оценка).  • схема обработки рисков по активу (качественная/количественная оценка).  • статус мероприятий по обработке рисков.  • история изменений уровня рисков по активу (качественная/количественная оценка).  • обзор уровня соответствия объектов нормативным требованиям.  • выполнение требований нормативного документа по объекту.  • обзор открытых замечаний по объекту.  • история изменений показателей соответствия по объекту.  Требования к совместной работе с графиками  • Возможность настройки прав доступа пользователей к дашбордам и объектов, в отношении которых доступно построение графиков.  • Возможность отображения разных панелей визуализации для разных групп пользователей.  • Возможность индивидуальной настройки панелей визуализации для разных пользователей одной группы.  • Возможность сохранения настроенного отображения карты/сети/других элементов для каждого пользователя.  Требования к модулю управления отчетностью подсистемы центрального управления  Требования к работе с отчетами  • Подготовка, генерация и просмотр отчетов на основе исторических данных, накапливаемых в Системе;  • Наличие предустановленных отчетов, соответствующих основным функциям Системы.  • Наличие встроенных средств для создания новых и модификации существующих отчетов;  • Возможность модификации встроенных шаблонов отчетов без применения HTML-разметки, языков программирования.  • Формирование отчетов вручную и автоматически согласно заданному расписанию.  • Возможность автоматически добавлять отчеты в базу документов в Системе.  • Экспорт отчетов в файлы различных форматов, таких, например, как переносимый формат данных (PDF), DOCX;  • Экспорт карт, планов помещений в графическом формате.  • Возможность автоматической рассылки сформированных отчетов заданным группам потребителей с использованием корпоративной электронной почты.  Требования к предустановленным отчетам  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 инцидентам ИБ – в отчете должна содержаться общая информация по произошедшим и зарегистрированным в Системе инцидентам ИБ;  • Отчет по текущему инциденту – в отчете должна содержаться детализированная информация по выбранному инциденту ИБ;  • Инциденты по группам ИТ-активов – отчет должен отображать распределение инцидентов по группам ИТ-активов за выбранный период;  • Отчет по бизнес-подразделениям – отчет должен отображать распределение инцидентов по бизнес-подразделениям за выбранный период;  • Отчет по территориальным подразделениям – отчет должен содержать статистику инцидентов по всем территориальным подразделениям за выбранный период;  • Отчет, содержащий данные о количестве инцидентов за период времени, находящихся в работе, закрытых инцидентах, их распределению по уровням критичности, категориям и типам;  • Сводка по задачам – отчет должен содержать детализированный перечень сведений по задачам, включая отражение их статуса;  • Отчет, отображающий количество открытых и закрытых инцидентов, за которые ответственны отдельные сотрудники. Возможность построения отчета по всем или по отдельным подразделениям;  • Отчет по обновлениям для Группы ИТ-активов;  • Отчет по ПО для Группы ИТ-активов, отчет по ПО для хоста.  • Детализированный отчет по результатам оценки выполнения требований – отчет должен содержать перечень оцениваемых требований/критериев с указанием степени выполнения по выбранному аудиту.  • Отчет по сводному аудиту – отчет должен содержать подробную информацию по результатам оценки соответствия выбранных аудитов и областей оценки с указанием выявленных замечаний.  • План-график проведения аудитов.  • Сводный отчет по соответствию – отчет должен содержать общую информацию по соответствию различным требованиям для выбранной области оценки.  • Сравнительный отчет по аудитам – отчет должен содержать сравнительные характеристики по всем проводимым аудитам выбранного требования.  • Детализированный реестр рисков – отчет должен содержать подробную информацию-описание активов с перечнем выявленных рисков информационной безопасности.  • План обработки рисков.  • Сводный реестр рисков – отчет должен содержать реестр выявленных рисков для выбранных активов.  Требования к модулю взаимодействия с системой через API  • Система должна поддерживать GET и POST методы запросов.  • Система должна использовать токены для авторизации в API.  Система должна поддерживать следующий набор запросов для использования в API:  Требования к запросам для работы с графиками: получение списка пользовательских графиков, получение данных пользовательского графика.  • Запрос на получение информации о системе.  Требования к запросам для работы с пользовательскими активами: получение списка типов пользовательских активов, в т.ч. с учетом фильтрации, создание и редактирование пользовательского актива, получение истории пользовательских активов.  Требования к запросам для работы с подразделениями  Требования к запросам для работы с организациями:  Требования к запросам для работы с ролями и пользователями  Требования к запросам для работы с персоналом  Требования к запросам для работы с бизнес-процессами  Требования к запросам для работы с оборудованием  Требования к запросам для работы с инцидентами  Требования к запросам для работы с комментариями к инцидентам:  Требования к запросам для работы с уязвимостями  Требования к запросам для работы с задачами  Требования к запросам для работы с документами   * + 1. **Система защиты сетевого периметра и контроля доступа между сетевыми сегментами**   **Требования к инструментам защиты сети:**  Предлагаемая программно-аппаратная продукция должна состоять из двух программно-аппаратных сетевых экранов (Next-Generation Firewall – NGFW) с возможностью выявления и предупреждения угроз (Intrusion Detection / Prevention Systems - IDS/IPS) для каждой площадки (внешнего и внутреннего периметра).  Программно-аппаратные сетевые экраны должны поддерживать отказоустойчивость;  Предлагаемый NGFW должен соответствовать стандартам ISO 27001, ISO 27017, ISO 27018, ISO 27701, SOC2, FedRAMP, Germany C5, Common Criteria, FIPS 140-2, CMVP, NCSC Foundation, ANSSI, DoDIN, CSfC, USGV6, ICSA и NEBS.  Оборудование должно актуальным, не вышедшим из поддержки и протестированным на заводах производителя. Вся необходимая техническая документация и руководства пользователя должны быть предоставлены в полном объеме, предусмотренном производителем. В комплект поставки должны входить все необходимые принадлежности для обеспечения работоспособности поставляемого Оборудования.  **Требования к производительности:**  **Для внутренней площадки:**  Пропускная способность устройства в режиме сетевого экранирования с обеспечением идентификации приложений и пользователей – не менее 43.5 Гбит/сек.  Пропускная способность устройства в режиме предупреждения и защиты от угроз (Application Control, IPS, Anti-Virus, Anti-spyware или Anti-bot, Zero Day Attacks Detection and Analysis и логирование на устройстве) – не менее 26.7 Гбит/сек; Этот показатель должен быть измерен с пакетами appmix. Эти данные должны быть опубликованы на официальном сайте производителя.  Пропускная способность функционала IPsec VPN должна быть не менее 21 Гбит/сек.  Устройство должно поддерживать не меньше 10 000 site to site туннелей.  Максимальное количество новых сессий в секунду – не менее 270 000.  Максимальное количество поддерживаемых сессий – не менее 3 600 000.  Система должна поставляться с максимальным количеством памяти, которую она поддерживает и позволяющую хранить журналы сроком не менее 6 месяцев.  Устройство должно состоять из двух программно и аппаратно разделенных компонент – компоненты управления устройством и компоненты обработки трафика. Каждый компонент должен иметь свой набор процессоров (CPU), оперативной памяти (RAM) и интерфейсов (Ethernet port). Компоненты управления и обработки трафика должны быть независимы друг от друга для того, чтобы предоставить возможность управления устройством в случае критической нагрузки трафиком, в частности, во время DoS/DDoS атак.  Устройство должно иметь следующие интерфейсы:  По меньшей мере 8 медных порта стандарта 100/1000/10G Copper.  Не менее 12 оптических портов стандарта 1/10G SFP/SFP+.  По меньшей мере 4 оптических порта стандарта 25G SFP28.  По меньшей мере 4 оптических порта стандарта 40/100G QSFP+/QSFP28  Порт управления (Management port) должен быть программно изолирован и аппаратно находиться отдельно от сетевых портов для обработки трафика. Порт управления (Management port) должен поддерживать отказоустойчивость (Management HA port) на устройстве.  Поддержка виртуальных маршрутизаторов – не менее 20 шт.  Наличие лицензии не менее 10 виртуальных файерволов, с возможностью расширения - от 20 и более.  Предлагаемая система должна иметь пару жестких дисков SSD типа размером не менее 480 ГБ.  Поддержка статической маршрутизации IPv4/IPv6 и протоколов динамической маршрутизации BGPv4, OSPFv2/v3, RIP v2. Если этот функционал требует лицензии, то она должна быть включена в предложение.  Поддержка работы сетевых интерфейсов в режимах прослушивания «дублирующего» трафика с подключаемого Span-портов коммутационного оборудования (TAP), в прозрачном режиме без изменения MAC и IP-адрес (Virtual Wire), в режиме коммутации трафика (Layer 2), в режиме маршрутизации трафика (Layer 3).  Поддержка одновременной работы разных сетевых интерфейсов в любых перечисленных режимах в любой комбинации, без ограничений в рамках одного виртуального сетевого экрана.  Поддержка изменения режима работы портов (Layer 2, Layer 3, прозрачный режим и режим прослушивания) без необходимости перезагружать устройство.  Поддержка Static и Dynamic (Hide) NAT.  Поддержка NAT в прозрачном режиме.  Поддержка IPV6, включая идентификацию приложений и пользователей.  Поддержка multicast маршрутизации и протоколов – PIM-SM, PIM-SSM, IGMP v1, v2, v3.  Поддержка маршрутизации между VLAN, организованными на сетевом экране.  Устройство должно поддерживать не менее 4000 vlan.  Поддержка функционала трансляции адресов NAT, сервера DHCP и DHCP relay.  Поддержка тегирования фреймов по 802.1.  Поддержка агрегирования интерфейсов по 802.3ad (поддержка LACP).  Поддержка передачи более крупных пакетов (Jumbo frames).  Поддержка SNMPv3.  Поддержка Netflow. Профиль Netflow должен определяться на основе физических портов.  Поддержка протокола LLDP (Link Layer Discovery Protocol). Таким образом, устройство должно иметь возможность подавать информацию о других устройствах (адрес MAC, имя системы, подключенный к нему порт).  Поддержка политики Policy Based Forwarding для IPv4 и IPv6 протоколов.  Поддержка BFD (Bidirectional Forward detection). Это позволит быстрее адаптироваться к любым изменениям на уровне маршрутизации.  Поддержка виртуальных маршрутизаторов – не менее 20 шт.  Наличие лицензии на 10 виртуальных файерволов, с возможностью расширения - до 20.  Поддержка зон безопасности – не менее 4 000 шт.  Поддержка site-to-site и client-to-site IPSec VPN.  Число максимально возможных Client SSL VPN – не менее 15 000.  Число максимально возможных Clientless VPN – не менее 2 500.  Число IPSEC VPN туннелей (Site to site) – не менее 10 000.  Число одновременных сеансов расшифровки SSL – не менее 360 000.  Поддержка проверки угроз и проверка содержимого туннельных протоколов: GRE до 2 уровней, GTP-U, нешифрованных IPSEC: ESP-null или AH.  **Для внешней площадки:**  Пропускная способность устройства в режиме сетевого экранирования с обеспечением идентификации приложений и пользователей – не менее 20.5 Гбит/сек.  Пропускная способность устройства в режиме предупреждения и защиты от угроз (Application Control, IPS, Anti-Virus, Anti-spyware или Anti-bot, Zero Day Attacks Detection and Analysis и логирование на устройстве) – не менее 10.5 Гбит/сек; Этот показатель должен быть измерен с пакетами appmix. Эти данные должны быть опубликованы на официальном сайте производителя.  Пропускная способность функционала IPsec VPN должна быть не менее 12 Гбит/сек.  Устройство должно поддерживать не меньше 10 000 site to site туннелей.  Максимальное количество новых сессий в секунду – не менее 240 000.  Максимальное количество поддерживаемых сессий – не менее 2 500 000.  Система должна поставляться с максимальным количеством памяти, которую она поддерживает и позволяющую хранить журналы сроком не менее 6 месяцев.  Устройство должно состоять из двух программно и аппаратно разделенных компонент – компоненты управления устройством и компоненты обработки трафика. Каждый компонент должен иметь свой набор процессоров (CPU), оперативной памяти (RAM) и интерфейсов (Ethernet port). Компоненты управления и обработки трафика должны быть независимы друг от друга для того, чтобы предоставить возможность управления устройством в случае критической нагрузки трафиком, в частности, во время DoS/DDoS атак.  Устройство должно иметь следующие интерфейсы:  По меньшей мере 12 медных порта стандарта 100/1000/10G Copper.  Не менее 10 оптических портов стандарта 1/10G SFP/SFP+.  По меньшей мере 4 оптических порта стандарта 25G SFP28.  По меньшей мере 2 оптических порта стандарта 40/100G QSFP+/QSFP28  Порт управления (Management port) должен быть программно изолирован и аппаратно находиться отдельно от сетевых портов для обработки трафика. Порт управления (Management port) должен поддерживать отказоустойчивость (Management HA port) на устройстве.  Поддержка виртуальных маршрутизаторов – не менее 11 шт.  Наличие лицензии не менее 1 виртуальных файерволов, с возможностью расширения - от 11 и более.  Предлагаемая система должна иметь пару жестких дисков SSD типа размером не менее 480 ГБ.  **Требования к поддерживаемым протоколам и режимам функционирования ПАК:**  - Поддержка статической маршрутизации IPv4/IPv6 и протоколов динамической маршрутизации BGPv4, OSPFv2/v3, RIP v2. Если этот функционал требует лицензии, то она должна быть включена в предложение.  - Поддержка работы сетевых интерфейсов в режимах прослушивания «дублирующего» трафика с подключаемого Span-портов коммутационного оборудования (TAP), в прозрачном режиме без изменения MAC и IP-адрес (Virtual Wire), в режиме коммутации трафика (Layer 2), в режиме маршрутизации трафика (Layer 3).  - Поддержка одновременной работы разных сетевых интерфейсов в любых перечисленных режимах в любой комбинации, без ограничений в рамках одного виртуального сетевого экрана.  - Поддержка изменения режима работы портов (Layer 2, Layer 3, прозрачный режим и режим прослушивания) без необходимости перезагружать устройство.  - Поддержка Static и Dynamic (Hide) NAT.  - Поддержка NAT в прозрачном режиме.  - Поддержка IPV6, включая идентификацию приложений и пользователей.  - Поддержка multicast маршрутизации и протоколов – PIM-SM, PIM-SSM, IGMP v1, v2, v3.  - Поддержка маршрутизации между VLAN, организованными на сетевом экране.  - Устройство должно поддерживать не менее 4000 vlan.  - Поддержка функционала трансляции адресов NAT, сервера DHCP и DHCP relay.  - Поддержка тегирования фреймов по 802.1.  - Поддержка агрегирования интерфейсов по 802.3ad (поддержка LACP).  - Поддержка передачи более крупных пакетов (Jumbo frames).  - Поддержка SNMPv3.  - Поддержка Netflow. Профиль Netflow должен определяться на основе физических портов.  - Поддержка протокола LLDP (Link Layer Discovery Protocol). Таким образом, устройство должно иметь возможность подавать информацию о других устройствах (адрес MAC, имя системы, подключенный к нему порт).  - Поддержка политики Policy Based Forwarding для IPv4 и IPv6 протоколов.  - Поддержка BFD (Bidirectional Forward detection). Это позволит быстрее адаптироваться к любым изменениям на уровне маршрутизации.  - Поддержка виртуальных маршрутизаторов – не менее 11 шт.  - Наличие лицензии на 1 виртуальный файервол, с возможностью расширения - до 11.  - Поддержка зон безопасности – не менее 200 шт.  - Поддержка site-to-site и client-to-site IPSec VPN.  - Число максимально возможных Client SSL VPN – не менее 2 000.  - Число максимально возможных Clientless VPN – не менее 200.  - Число IPSEC VPN туннелей (Site to site) – не менее 8 000.  - Число одновременных сеансов расшифровки SSL – не менее 250 000.  - Поддержка проверки угроз и проверка содержимого туннельных протоколов: GRE до 2 уровней, GTP-U, нешифрованных IPSEC: ESP-null или AH.  **Требования к отказоустойчивости ПАК:**  Поддержка построения отказоустойчивого кластера высокой доступности High-Availability (HA) – Active/Passive и одновременной работы обоих межсетевых экранов кластера в активном режиме – Active/Active.  Поддержка режима работы HA Clustering с синхронизацией состояния сессий между брандмауэрами в кластере высокой доступности (HA).  Режим работы HA Clustering должен поддерживать горизонтальное масштабирование NGFW до 8 устройств, а также работу с несколькими разнесенными датацентрами.  Для переключения между компонентами кластера должен производиться мониторинг интерфейсов (interface monitoring) и пути к указанным ресурсам (path monitoring).  **Требования к функционалу системы ПАК:**  Устройство должно контролировать состояние сессий (Stateful inspection) с фильтрацией пакетов и идентификацией приложений.  Устройство должно быть зонным сетевым экраном (Zone-based). Один или несколько интерфейсов или субинтерфейсов могут принадлежать одной зоне. Политики доступа (security rules) и политики NAT должны быть основаны на зонах.  Политики NAT должны иметь набор правил, независимо от политик доступа (security rules).  Распознавание и блокировка сетевых приложений на седьмом уровне модели OSI по трафику, проходящей через сетевой экран, в том числе индивидуально для всех приложений, использующих общий порт; в том числе 80 и 443, использующих динамические TCP/UDP-порты.  Распознавание трафика инспектируемого на Layer-7 модели OSI по сигнатурам, следующему программному обеспечению (приложениям), протоколам или сервисам:  - сервисов аутентификации, включая Microsoft Active Directory, LDAP, RADIUS, TACACS+, Kerberos, SAML, Syslog Monitoring/Parser (Устройство должно поддерживать сопоставление user-to-ip, обрабатывая сообщения от Syslog);  - СУБД, включая Microsoft SQL, Oracle и т.п.;  - файловые сервисы, включая Microsoft SMB;  - систем электронного документооборота и обмена сообщениями, включая Microsoft Sharepoint, Exchange, Office 365, Google Docs;  - протоколы обмена по электронной почте: SMTP, POP3, IMAP;  - протоколы VOIP и аудио-видео-конференций, включая SIP, H.323, H.245, H.225, Webex, потокового аудио-видео (независимо от веб-сайта), аудио и видео по HTTP;  - сервисов обновления программного обеспечения, включая Microsoft Update, антивирусного ПО, Adobe, Java;  - сервисов резервного копирования;  - сервисов виртуализации и терминального доступа, включая Vmware, Microsoft RDP;  - протоколы дистанционного доступа, включая Telnet, SSH, VNC, Radmin;  - сетевые протоколы, включая протоколы динамической маршрутизации и SSL/IPSec VPN;  - социальных сетей, средств мгновенного обмена сообщениями;  - средств публикации рабочего стола и предоставления дистанционного доступа, включая Team-Viewer;  - внешних прокси-серверов и анонимайзеров, включая Tor, Ultrasurf, Freegate, SOCKS, PHP Proxy;  - средств построения VPN и туннелей поверх других приложений, включая Freenet, Open-vpn, Vtun, RDP-to-TCP, TCP-over-Dns.  Решение должно поддерживать режим "Безопасный поиск" для YouTube и CIPA-совместимого поиска Google (не должно работать в режиме прокси).  Предоставление встроенных в сетевом экране средств создания собственных сигнатур приложений по регулярным выражениям с использованием декодеров HTTP(S), FTP, SMB, SMTP, RPC и др., а также по маске для содержимого TCP/UDP-пакетов;  Распознавание сетевых приложений по зашифрованному SSL (поддержка ключей RSA до 2048 бит) и SSHv2 трафика, проходящего через сетевой экран (дешифрация SSL, SSHv2), – как для входящих, так и для исходящих подключений, прозрачно для пользователей в домене, с возможностью контроля отдельных функций приложений, включая отправку сообщений в социальных сетях, файловый обмен, потоковое аудио, видео;  Последовательное распознавание различных приложений, используемых в рамках одной сессии;  Правила контроля доступа должны поддерживать возможность учитывать время, день, дату и период предоставления такого доступа.  Распознавание пользователей, использующих сетевые приложения, за счет интеграции с корпоративными сервисами аутентификации пользователей, такими как Microsoft Active Directory, Microsoft Exchange, LDAP, Novell eDirectory;  Интеграция с Microsoft Active Directory должна осуществляться без изменений в Active Directory и не должна использовать учетную запись администратора Active Directory домена.  Возможность интеграции с другими сервисами аутентификации (например, контроллерами беспроводных сетей) через открытый XML API;  Возможность создания пользователь-ай-пи меппинга (user-IP mapping) благодаря парсингу syslog сообщений отправленных системой аутентифицировавшей пользователей.  Возможность создания и использования в правилах динамических групп пользователей. Динамические группы пользователей позволяют на лету удалять пользователя из группы (добавлять пользователя в группу) без необходимости изменений в соответствующей директории (например Active Directory) и без необходимости устанавливать политики. Это позволяет уполномоченным администраторам или внешним системам удалять пользователя из динамической группы пользователей, например в случае компрометации соответствующего пользователя.  Создание правил в единой политике безопасности, используя в качестве классификаторов данные об IP-адресе отправителя, получателя, используемых сервисов (TCP/UDP-портов), имена пользователей, групп пользователей и используемых пользователем или группой пользователей приложений или определенных категорий приложений.  В создаваемых политиках должна быть возможность реализации следующих действий:  Разрешения или запрещения;  Разрешение конкретного приложения или категории приложений использовать только стандартные или строго определенные TCP/UDP-порты. При этом эти порты не должны быть использованы другими приложениями без политики, разрешающей такие взаимодействия в явном виде;  Разрешения или запреты, основанного на расписании, пользователе или группе пользователей;  Применить маркировку DSCP и ограничения по трафику, используя политики QOS на основе приложений, IP-адресов, DSCP, пользователей и групп пользователей;  Реализация QOS для трафика real-time, идентифицированного на уровне приложений;  Возможность применять перенаправление трафика на основе политик (Policy Based Forwarding) на основе IP адреса (source и/или destination), пользователя, приложения или URL;  Возможность запрета отдельного функционала в приложениях;  Возможность использовать любую комбинацию из вышеприведенных действий;  Возможность построения whitelist/blacklist политики для отдельно взятых пользователей.  Инспекция по содержанию трафика протоколов:  Generic Routing Encapsulation;  Non-encrypted IPsec traffic (NULL Encryption Algorithm for IPsec and transport mode AH IPsec).  Устройство должно обеспечивать функционал оптимизации политик, в частности на основе использования приложений; выявление и удаление неиспользованных правил политики:  Для создания более строгих правил и оптимизации политики в интерфейсе управления на устройстве должны быть доступны следующие функции:  Сообщать о правилах с неопределенными приложениями, идентифицировать приложения, проходящие через эти правила, и активировать их в правиле, выбрав нужные из перечисленных приложений.  Система может сообщать о приложениях, определенных и не используемых в правилах за последние 7, 15, 30 дней.  Система имеет возможность сообщать информацию о первой и последней дате идентификации приложения, которое идентифицировались в правиле, и сколько пропускной способности он потребил за последние 30 дней.  Система идентифицирует правила, которые не использовались за последние 30 дней и 90 дней.  Правила безопасности могут применяться в соответствии с географическими регионами; к правилу можно добавить несколько географических регионов.  Ограничение пропускной способности может применяться на основе имени пользователя/группы, IP-адреса цели/источника и программы.  Возможность автоматически блокировать трафик из определенных источников отдельной частью сетевого экрана, прежде чем эти пакеты будут использовать ресурсы основного процессора или буфера пакетов виртуального NGFW.  Наличие сервиса сканирования новых потенциально вредоносных файлов в среде Microsoft Windows, включая выполняемые файлы (в том числе EXE, DLL, SCR, BAT, и др.), передаваемые по сети, в почтовых сообщениях SMTP/POP3, включая шифрованные сообщения с помощью SSL, обеспечивающее поведение подозрительных файлов и ссылок в частном или внешнем облаке («песочнице»), выявление нового вредоносного ПО и автоматическую генерацию антивирусной сигнатуры в течение 24 часов минут и обновление репутационной базы URL в течение 30 мин.  Развиты функции визуализации: визуализация в простом и удобном формате, активности сетевых приложений, обнаруженных и блокированных сетевых угроз приложений, которые используют пользователи. Возможность фильтрации информации, используя различные фильтры (по приложениям, по угрозам, по пользователям, IP-адресам, TCP/UDP-портам, зонам безопасности, типам угроз и др.).  Иметь возможность создания отчетов. Сетевой экран должен иметь функции по автоматической генерации отчетов и отчетов по расписанию по различным тематическим функциям по ручной настройке создаваемых отчетов. Должна быть возможность просмотра отчетов как непосредственно через графический веб-интерфейс управления (GUI) сетевым экраном, так и возможность экспорта отчетов в форматы PDF и CSV.  Иметь возможность интеграции с подсистемой централизованного управления, логирования, отчетности, обновления программного обеспечения сетевых экранов того же производителя.  Иметь возможность буферизации логов локально на выделенное дисковое пространство виртуальной машины в случае кратковременной недоступности подсистемы централизованного логирования.  Иметь ролевое управление доступом локальных администраторов:  возможность ограничить область просмотра и управления на уровне виртуального устройства в целом, а также отдельных виртуальных систем (контекстов);  Возможность предоставления доступа в режиме редактирования, либо только для чтения, либо запрета доступа к любому разделу веб-интерфейса сетевого экрана;  Возможность предоставить доступ в режиме редактирования, либо только для чтения, либо запретить доступ к CLI сетевому экрану.  Управление политиками безопасности и сетевыми настройками должно производиться по протоколам HTTPS и SSH без необходимости установки какого-либо дополнительного ПО управления на рабочую станцию администратора.  Интерфейс управления сетевыми экранами (веб и CLI) должен быть унифицирован с подсистемой централизованного управления, логирования, отчетности, обновления программного обеспечения; [Система должна предусматривать возможность добавления централизованного сервера управления в будущем].  Поддержка функционала динамических групп адресов (Dynamic Address Group) и динамических групп пользователей (Dynamic User Group), что позволяет динамически с помощью XML API обновлять такие группы в правилах безопасности без необходимости устанавливать политики безопасности.  Поддержка принудительной многофакторной аутентификации для внутренних приложений.  **Требования к возможностям предотвращения вторжений, распознавания и блокировки вредоносного или запрещенного трафика в системе ПАК:**  Устройства должны иметь архитектурную проверку, фильтрацию пакетов IP и функции распознавания приложений и иметь такие службы безопасности: Брандмауэр следующего поколения (NGFW), IPSEC VPN, SSL VPN, Контроль приложений (Application Control), Антивирус (Antivirus/Antimalware), Предотвращение вторжений (IPS), Анти-шпион (antispyware/antibot), Блокировка атак с использованием DNS протокола (DNS Security), Фильтрация URL ссылок (URL filtering), Интеграция с каталогами для идентификации пользователей (Identity Awareness).  Возможность инспекции передаваемого через сетевой экран содержимого трафика в реальном режиме времени в потоке по сигнатурам и поведению, защита от уязвимостей, сетевых атак и вредоносного программного обеспечения, распознавание типов файлов по их сигнатурам, определение вирусов, передаваемых по веб, по электронной почте, FTP SMB, шпионского программного обеспечения, сетевых «worms», блокирование передачи определенного содержимого с использованием регулярных выражений, в том числе для приложений, использующих шифрование SSL и SSHv2.  Антивирусная защита, защита от шпионского программного обеспечения, защита от уязвимостей и сетевых атак (система обнаружения и предотвращения вторжений), URL-фильтрация с использованием динамической репутационной базы, поддерживающая категоризацию для различных разделов того же веб-сайта, включая поддержку категорий для веб-сайтов на разных языках, блокировка передачи файлов по типам, определенных сигнатур.  Возможность интеграции с системами автоматической корреляции событий информационной безопасности на сетевом экране с помощью обновляемых корреляционных объектов, которые задействуют информацию, полученную от антивирусной защиты, защиты от шпионского программного обеспечения, защиты от уязвимостей и сетевых атак, защиты от угроз и вирусов 0-го дня.  Автоматическая корреляция логов разного типа (сетевое экранирование, защита от угроз, контроль передачи файлов, URL-фильтрация), сгенерированных в рамках одной сессии.  Устройство должно иметь следующие функции системы противодействия вторжениям (IPS):  Возможность создания разных политик IPS для разных пользователей или групп пользователей.  Возможность поиска IPS сигнатур на устройстве с помощью CVE, уровней критичности и типа хоста (клиент/сервер).  Возможность индивидуальной настройки сигнатур IPS системы реагировать на атаки следующим образом: Allow, Alert, Deny, reset-both, reset-client, reset-server, Block-IP. Блокировка на основе IP должна выполняться на основе source IP и одновременно source и destination IP.  Фильтры IPS, используемые для противодействия атакам, должны быть в состоянии обновляться из файла обновления или через Интернет. Кроме того, при необходимости обновление сигнатур должно производиться автоматически без вмешательства пользователя.  Предлагаемая функциональность IPS должна включать технологию детектирования аномалий в используемых аномалиях (Protocol Anomaly Detection), позволяющих блокировать атаки, не опираясь на имеющиеся сигнатуры.  Функциональность IPS должна быть в состоянии противостоять следующим атакам:  (Brute Force, Code/Command execution, Sql-injection, Exploit-kit, Denial of Service, Info-leak, Overflow, Scan и др.)  Устройство должно иметь функциональность Anti-Spyware/Anti-bot для обнаружения и блокировки со следующими возможностями:  Эта функциональность должна работать вне зависимости от порта и протокола и должен проверять весь IP трафик в Интернет;  Выявлять запросы на определение (resolution requests) IP адресов командных центров ботнетов (Botnet command and control centers) и блокировать их через ДНС запросы;  Функциональность DNS Sinkhole в случае запроса вредоносного доменного имени должна выдавать IP address назначенный администратором. Таким образом, инфицированные системы могут быть легко идентифицированы;  Функциональность блокировки известных ботнетов с помощью сигнатур. Система должна предоставлять возможность администратору настраивать ботнет сигнатуры;  Следующие действия для действий сигнатур должны быть доступны: Allow, Alert, Deny, reset-both, reset-client, reset-server, Block-ip;  Различные политики Anti-spyware должны создаваться для разных пользователей и групп пользователей;  Функциональность Anti-spyware должна включать идентификацию и блокировку следующих атак: adware, Botnets, Backdoor, Browser-Hijacker, Data-theft, keylogger, spyware, net-worm, p2p-communication.  Устройство должно иметь Anti-Virus функциональность для обнаружения и предупреждения со следующими возможностями:  Блокировка известного вредоносного ПО на основе сигнатур;  Должен иметь возможность потокового сканирования. Должен сканировать архивные файлы;  Архитектура Anti-virus должна иметь возможность интегрироваться с Active Directory таким образом, чтобы правила Anti-virus могли быть определены на основе пользователя или группы пользователей в Active Directory;  Возможность исключить антивирусные сигнатуры из базы данных сигнатур (возможность задавать исключения);  Различные политики Anti-virus должны создаваться для разных пользователей и групп пользователей;  Anti-virus должен блокировать вредоносные файлы, передаваемые через протоколы FTP, HTTP, SMB, POP3, IMAP, SMTP.  Устройство должно иметь функционал URL-фильтрации.  Устройство должно иметь функционал защиты от фишинговых атак посредством функции контроля идентичности пользователя. Предложенное решение должно иметь возможность предотвратить отправку/похищение информации о пользователе (логине) и пароле на уровне HTTP/HTTPS POST. Он должен иметь возможность контролировать учетные данные пользователей в интеграции с Active Directory. Соответствующая лицензия должна быть включена в предложенное решение.  Устройства должны иметь возможность расшифровки SSL/TLS и SSH. Поддержка расшифровки протоколов TLS 1.0, TLS 1.1, TLS 1.2 и TLS 1.3.  Устройство должно иметь возможность проверять трафик HTTPS и применять IPS, контроль приложений, фильтрацию URL и антивирусные средства защиты.  Устройство должно осуществлять расшифровку HTTPS во входном (inbound) и исходящем (outbound) направлениях.  Устройство должно поддерживать интеграцию с HSM (Hardware Security Module) для управления цифровыми ключами.  Поддержка инспекции тоннелей VxLAN  Правила инспекции (дешифрования) трафика HTTPS должны создаваться на основе имени пользователя/группы пользователей, источника IP (source IP)/сети/зоны, целевого IP (destination IP)/целевой сети/целевой зоны и категории URL.  Устройство должно предоставлять возможность создавать правила исключения дешифрования в случаях, когда содержимое трафика HTTPS не следует видеть (банковские операции и т.п.).  Должна быть возможность проверять сертификат HTTPS сессий и предотвращать сессию с законченными, ненадежными или отозванными сертификатами.  Устройство должно уметь дешифровать SSL веб-трафик и отправлять копию дешифрованного трафика на внешние устройства аналитики, используя функционал зеркалирования трафика. Соответствующая лицензия должна быть добавлена в предложение.  Система должна иметь возможность применять правила безопасности в соответствии с географической зоной, с возможностью создания одного правила с несколькими географическими зонами.  Предлагаемый NGFW должен предлагать удаленный пользовательский VPN-агент для Windows, Mac OS, Linux, IOS и Android с возможностями:  Поддержка MFA;  Поддержка применения политик безопасности на основе устройств;  Поддержка интеграции со сторонними решениями MDM, такими как AirWatch или MobileIron;  Поддержка раздельного туннелирования на основе IP-адресов, доменов и приложений;  Поддержка переопределения аутентификации VPN с использованием файлов cookie;  Поддержка исключение видео-трафика из основного VPN-туннеля удаленного пользователя;  Поддержка отправки доверенных корневых сертификатов на удаленные пользовательские устройства VPN, чтобы помочь включить такие функции, как загрузка SSL;  Поддержка выбора шлюза VPN на основе исходного идентификатора пользователя, региона, ОС и IP-адреса.  **Дополнительные обязательные требования к NGFW:**  Устройство должно поддерживать создание внешних динамических списков блокировки IP/URL/домена. Устройство должно получать доступ к этому списку по протоколу HTTP. При внесении изменений в этот список устройство должно автоматически заблокировать (или разрешить – в зависимости от установленной политики) эти IP/URL/домена без необходимости устанавливать (применить) политики на самом устройстве. Емкость списков должна включать в себя не менее 150 000 IP и URL и не менее 4 000 000 доменных имен.  Список вредоносных IP-адресов, обнаруженных производителем в службе кибер-разведки, должен постоянно обновляться на устройстве. Таким образом, доступ к этим IP может быть заблокирован.  Система должна иметь опцию настройки порогового количества одновременных сессий для противостояния SYN Flood, UDP Flood, ICMP Flood.  Система должна уметь идентифицировать и блокировать сканирования портов: TCP port scan, UDP Ports scan и sweep scan.  Резервные правила должны возобновляться и активироваться без необходимости перезагрузки.  Все сервисы, используемые NGFW, имеют возможность получать обновления ПО и сигнатур безопасности (а именно - Application Control, Data Filtering, IPS, Antivirus, Antispyware, SSL Decryption), со дня активации лицензии NGFW минимум до 31.12.2025 года.  Предлагаемый NGFW должен поддерживать беспрепятственный открытый API без платного доступа (подписки) для доступа к инструментам разработки, инструментам, сценариям и образцам.  **Требования к сервисной поддержке NGFW:**  Сервисная поддержка программного обеспечения, с возможностью:  Локального обращения к первой линии поддержки от производителя NGFW в Казахстане с сертифицированными инженерами;  Обращение по телефону или через Интернет (чат и электронная почта);  Доступ к загрузке обновлений, исправлений;  Доступ к документации.  **Требования к разворачиванию системы миграционным услугам**  Техническая команда подрядчика должна оказать содействие в первоначальном разворачивании системы и миграционным услугам, включая:  Обсуждение и планирование ИТ-архитектуры, регистрацию устройств, активацию всех лицензий, установку предпочитаемой версии операционной системы и крайней версии динамических обновлений, конфигурацию функционала отказоустойчивости (High Availability) устройств.  Перенос действующей конфигурации «как есть» с действующего оборудования на новое, включая: Зоны безопасности; Конфигурацию интерфейсов; Маршрутизацию; Политики NAT; Политики безопасности; Профили безопасности; Объекты адресов (Address Objects) и групп адресов (address groups); Конфигурацию защиты зоны (Zone Protection); Интеграции с сервисами аутентфикации; Конфигурацию идентификации пользователей; Конфигурацию администраторов и ролей администрирования; Конфигурацию VPN;  Техническая команда должна обладать наивысшей возможной степенью сертификации  **Система управления для программно-аппаратных комплексов (ПАК) для защиты сети.**  Требования к системе централизованного управления, логированию, отчетности и обновлению программного обеспечения (далее - Системы централизованного управления) программно-аппаратных сетевых экранов:  - Поддержка всех моделей и версий ПО сетевых экранов того же производителя, что и программно-аппаратных сетевых экранов;  - Унификация веб-интерфейса с NGFW того же производителя – аналогичные управления, разделы, закладки и графическое оформление;  - Унификация CLI с NGFW того же производителя – аналогичные команды;  - Возможность веб-интерфейса Системы централизованного управления переключаться в веб-интерфейс управления конкретным NGFW и обратно;  - Лицензия для системы централизованного управления должна позволять управлять до 25 устройствами NGFW  **Требования к функциям централизованного управления:**  - Возможность объединения управляемых NGFW в группы – как физических устройств, так и отдельных виртуальных систем (контекстов);  - возможность применения единых настроек информационной безопасности и тиражирования настроек сетевых и системных параметров с последующей корректировкой для учета локальных особенностей;  - Возможность применения к группам устройств централизованных настроек объектов: Адресных объектов (IP-адреса, FQDN) и групп; созданных встроенными средствами NGFW сигнатур приложений и угроз; статических и динамических групп приложений; созданных категорий URL; профилей настройки динамической URL-фильтрации, системы обнаружения и предотвращения вторжений (IDS/IPS), антивирусной защиты, защиты от шпионского ПО (в том числе ботнетов) и DoS-атак; профилей отправки логов; расписание действия политик.  - Возможность применения к группам устройств централизованных настроек политик: Информационной безопасности (межсетевого экранирования и защиты от угроз); Дешифрование SSL и SSHv2; QoS; Переопределение приложений; Защиты от DoS-атак.  - Возможность выборочного применения политик к отдельным устройствам в группе, а также ко всем, кроме отдельных.  - Возможность комбинирования централизованно настроенных и локальных политиков на устройстве. При этом централизованно настроенные политики и объекты должны быть доступны локальному администратору в режиме "только для чтения".  - Возможность применения к группам устройств шаблонов конфигурации всех сетевых и системных параметров, в том числе: Создание виртуальных систем (контекстов) – при условии поддержки со стороны NGFW; Настройка ролей администраторов, идентификации и аутентификации пользователей; Настройка зон безопасности, параметров сетевых интерфейсов (тип, IP-адресация), маршрутизации, VLAN, IPsec/SSL VPN, QoS; Настройка защиты зон МЭ от атак L3-L4, включая flood, сканирование сети и модификацию заголовков TCP/UDP.  - Предоставление возможности локального администратора выборочно скорректировать сетевые и системные параметры после централизованного применения шаблонов.  - Прием и хранение логов в формате NGFW того же производителя.  - Поддержка двухуровневой системы логирования и отчетности: Роль сервера логирования – хранение логов от подключенных МЭ; Роль сервера управления – централизованное конфигурирование и генерация отчетов на основе данных, сохраненных распределением на серверах логирования, агрегирование отчетности; Возможность совмещения ролей сервера управления и логирования на одном устройстве.  - Визуализация трафика и угроз, идентична отдельному NGFW, но на основе агрегированных логов и статистики.  - Возможность построения всех типов отчетов, идентично отдельному NGFW, но на основе агрегированных логов и статистики.  - Возможность централизованного обновления ПО для каждой модели управляемых NGFW.  - Возможность централизованного обновления сигнатур приложений и угроз.  - Возможность централизованного контроля наличия и актуальности лицензий, подписок и контрактов технической поддержки производителя.  - Ролевое управление доступом администраторов: Возможность ограничить область просмотра и управления на уровне групп управляемых МЭ, а также отдельных устройств; Возможность предоставить доступ в режиме редактирования либо только для чтения, либо запретить доступ к любому разделу веб-интерфейса ПО управления, логирования, отчетности и обновления; Возможность предоставить доступ в режиме редактирования либо только для чтения, либо запретить доступ к CLI.  - Возможность интеграции с контроллером Cisco ACI, позволяющим вставлять межсетевой экран NGFW между EPG как услугу уровня 4 до уровня 7, что позволяет инспектировать трафик восток-запад (East-West) между уровнями программ в этих EPG и трафик север-юг (North-South) между пользователями и программами.  - Возможность конвертации Snort и Suricata сигнатур для IPS-подсистем управляемых NGFW.  **Требования к сервисной поддержке системы управления:**  Сервисная поддержка программного обеспечения не менее 12 месяцев, с возможностью: Локального обращения к первой линии поддержки от производителя системы управления в Казахстане с сертифицированными инженерами; Обращение по телефону или через Интернет (чат и электронная почта); Доступ к загрузке обновлений, исправлений, к документации.  **Требования к разворачиванию системы**  Техническая команда подрядчика должна оказать содействие в первоначальном разворачивании системы, включая: Разворачивание образа системы управления на выбранной системе виртуализации (предоставляется заказчиком), Регистрацию устройства; Активацию всех лицензий; Установку предпочитаемой версии операционной системы и крайней версии динамических обновлений; Добавление всех необходимых NGFW в систему управления; Создание администраторов и ролей администрирования;  Техническая команда должна обладать наивысшей возможной степенью сертификации  **Требования к обучению по компонентам системы защиты сетевого периметра и контроля доступа между сетевыми сегментами**  Возможность проведения обучения оффлайн на стороне заказчика.  **Двухфакторная аутентификация к системе защиты сетевого периметра и контроля доступа между сетевыми сегментами**  **Требование к двухфакторной аутентификации**  Предоставление двухфакторной аутентификации без необходимости подключения к сети Интернет.  Возможность получения одноразового пароля с помощью мобильного приложения, push-уведомления, SMS-сообщения или токена.  Возможность указать собственные пути доставки одноразовых паролей.  Уникальный алгоритм генерации паролей для каждого пользователя.  Интеграция с Active Directory.  Возможность использования в инфраструктуре без домена.  Поддержка LDAP и MAC Open Directory.  Возможность добавления 2FA для безопасного доступа входа как локальной учетной записи, так и доменной учетной записи системы под управлением: Miscrosoft Windows, Linux или MAC OS X.  Наличие Identity Provider Connector для обеспечения 2FA облачных служб (поставщиком услуг) и поставщиком идентификационных данных, таких как: OpenAM, Okta, Azure AD, AD FS, Shibboleth, Keycloak, Dropbox, Confluence.  Возможность использования резервного пароля (Master Recovery Key).  Поддержка аппаратных токенов, работающих по стандартам OATH, HOTP, TOTP, FIDO, FIDO2.  Защита VPN и VDI систем, таких как: Microsoft Forefront Threat Management Gateway, Barracuda, F5 FirePass, Cisco ASA IPSEC, Cisco ASA SSL, Fortinet FortiGate, Citrix Access Gateway, Juniper, Citrix NetScaler, Palo Alto, Check Point Software, SonicWall, Netasq, VMware Horizon View и Citrix XenApp, Cyberoam.  Возможность использования двухфакторной аутентификации для защиты VPN подключений, Remote Desktop Protocol, авторизация в ОС, Web сервисов которые используют Microsoft ADFS 3 или 4, Microsoft Web Apps, Microsoft Exchange Server, Microsoft Share Point Server, Remote Desktop Web Access, Microsoft Dynamics CRM, VMware Horizon View, сервисы на основании RADIUS.  Защита через SSO и Microsoft Active Directory Federation Services для входа в Office 365 или Azure.  Использование двухфакторной аутентификации в безопасном режиме Windows и в режиме блокировки ПК.  Защита UAC доступа двухфакторной аутентификацией.  RADIUS PAM для ОС Linux/Mac, (Защита SSH, cli login, GUI login). (При условии членства в AD).  Возможность создавать белые списки IP адресов, доступ с которых не потребует двухфакторной аутентификации; наличие пакетов API и SDK позволяющих использовать двухфакторную аутентификацию с любым пользовательским приложением  Возможность использования отказоустойчивой конфигурации из нескольких серверов в режиме Active/Pasive.  Информирование пользователя о попытке авторизации с возможностью подтвердить или отклонить проверку подлинности.  Наличие системы отчетности, которая может использоваться как для панели мониторинга, так и для формирования отчетов.  Наличие журнала аудита, в котором регистрируются и отслеживаются все изменения в конфигурации, запуске и остановке службы двухфакторной аутентификации.  Возможность интеграции с SIEM и другими системами мониторинга, анализа и реагирования.  Возможность администратора предоставлять альтернативный одноразовый пароль OTP в случае, если у пользователя нет доступа к токену или мобильному приложению.  Возможность импортировать пользователей в специальные области с помощью CSV или LDF.  Возможность ограничить количество использования одноразовых паролей для компьютеров, не имеющих подключения к серверу 2FA.  Наличие защиты от подбора одноразового пароля путём блокировки пользователя.  Наличие системы уведомлений о выбранных типах действий.   * + 1. **Система контроля конечных рабочих станций (антивирусная защита)**   Система контроля конечных рабочих станций должна обеспечивать следующий функционал:  **Сервер управления**  - Возможность централизованного управления антивирусной защитой всей сетевой инфраструктуры.  - Возможность построения иерархической структуры администрирования, которая состоит из главного сервера и подчиненных серверов, что дает возможность осуществлять централизованное управление антивирусной защитой рабочих станций, серверов и мобильных устройств, что принадлежат как главному, так и региональным подразделениям.  - Возможность удаленно активировать и деактивировать модули защиты, такие как персональный брандмауэр, защита в режиме реального времени, защита почтового клиента, защита доступа в Интернет, контроль устройств, веб-контроль, антиспам на отдельно взятом клиенте.  - Возможность выполнять с помощью инструмента удаленного управления дополнительные сетевые действия, такие как: завершение работы и перезагрузка, отправка сигнала пробуждения компьютера, отправка сообщений, выполнение конкретных инструкций командной строки на клиентском компьютере, старт обновления операционной системы клиентского компьютера.  - Использование независимого агента, который позволяет осуществлять удаленное управление антивирусным продуктом на конечных точках, а также контролировать уровень антивирусной защиты на рабочих станциях и состояние операционной системы.  - Поддержка инструментом удаленного администрирования следующих баз данных: MS SQL Server, MySQL.  - Возможность создания зеркала обновлений на основе сторонних HTTP-серверов.  - Возможность настраивать параметры журналов и отчетов или выбрать из более чем 50 шаблонов для различных систем/клиентов.  - Возможность отслеживать установленное на рабочей станции ПО, а также удалять установленное ПО на выбор.  - Возможность деактивировать лицензию антивирусных продуктов даже на рабочих станциях, к которым нет физического или удаленного доступа.  - Наличие функционала для определения администратора площадки или филиала с соответствующей частью лицензии.  - Наличие предустановленных шаблонов в системе уведомлений для информирования о некорректной идентификации клонированных машин, что дает возможность оповещать о некорректно настроенной интеграции с системами VDI.  - Возможность определять, какая виртуальная машина будет являться источником для копирования или клонирования в системах VDI.  - Наличие функционала создания площадок в соответствии с филиалами компании, что дает возможность назначить определенную часть лицензии отдельным филиалам.  - Возможность удаленного полнодискового шифрования/расшифровки всех дисков на клиентских машинах.  - Возможность удаленного полнодискового шифрования/расшифровки только загрузочного диска на клиентских машинах.  - Наличие в консоли сервера управления мастера включения шифрования, что позволяет администратору очень удобно и быстро выбрать для удаленной рабочей станции соответствующую политику с необходимыми параметрами и запустить на ней процесс шифрования дисков.  - Возможность для пользователей каждой рабочей станции создавать свой собственный пароль предзагрузочного входа.  - Возможность администратора устанавливать для предзагрузочного пароля различные критерии, такие как: сложность пароля, количество попыток ввода, срок действия.  - Возможность администратора удаленно блокировать предзагрузочный пароль, что приведет к отключению предзагрузочного входа после последующей перезагрузки, а для разблокировки необходимо будет установить новый предзагрузочный пароль с помощью пароля восстановления.  - Возможность администратора удаленно стереть предзагрузочный пароль, что приведет к немедленной блокировке удаленной рабочей станции, а пользователю будет отображено на экране сообщение о критической ошибке типа «синий экран». После этого доступ к информации на дисках можно получить только после расшифровки с помощью загрузочного диска восстановления.  **Защита рабочих станций**  - Предоставление защиты от вредоносного ПО – определенного вредоносного кода, который добавляется в начало или конец кода файлов на компьютере. Выявление вредоносного ПО должно осуществляться ядром обнаружения в сочетании с компонентом машинного обучения.  - Предоставление защиты от потенциально нежелательных программ, которые нельзя однозначно отнести к вредоносному ПО по аналогии с такими безусловно вредоносными программами, как вирусы или трояны, но эти программы могут устанавливать дополнительное нежелательное ПО, менять настройки системы, а также выполнять неожиданные действия или действия, не подтвержденные пользователем.  - Предоставление защиты от опасных программ руткитов, которые предоставляют злоумышленникам из Интернета неограниченный доступ к системе, в то же время скрывая свое присутствие в операционной системе.  - Возможность делать исключения из сканирования определенных файлов, которые не вредоносные, но сканирование которых может привести к отклонениям в работе или влиять на продуктивность системы.  - Обеспечение антивирусной защиты в режиме реального времени.  - Антивирусное сканирование по требованию пользователя или администратора и в соответствии с графиком.  - Возможность использования технологий машинного обучения для более углубленного анализа кода с целью выявления вредоносного поведения и характеристик вредоносного программного обеспечения.  - Возможность создавать группы разрешенных или запрещенных внешних устройств.  - Наличие встроенного инструмента, что объединяет несколько утилит для очистки остатков сложных устойчивых угроз, таких как Conficker, Sirefef, Necurs и других  - Наличие дополнительного модуля, который позволяет запускать браузеры в защищенном режиме с целью блокирования попыток вмешательства в область памяти браузера и содержимого его окон, а также дополнительной защиты критических Интернет-соединений, таких как Интернет-платежи и Интернет-банкинг и т.д.  - Возможность создавать и удаленно выполнять скрипты, что позволит на удаленном ПК останавливать запущенные процессы и службы, удалять ветки реестра, блокировать сетевые соединения.  - Возможность запрещать или разрешать подключение внешних устройств как для всех, так и для отдельных пользователей или групп Windows или домена.  - Наличие дополнительного функционала персонального брандмауэра, что позволяет просматривать всю подробную информацию по всем имеющимся сетевым соединениям, а также предупреждать пользователя о подключении к незащищенной сети Wi-Fi.  - Наличие дополнительного функционала персонального брандмауэра, что дает возможность просматривать на ПК перечень заблокированных IP-адресов, предоставляет информацию о причинах попадания в черный список и позволяет сделать исключения для конкретных безопасных адресов.  - Наличие в персональном брандмауэре режима обучения, что позволяет администратору удаленно настраивать разрешительные правила для сетевых приложений и оборудования.  - Возможность использовать в персональном брандмауэре дополнительную аутентификацию сети с целью предотвращения несанкционированного подключения ПК к неизвестным опасным сетям.  - Наличие дополнительного функционала персонального брандмауэра, который способен обнаруживать те изменения в сетевых программах, которые повлекли за собой новые несанкционированные сетевые соединения.  - Получение обновления клиентов из локального хранилища на сервере, что позволяет поддерживать актуальность антивирусной защиты в закрытых изолированных сетях, у которых нет доступа к сети Интернет.  - Возможность обновления в режиме получения регулярных, тестовых и отложенных обновлений.  - Наличие режима переопределения политики, что дает системному администратору временную возможность изменять на ПК те настройки антивирусного ПО, которые назначаются политикой и недостижимые для редактирования, с целью гибкой настройки антивирусного ПО в специфической среде.  - Низкое потребление ресурсов ПК актуальными антивирусными продуктами (совместно с всеми процессами: графический интерфейс, процесс комплексной защиты, служба удаленного администрирования): 50-100 МБ оперативной памяти, 2-35 % центрального процессора.  - Сканирование компьютера в неактивном состоянии.  - Использование 64-битного ядра для сканирования, что уменьшает нагрузку на систему и позволяет сделать самые быстрые и эффективные сканирования.  - Модуль сканирования оперативной памяти, который способный отслеживать работу подозрительных запущенных процессов, что позволяет предотвратить заражение даже тщательно зашифрованными и скрытыми угрозами.  - Возможность определения уровня критичности (опасный, неизвестный, малоизвестный, безопасный) значений различных параметров операционной системы с целью выявления несанкционированных и опасных изменений в операционной системе.  - Поддержка ОС: Microsoft Windows Vista (Professional или выше); Microsoft Windows 7 (Professional или выше); Microsoft Windows 8 (Professional или выше); Microsoft Windows 8.1 (Professional или выше); Microsoft Windows 10 и Microsoft Windows 11.  - Обеспечение управления полным шифрованием диска на управляемых рабочих станциях Windows с дополнительным уровнем защиты на этапе предзагрузочного входа.  - Возможность использовать для шифрования дополнительные технологии от производителей оборудования: такие как доверенный платформенный модуль (TPM) или самошифрованные диски (OPAL).  - Различные режимы для графического пользовательского интерфейса: обычный, где будет доступен весь функционал графического интерфейса или минимальный, когда будут отображаться только уведомления.  - Поддержка работы программ, работающих в полноэкранном режиме, с возможностью скрыть все сообщения, связанные с шифрованием.  - Возможность пользователя изменить свой предзагрузочный пароль с помощью текущего пароля  - Возможность администратора создавать пароль восстановления в случае, если пользователь забыл свой собственный пароль.  - Возможность администратора создавать загрузочный диск или USB-накопитель для аварийной расшифровки диска в случае, если к данным на зашифрованном диске нельзя будет получить доступ с помощью стандартных средств.  - Возможность администратора удаленно аннулировать предзагрузочный пароль, что приведет к отображению пользователю запроса на изменение пароля и заставит его изменить пароль при последующей перезагрузке ОС.  **Защита серверов**  - Автоматическое определение ролей сервера для создания автоматических исключений для специфических файлов, папок, приложений, позволяющее минимизировать влияние на работу серверной операционной системы.  - Возможность интеграции защиты рабочих станций и серверов с облачной песочницей (при наличии дополнительной лицензии) без необходимости установки дополнительных программных продуктов.  - Сканирование интерфейса UEFI – проверка на наличие вредоносного программного обеспечения в главной загрузочной записи.  - Использование эвристических технологий во время сканирования.  - Предоставление защиты от вредоносных программ, троянского ПО, клавиатурных шпионов, рекламного ПО, фишинга, шпионского ПО, руткитов, скриптов, потенциального нежелательного и опасного ПО.  - Регламентное обновление вирусных баз не менее 24 раз в сутки.  - Возможность помимо основного указать резервные серверы администрирования.  - Наличие инструмента, который сможет осуществлять контроль подключения к рабочей станции периферийных устройств путем создания правил доступа по типу устройства, по уровню доступа, по производителю, модели или серийному номеру устройства. Правила могут быть созданы как для всех, так и для отдельных пользователей или групп Windows.  - Наличие инструмента для диагностики системы, который может создавать снимки состояния операционной системы для дальнейшего глубоко анализа различных аспектов работы операционной системы, включая запущенные процессы, контент реестра, установленное ПО, сетевые соединения. Благодаря умению сравнивать различные снимки состояния системы, этот инструмент может обнаружить изменения, которые произошли в системе. Также он может создавать и выполнять скрипты, что позволит останавливать запущенные процессы, удалять ветки реестра, блокировать сетевые соединения.  - Возможность блокировать загрузку из Интернета файлов по указанному расширению.  - Возможность обновления в режиме получения регулярных, тестовых и отложенных обновлений.  - Наличие специальной технологии, значительно снижающей нагрузку на виртуальные рабочие станции, а также на гипервизор в целом.  - Возможность настройки режима запуска путем отключения графического интерфейса для терминальных пользователей, что позволяет уменьшить нагрузку на сервер, работающий в режиме сервера терминалов.  **Расширенное обнаружение и реагирование**  - Наличие панели мониторинга для отслеживания актуальной информации об аномальных событиях, возникших в корпоративной сети.  - Получение предупреждений об аномальных событиях, возникших в работе ПО на основе правил.  - Список правил по умолчанию и возможность создания собственных правил, характеризующих поведение ПО как аномальное.  - Автоматическая классификация предупреждений по уровню критичности позволяет быстро определять и реагировать на критические события.  - Возможность устанавливать приоритет для предупреждений для более гибкой сортировки и фильтрации событий.  - Возможность группировки предупреждений по разным критериям, таким как тип, компьютер, правило, процесс, файл.  - Возможность фиксировать инциденты информационной безопасности путем создания тревожных обнаружений, которые будут содержать как сводную информацию о происшествии (когда и где это произошло (компьютер), от какого пользователя, какой выполняемый файл запускался, даже какой конкретный процесс вызвал запуск), так и подробную информацию по каждому из перечисленных параметров.  - Наличие в каждом тревожном выявлении специального информационного раздела, в котором будет представлено детальное описание события, вызвавшего срабатывание правила, перечень возможных причин, возможные риски и последствия и рекомендации относительно необходимых действий для дальнейшего анализа инцидента.  - Наличие интерактивного интерфейса тревожных обнаружений позволяет углубляться в более детальное рассмотрение инцидента информационной безопасности для основных параметров из имеющихся в сводном тревожном обнаружении.  - Предоставление подробной информации о процессе, вызвавшем срабатывание, такой как дерево процессов, изменения в файловой системе и в реестре ОС, сетевая активность, соединение с URL-адресами, дополнительно загруженные исполняемые файлы, а также самый подробный журнал событий в ОС.  - Автоматическая классификация EXE/DLL файлов по уровню критичности позволяет быстро определять и реагировать на аномальное поведение файлов.  - Автоматическая классификация скриптов по уровню критичности позволяет быстро определять и реагировать на аномальное поведение.  - Возможность создания детализированных исключений для отдельных событий, которые должны включать информацию о контрольных суммах исполняемых файлов, их местонахождении, цифровой подписи и другой информации.  - Возможность помечать EXE/DLL файлы как доверенные или безопасные.  - Возможность помечать EXE/DLL файлы как проверенные или проанализированные.  - Возможность помечать проверенные скрипты как доверенные или безопасные.  - Создание списка всех EXE/DLL файлов на рабочих станциях и серверах с целью дальнейшего анализа.  - Список заблокированных EXE/DLL файлов с возможностью их восстановления, удаления и загрузки для более подробного анализа.  - Возможность загрузки подозрительных файлов из конечных точек для дальнейшего анализа.  - Возможность загрузки подозрительных файлов-сценариев (скриптов) из конечных точек для дальнейшего анализа.  - Создание списка всех сценариев, скриптов, выполняемых на рабочих станциях и серверах.  - Возможность группирования скриптов по разным критериям, таким как родительский процесс, первый дочерний процесс, командная строка.  - Формирование списка компьютеров с подробной информацией о событиях, EXE/DLL файлах, скриптах.  - Возможность удаленной перезагрузки рабочей станции или ее полного отключения.  - Возможность мгновенного создания на удаленной рабочей станции снимка состояния операционной системы, который зафиксирует информацию обо всех текущих запущенных процессах, сетевых соединениях, а также предоставит информацию о критическом контенте реестра ОС, задании в планировщике ОС, пользователях ОС и их привилегиях, содержимом критических файлов ОС, таких как "hosts", "win.ini" и другие, и всю подробную информацию об ОС и установленном ПО.  - Возможность использования двухфакторной аутентификации для учетных записей администраторов, что позволяет предотвратить несанкционированное подключение к серверу централизованного управления.  - Возможность использования EDR-решения при условии, что управление им будет осуществляться существующими серверами администрирования, которые настроены на централизованный мониторинг и управление всеми разветвленными системами антивирусной защиты.   * + 1. **Система защиты от таргетированных атак:**   Система защиты от таргетированных атак должна обеспечивать следующий функционал:   * Агентский контроль активов в количестве не менее указанного в таблице 1; * Поддержка следующих способов интеграции в ИТ-инфраструктуру:   + Интеграция с почтовым сервером для обработки копий сообщений электронной почты, поступающих с почтового сервера по протоколу POP3 (при наличии технической возможности на почтовом сервере);   + Интеграция с рабочими станциями и серверами, для получения и обработки данных о запущенных процессах, открытых сетевых соединениях и изменяемых файлах, в том числе используя совместимый агент антивирусного ПО. * Выявление аномалий и угроз на основе собранной информации; * Возможность предоставить в случае обнаружения критических инцидентов информацию о перечне известных техник и средств, ранее используемых злоумышленниками в подобных ситуациях со ссылками на соответствующие разделы ресурса MITRE ATT&CK, где можно ознакомиться с более подробной информацией о действиях злоумышленников. * Проверка данных на вирусы и другие представляющие угрозу программы с помощью антивирусных баз; * Анализ подозрительных исполняемых файлов и скриптов в «песочнице»; * Статистический анализ и проверка сетевой активности компьютеров на наличие признаков нетипичного поведения в сети; * Репутационный анализ файлов и URL-ссылок; * Поведенческий анализ действий пользователей; * Обнаружение фишинговых и вредоносных ссылок; * Хранение исторических данных об инцидентах; * Возможность создания собственных сигнатур; * Приоритезация выявленных угроз по уровню риска; * Наличие графической системы управления для доступа к статистическим данным и отчетности.   + 1. **Система выявления и предотвращения утечек данных**   **Общие требования**  Приобретаемая услуга по предоставлению программного обеспечения (далее - ПО) предназначено для сбора, хранения, анализа и просмотра информации об активности пользователей.  ПО должна отвечать следующим требованиям:  Подключаться к серверу по защищенному соединению;  Поддерживать работы в любых сетевых инфраструктурах, обеспечивающих подключение от клиента к серверу: через VPN, NAT и другие каналы подключения;  Программа агент должна запускаться на рабочих станциях или терминальных серверах, с операционными системами семейства Windows, Linux и macOS, отслеживать действия пользователя и события на его компьютере, передавать их на сервер;  Вне зависимости от наличия доступа к локальной сети (на удаленной работе компьютера) агент обеспечивает накопление информации о действиях пользователя для дальнейшей передачи на сервер;  ПО должно относиться к корпоративному классу систем (Enterprise DLP) и иметь как функционал защиты конечных точек от утечек конфиденциальных данных с помощью установленного на конечные точки агенту (EndPoint DLP), так и функционал контроля утечки конфиденциальных данных по сетевым каналам (Network DLP).  ПО должно обеспечивать возможность поиска конфиденциальной информации, находящейся на рабочих станциях и файловых серверах (с возможностью перемещения найденных файлов в карантин и оставление на месте таких файлов информации / текстовых файлов / о причинах такого перемещения).  ПО должно контролировать следующие каналы потенциального утечки конфиденциальной информации:  - исходящие SMTP-соединения;  - исходящие HTTP-соединения;  - исходящие HTTPS-соединение;  - исходящие IM-соединения;  - копирование информации на внешние носители информации и информационные ресурсы;  - печать информации на локальном \ сетевом принтере.  ПО должно обеспечивать следующие функциональные возможности:  - предотвращения разглашения конфиденциальной информации через корпоративную почтовую систему;  - возможность блокировки исходящих писем, содержащих конфиденциальную информацию;  - предотвращение разглашения конфиденциальной информации через корпоративную систему доступа в сеть Интернет;  - возможность извлечения конфиденциальной информации с HTTP- / HTTPS-трафика;  - возможность блокировки HTTP- / HTTPS-трафика;  - предотвращения разглашения конфиденциальной информации и мониторинг каналов утечки, а именно: копирование конфиденциальной информации с сетевой папки на локальные жесткие диски, копирование конфиденциальной информации на съемные носители, отправка конфиденциальной информации на локальную и сетевую печать, а также по факсу, защита содержимого буфера обмена при операциях копирования / вставки;  - возможность сканирования (в том числе - по заданному расписанию) локальных жестких дисков конечного узла сети на предмет конфиденциальной информации с возможностью перемещения найденных файлов;  - возможность распознавания текстовой информации, находящейся в графических объектах (pdf-файлы, изображения и т.д.), а также графических образов в таких объектах (подписей ответственных лиц, штампов, логотипов и т.п.);  - возможность сканирования конфиденциальных данных и снятия с них «цифровых отпечатков»;  - возможность автономной работы клиентов и модулей ПО (серверов детектирования), в случае отключения конечного узла от корпоративной сети или потери соединения с сетью;  - возможность централизованного администрирования политик безопасности;  - возможность оперативного внесения изменений в режиме реального времени в политике безопасности ПО, изменения существующих и добавление новых правил, настроек;  - настройка автоматических сообщений о нарушениях политик ПО;  - настройки различных вариантов реагирования на нарушения политики безопасности;  - настройка и генерацию отчетов по датам, фактам нарушения политик безопасности;  - возможность работать с консолью управления на русском или английском языке;  - возможность использовать учетные записи существующей Active Directory для аутентификации в консоли управления;  - возможность просмотра атрибутов учетных записей AD (имя, телефон, департамент, должность и т.д.) непосредственно из консоли ПЗ.  Технические требования  Возможность контроля операций:  - запись конфиденциальной информации (далее - КИ) на съемные носители (USB, CompactFlash, SD);  - встроенный функционал «Device Control», без необходимости развертывания (установки) дополнительных модулей;  - печать КИ (сетевые и локальные принтеры);  - копирование КИ в буфер обмена;  - запись КИ на локальные диски;  - контроль обращения приложений к КИ (в том числе передача файлов, содержащих КИ через Skype, и Teams;  - отправка КИ данных через HTTP протокол;  - отправка КИ данных через HTTPS протокол;  - контроль SMTP на уровне почтовых клиентов;  - копирование КИ файлов на сетевые ресурсы, в том числе ресурсы и сервисы Office 365;  - контроль функции PrintScreen, с возможностью централизованной блокировки на уровне конечных точек;  - возможность настройки и применения политик и конфигураций агенту на конечных точках по месту нахождения - в корпоративной сети, или за пределами корпоративной сети;  - возможность контроля массового копирования документов на внешние носители, система должна контролировать количество файлов которые пользователь может копировать на внешний носитель в течение установленного периода времени;  - возможность шифрования документов при копировании на внешние носители, возможность установки пароля пользователем или администратором ПО;  - возможность блокировки протокола MTP, под контролем подразумевается возможность как детектирования КИ так и блокировки (препятствование передачи) КИ в соответствии с заданными политиками.  Возможность развертывания (установки) всех модулей детектирования системой на ОС Windows и Linux.  Возможность реакции на инциденты: автоматическое оповещение ответственного лица или владельца информации, блокирование отправки по электронной почте, блокировка отправки данных через веб-формы, выполнение скрипта, удаления конфиденциальной информации.  Возможность эскалации инцидента и запуска дополнительных действия (таких как шифрование КИ, перемещения КИ и т.д.).  Сканирование OCR (Optical Character Recognition), должно обеспечиваться встроенной технологией \ механизмом без использования дополнительного программного обеспечения сторонних производителей.  Распознавание текста должно поддерживать латинский и кириллический алфавит с поддержкой английского, русского и казахского языков.  Распознавание и преобразование отсканированных образов должно поддерживать следующие форматы документов: PDF, BMP, JPEG, PNG, TIFF.  Сканирование OCR должно поддерживать такие типы сканирования:  - локальное сканирование;  - сканирование копировании КИ на внешние носители;  - сканирование копировании КИ на файловый сервер;  - сканирование отправок КИ через HTTP / HTTPS;  - сканирование отправок КИ через Webmail протокол;  - сканирование отправок через SMTP протокол.  Возможность регулировать уровень доступа пользователей к USB.  Возможность развертывания модуля конечных точек на системах Ubuntu и Centos с возможностью:  - выявления КИ, которая находится в состоянии покоя;  - контроля утечки КИ на сменные носители в том числе блокировку и логирование такой информации;  - контроля утечки КИ через HTTP / HTTPS каналы;  - контроля утечки КИ через Webmail протокол.  ПО должно поддерживать возможность превентивного информирования администратора, когда пользователь вставляет ненадежный USB накопитель в компьютер.  Агент ПО должен поддерживать работу в «стелс» режиме, все процессы должны быть скрыты от конечного пользователя.  Требования к интерфейсу  ПО должно поддерживать следующие языки интерфейса: английский, русский.  ПО должно поддерживать единый Web-интерфейс управления системой и работы с инцидентами.  Должна присутствовать возможность удаления агентов конечных точек с помощью интерфейса решения.  Должна присутствовать возможность обновления агентов конечных точек с помощью интерфейса решения.  Требования к классификации  ПО должно поддерживать классификацию файлов Microsoft Office.  Классификация должна осуществляться при сохранении файла, а не при его закрытии.  При поиске данных в реальном времени ПО должно поддерживать классификацию текстовых документов и изображений в состоянии покоя.  ПО должно поддерживать возможность ставить водяной знак на документ при классификации данных.  ПО должно поддерживать возможность аудита сетевых хранилищ, должен производиться мониторинг открытия, изменения, удаления, переименования файлов.  ПО должно уметь классифицировать документы во время операций печати.  ПО должно иметь возможность ставить водяной знак на экран пользователя с возможностью выбора позиции, видимости, а также возможностью ставить водяной знак на весь экран.  ПО должно классифицировать файлы и папки в режиме реального времени.  ПО должно контролировать копирование файлов на уровне буфера обмена и иметь возможность блокировать такую операцию в зависимости от уровня классификации файла.  Дополнительные требования  ПО должно поддерживать интеграцию со сторонними почтовыми сервисами с помощью специализированных стандартных протоколов (МТА).  ПО должно поддерживать интеграцию с посторонними веб-сервисами (шлюзами) с помощью специализированных стандартных протоколов (ICAP).  Участник должен иметь возможность обеспечить в рамках технической поддержки (ТП) внедрение и настройку системы у Заказчика в полном объеме с предоставлением консультационной поддержки по эксплуатации и администрирования системы и ее составляющих.  Требования к ТП системы:  - ТП должно обеспечиваться в режиме 24х7;  - ТП должна предоставляться как на английском, так и на русском языках;  - внедрение и настройка системы у Заказчика в полном объеме с предоставлением консультационной поддержки не менее чем трем специалистам Заказчика, по эксплуатации и администрирования системы и ее составляющих;  - проведение технических консультаций персонала Заказчика (не менее 3х человек) по установке и настройке(системы) предотвращения утечки конфиденциальной информации.  Перехват трафика с помощью агента должно осуществляться без установки плагина в браузер пользователя.  Система должна иметь возможность задавать максимальное время сканирования файла для каждой функции в отдельности.  Должна присутствовать возможность создавать свои группы пользователей без привязки к Active Directory.  ПО должно иметь возможность применять полное игнорирование инспекции без инспектирования пакетов для определенных сайтов/ресурсов.  Хранение архива всей перехваченной информации для отслеживания маршрутов движения информации общим объемом не менее последних 6 месяцев для выявления случаев нецелевого использования корпоративных ресурсов, поиска нарушителей и формирования доказательной базы.  Интеграция с системой SIEM.  Техническая поддержка должна быть предоставлена со сроком на 12 месяцев, в период оказания услуг по Договору.   * + 1. **Системы анализа трафика сети и каналов связи**   Функциональные требования:  • Поддержка анализа трафика flow (потоков), отправленных с сетевых устройств инфраструктуры Заказчика на сервер-коллектор. Типы поддерживаемых протоколов перечислены ниже, в разделе «Функциональные требования».  • В случае если сетевое оборудование инфраструктуры Заказчика не имеет функционала генерации и отправки поддерживаемых flow протоколов, будет предусмотрена возможность генерации flow трафика специальным устройством – зондом, путем приема SPAN трафика и инкапсуляции в поддерживаемый системой flow протокол. В рамках поставки должен быть предусмотрен один зонд, встроенный в коллектор.  • Поддержка анализа трафика на нескольких интерфейсах  • Поддержка мониторинга «сырого» SPAN трафика  • Поддержка протокола мониторинга NetFlow v5  • Поддержка протокола мониторинга NetFlow v9  • Поддержка протокола мониторинга jFlow  • Поддержка протокола мониторинга IPFIX  • Поддержка протокола мониторинга sFlow v2/4/5 RFC 3176  • Поддержка протокола мониторинга NetStream  • Поддержка протокола мониторинга cFlowd  • Поддержка протокола мониторинга NetFlow Lite  • Поддержка стандартов Cisco NEL, Cisco NSEL, Cisco AVC, Cisco NBAR2  • Поддержка мониторинга проприетарных полей OneAccess, IXIA, VMware, Gigamon, Cisco Systems по протоколу IPFIX  • Поддержка IPFIX записей переменной длины  • Поддержка IPFIX модификаций сторонних производителей, включая VMware NSX, Gigamon и Ixia IPFIX Extensions  • Возможность анализа и контроля сетевых взаимодействий с поддержкой подхода drill-down (углубление в данные) для получения детальной статистики по каждому сетевому подключению (сетевому потоку);  • Поддержка синхронизации системного времени по протоколу NTP;  • Поддержка DNS кэш;  • Поддержка стандарта Cisco AVC, включая метрики производительности сети (AVC ART) и значения HTTP (имя хоста и URL);  • Поддержка мониторинга сетевой производительности. Сбор и анализ RTT, SRT, delay, jitter, retransmission, out-of-order пакетов;  • Поддержка мониторинга протоколов 7 уровня ISO OSI (HTTP, VoIP SIP, DNS, Samba/CIFS, DHCP, SMTP, POP3, IMAP и MS SQL (TDS));  • Поддержка расширенного мониторинга L3/L4 ISO OSI (TTL (Time To Live), TCP Window Size, TCP SYN размер пакета для NAT обнаружения);  • Поддержка различных уровней семплирования потоков с разных интерфейсов одного источника;  • Поддержка языка написания скриптов (сценариев). Язык написания скриптов будет поддерживать общепринятые команды языка Python;  • Поддержка возможности форвардинга получаемого трафика мониторинга для обработки на других коллекторах, включая возможность семплирования трафика;  • Возможность конвертирования Flow форматов при пересылке трафика (NetFlow v5/v9, IPFIX);  • Возможность обработки трафика данных IPv4 и IPv6, VLAN,MPLS и передача его коллектору;  • Возможность мониторинга трафика в туннелях GRE, VxLAN, ESP,4in6, DS-Lite и OTV (декапсуляция);  • Возможность обнаружения и удаления дублированных пакетов  • Возможность профилирования устройств в сети: идентификация ОС, включая ее версию. Идентификация браузера, включая его версию;  • Возможность установки времени истечения потока: настройки таймаута для активного и неактивного истечения потоков (RFC 3954);  • Поддержка возможности надежной и безопасной передачи IPFIX трафика с использованием TCP/TLS подключений согласно стандарту RFC 7011;  • Поддержка мониторинга зашифрованного (SSL/TLS) трафика: определение версии протокола, алгоритма шифрования, набора шифров, данных сертификата;  • Автоматическая идентификация источника Flow статистики, включая имя источника данных, наименование интерфейса и его параметры;  • Резервное копирование, с возможностью дальнейшего восстановления, Flow данных на внешнее хранилище информации;  • Сбор и отображение данных о пользователях в ЛВС, включая IP адрес хоста и ID пользователя, получаемых из внешних хранилищ данных, как Active Directory и аналогичные;  • Наличие возможностей по фильтрации отображаемых данных на основании информации из полей 7 уровня модели ISO OSI с поддержкой запросов на основании регулярных выражений (AND, OR, NOT);  • Отображение ТОП-Х статистики по заданным опциям и атрибутам: включая количество переданных байт, пакетов, потоков, максимальное RTT и среднее SRT;  • Поддержка оперативных уведомлений пользователей по email, SNMP traps и Syslog;  • Поддержка профилей трафика, определенных под задачи пользователей индивидуально;  • Обнаружение и мониторинг активных устройств в ЛВС, а также хранение истории, включая информацию о MAC адресах, VLAN, OS и идентификационные данные пользователей;  • Поддержка автоматической геолокации, основанной на IP адресах с возможностью фильтрации трафика по странам;  • Открытый интеграционный интерфейс API;  • Мониторинг доступности источников Flow информации по SNMP.  • Поддержка интеграции со сторонними решениями защиты периметра, в частности FortiNet, Checkpoint;  • Объем лицензированного хранилища данных 3 (три) Тб. Объем обрабатываемых системой сбора и хранения данных (коллектором) - 75 тысяч потоков в секунду;  • Поддержка механизмов управления внутренней дисковой квотой;  • Возможность постепенного вертикального масштабирования системы;  • Отсутствие семплирования (урезания) накапливаемых данных в базе данных.  • Возможность вертикальной модернизации системы без необходимости переустановки системы;  • Поддержка использования центрального / агрегирующего контроллера мониторинга (для схем с распределенной архитектурой);  • Поддержка совместного функционирования нескольких распределенных контроллеров мониторинга под управлением центрального / агрегирующего контроллера;  • Поддержка доступа пользователей к системе через веб-интерфейс и без установки какого бы то ни было клиентского ПО. Допускается использование любого ПО, входящего в состав операционной системы, и стандартных библиотек.  • Наличие единого общего графического веб-интерфейса управления, основанного на HTTP/HTTPs с возможностью персонализации разделов для каждого пользователя  • Поддержка многоуровневой ролевой модели с поддержкой механизма разделения прав и привилегий пользователей  • Поддержка HTTP/HTTPs управления  • Поддержка SSHv2/Secure Copy  • Поддержка протокола SNMP v1/v2c/v3;  • Поддержка протокола аутентификации TACACS+;  • Поддержка аутентификации по LDAP (Active Directory);  • Поддержка хранения на устройстве резервной конфигурации устройства, а также возврат устройства на предыдущую конфигурацию;  • Неограниченное количество сохраняемых по требованию конфигураций, на которые можно осуществить возврат в любое время;  • Поддержка функционала по фильтрации и ограничению удаленного доступа;  • Поддержка кастомизации интерфейса управления (настройка панелей и виджетов, их расположения и типов отображаемой информации);  • Поддержка встроенного межсетевого экрана, фильтрующего взаимодействие виртуальной машины с удаленными узлами  • Визуализация статистики, отчетов различных типов, графиков, основанных на информации о трафике (количество переданных байт, потоков, пакетов);  • Визуализация метрик производительности сети;  • Анализ данных и возможность экспорта в PDF и CSV  • Встроенный механизм отчетов с возможностью экспорта данных в PDF или CSV, а также возможностью автоматической отправки на электронную почту;  Требования к системе детектирования аномалий:  • Поддержка механизмов выявления аномалий в сетевом трафике NetFlow v5, NetFlow v9, IPFIX, jFlow, cflowd, NetStream;  • Поддержка механизмов дедупликации сетевых потоков;  • Семплирование трафика на уровне сетевых потоков;  • Поддержка распознавания и хранения доменных имен источников трафика;  • Наличие предустановленных правил и алгоритмов, используемых для анализа сетевых потоков, инцидентов информационной безопасности и сетевых аномалий;  • Обнаружение сетевых атак (включая сканирование портов, атаки перебора паролей, DoS / DDoS, атаки на сетевые протоколы SSH, RDP, Telnet и прочие) с использованием безсигнатурных методов;  • Обнаружение аномалий в сетевом трафике, включая DNS, DHCP, SMTP, multicast и прочее;  • Поддержка анализа зашифрованного трафика с помощью отпечатков пальцев JA3;  • Обнаружение нелегитимных протоколов и приложений, включая P2P сети, сервисы “анонимизации” (включая TOR) и прочее;  • Обнаружение инцидентов информационной безопасности и сетевых аномалий, основанное на репутационных списках IP адресов и стран;  • Обнаружение операционных проблем, связанных с функционированием системных служб (включая DNS), а также выявление новых узлов и сервисов в сети;  • Автоматическое обнаружение инцидентов информационной безопасности и сетевых аномалий, на основании модели поведения узлов в ЛВС;  • Наличие предустановленных процедур для автоматизации настройки методов обнаружения инцидентов информационной безопасности и сетевых аномалий;  • Поддержка платформы MISP;  • Поддержка системы MITRE ATT&CK и отображение с учетом контекста;  • Пользовательская настройка методов обнаружения инцидентов информационной безопасности и сетевых аномалий для разных IP адресов, сегментов, сервисов и служб;  • Возможность настройки пользователем собственных методов обнаружения инцидентов информационной безопасности и сетевых аномалий на основании информации 7 уровня модели ISO OSI;  • Обнаружение NAT на основании информации 3 и 4 уровня модели ISO OSI;  • Механизм фильтрации событий, включая вложенные фильтры. Возможности импорта и экспорта фильтров через CSV файлы;  • Управление ложными срабатываниями (ручная настройка исключений)  • Пользовательская приоритезация событий, основанная на IP адресах, типах событий и привязанности событий к географической метке;  • Уведомления пользователей по протоколу Syslog, в формате CEF;  • Уведомления пользователей через механизм SNMP Trap;  • Уведомления пользователей через E-mail (в формате HTML или TXT);  • Автоматизированное реагирование на системные события на основании предопределенных пользовательских скриптов;  • Обработка потоков информации - 5000 потоков / с;  • Обработка поведенческих шаблонов - 5000 потоков / с;  • Поддержка механизмов интеграции со внешними информационными сервисами, включая DNS, WHOIS, геолокационные сервисы и прочие пользовательские сервисы, основанные на HTTP протоколе;  • Категоризация и комментирование событий пользователями системы;  • Поддержка механизмов поиска событий, основанных на типе событий, IP адресе источника событий, категории событий, ID событий и т.д);  • Интерактивная визуализация событий, основанная на графиках и таблицах пользовательского интерфейса;  • Наличие механизма отчетности и экспорта в PDF, основанного на предопределенных шаблонах и пользовательских настройках, с поддержкой передачи по e-mail;  • Экспорт событий в CSV формат;  • Поддержка интеграции по открытому API интерфейсу;  • Журналирование событий изменения конфигураций системы по Syslog во внешнюю SIEM систему;  • Поддержка визуализации событий следующих видов: Дерево событий, Временной график, Детализация, Подтверждения, Интерактивный режим;  • Поддержка интеграции со следующими сторонними продуктами: IBM QRadar App, LDAP/AD  Система должна обеспечивать:  - захват с выбираемого пользователем сетевого интерфейса, подключенного к каналу связи в высокоскоростных сетях передачи данных 10Gb/s (максимально, с учетом возможной модернизации, до 40Gb/s per link), всего сетевого трафика;   * + 1. **Система фильтрации почтового трафика**   Система фильтрации почтового трафика должна обеспечивать следующий функционал:  - проверку IP-адреса отправителя на соответствие списку разрешенных адресов для домена с помощью технологии Sender Policy Framework (SPF); Поддержка технологий DKIM/DMARC;  - поиск и удаление в режиме реального времени всех типов вирусов, червей, троянских и других вредоносных программ в потоке входящих и исходящих почтовых сообщений, проверки контрольных сумм спам-писем, включая вложения;  - детектирования вредоносных и фишинговых ссылок в теле письма;  - обеспечивать эвристические методы детектирования;  - должен обеспечить подключение и использование репутационных облачных сервисов;  - проверять на наличие спама входящий поток почтовых сообщений;  - обеспечить полноценное функционирование компонента защиты, позволяющего распаковывать и анализировать составные файлы на предмет аномалий для блокировки ранее неизвестных угроз;  - контентная фильтрация почтовых сообщений по имени, типу и размеру вложений;  - интеграция со службами каталогов Active Directory и Open LDAP;  - работа по протоколу IPv6;  - фильтрация или исключение из фильтрации сообщения по адресу отправителя письма (e-mail и/или IP-адрес) на основе собственных «черных» и «белых» списков;  - поддержка механизма защиты от спама на основе greylisting (“серые списки”;  - проверка наличия IP-адреса отправителя в списках DNS-based realtime blackhole list (DNSBL);  - проверка адресов и ссылок на сайты, присутствующих в теле письма, поддержка проверки и перезаписи URL ссылок в теле письма;  - проверка графических вложений на совпадение с известными сигнатурами спам-сообщений;  - перенос в карантинный каталог зараженных, подозрительных и поврежденных объектов почтового трафика, определять защищенные паролем файлы;  - наличие общего и персонального карантина;  - создание персональных черного и белого списков;  - осуществление по запросу антивирусной проверки объектов;  - обработка почтового трафика в соответствии с правилами, заданными для групп отправителей и получателей;  - организация дополнительной фильтрации почтового потока сообщений по именам и типам вложенных файлов и применение к отфильтрованным сообщениям отдельных правил обработки;  - использование регулярных выражений при создании правил фильтрации;  - уведомления отправителя, получателя и администратора сервера о почтовом сообщении, содержащем заражённые и подозрительные объекты;  - управление работой программы должно осуществляться с помощью командной строки (SSH), так и через специальный веб-интерфейс, работающий на браузерах: Internet Explorer, Google Chrome, Yandex;  - выявление и удаление не только однозначно вредоносных, но и потенциально опасных приложений, таких как: рекламные программы, программы-сборщики информации, программы автоматического дозвона на платные сайты и другие утилиты, которые могут использоваться злоумышленниками в своих целях;  - защита от таргетированных атак: компрометация корпоративной электронной почты (BEC), многоуровневая защита от подмены отправителя, защита от доменов-близнецов;  - поддержка высокой доступности (HA): Active-Passive; обнаружение и оповещение о неисправности устройства;  - синхронизация карантина и почтовых очередей;  - повторная инспекция при «выпуске» письма из карантина;  - анализ PDF файлов и изображений на принадлежность к спаму;  - выявление недавно зарегистрированных доменов.   * + 1. **Система сканирования на уязвимости**   Общие системные требования  Система должна иметь возможность поставки, включая, но не ограничивая, в виде следующих вариантов:  • Готового виртуального устройства (VA - Virtual Appliance) для VMware или Hyper-V;  • Пакета установки на ОС Linux.  • Центральное управление  • Система должна обеспечивать централизованное управление всеми её компонентами и функционалом через единый Веб-интерфейс.  • Система должна сохранять результаты сканирований и оценки активов в базе данных для возможности построений отчетов и хронологии изменений.  • База данных должна соответствовать следующим критериям:  • Не требовать использования сторонних БД для сохранения результатов  • Обеспечивать раздельное хранение данных сканирования в репозиториях в зависимости от результата (типы уязвимостей, группы ресурсов и пр.), при анализе или запросе данных комбинировать результаты в любой комбинации  • Хранить данные заданный и настраиваемый период времени, после истечения которого автоматически очищать базу данных (БД) от устаревшей информации.  • Пользователи системы  • Система должна поддерживать управление на основе ролей и разграничение прав доступа: Создание сканеров; Создание заданий синхронизации агентов; Создание агентских сканирований; Управлние ролями; Управление группами; Управление связами групп; Обновление проверок базы данных; Выполнение любого сканирования, при условии наличия политики сканирования или отсутствии ее; Управление пользователями; Доступ к просмотру данных об уязвимостях; Определение, создание и предоставление совместного использования списков активов; Добавление файлов аудита; Создание оповещений; Определение и совместное использование учетных данных для сканирования с предоставлением учетных данных; Создание и совместное использование политик сканирования; Управление билетами (Workflow); Аудит пользовательских действий.  • Система должна позволять пользователю принять риск обнаруженной уязвимости или переопределить до необходимого уровня, не зависимо от определенного поставщиком.  • Система должна поддерживать управление билетами рабочих процессов для расследований и устранения уязвимостей.  • Система должна позволять назначать билеты персонально.  • Система должна поддерживать список уязвимостей, которые относятся к билету.  • Система должна предоставлять возможность пользователю настраивать базовые параметры безопасности и доступа к платформе, такие как:  • Парольную политику;  • Журналирование действий;  • Таймаут сессии.  • Система должна предоставлять возможность создания неограниченного количества пользователей Cистемы.  • Шифрование передаваемых данных  • Система обязана шифровать коммуникации между компонентами/модулями Системы.  • Система должна обеспечивать шифрование коммуникации между пользователями и Системой.  • Поддержка внешней аутентификации и авторизации  • Система должна интегрироваться с системами сторонних производителей (LDAP, AD) для обеспечения аутентификации и авторизации внутренних пользователей.  • Производительность системы  • Система должна обеспечивать возможность сканировать не менее 500 IP адресов в ИТС.  • Система должна обеспечивать возможность сбора и анализа, аудита с коммутационного оборудования, маршрутизаторов, межсетевых экранов и систем предотвращения вторжений.  • Управление активами  • Система не должна полагаться на внешние сканеры для обнаружения активов, сканирования портов или идентификации ОС.  • Система должна иметь возможность ручного добавления активов.  • Система должна иметь возможность без использования активного, либо агентского сканирования, на основании разбора трафика, определять появление новых активов в сети. При этом система как минимум должна идентифицировать активы по следующим типам: Сервера, Рабочие станции, Приложения, Операционные системы, Сетевые устройства, Виртуальные и облачные системы, BYOD устройсва, Мобильные телефоны, Устройства с взломанной iOS.  • Система должна иметь возможность неограниченного инвентаризационного сканирования сети как по расписанию, так и по требованию.  • Система должна уметь связывать результаты сканирования с активами в DHCP-среде, где IP-адреса могут изменяться.  • Система должна иметь возможность динамического добавления активов на основании различных критериев и правил.  • Система должна иметь встроенный функционал автоматической классификации и динамической маркировки определенных активов в сети, включая, но не ограничивая следующие критерии: По принадлежности к IP подсети; На базе NetBIOS и FQDN имени; На базе операционной системы; По открытым портам/сервисам; По наличию конкретной уязвимости; На основании сроков сканирования; Активы, которые пропустили сканирование по расписанию и т.д.  • Система должна позволять настраивать нагрузку на инфраструктуру, во избежание перегрузки каналов заказчика во время проведения задач сканирования  • Система должна автоматически запускать службы удаленного реестра на системах Windows при выполнении сканирований с предоставлением прав, а затем автоматически останавливать эти службы после того, как сканирование завершено.  • Поддерживаемые ОС и БД для сканирования  • Система должна поддерживать, включая, но не ограничивая сканирование следующих операционных систем: Microsoft Windows; AIX; Solaris; HP/UX; Linux; Netware; MacOS.  • Система должна поддерживать, включая, но не ограничивая сканирование следующих баз данных: MS SQL; IBM DB2; Informix/DRDA; MySQL; Oracle Database; PostgreSQL; Sysbase ASE.  Визуализация данных (Dashboard)  • Система должна иметь встроенный набор панелей для визуализации данных (Dashboard).  • Система должна позволять создавать пользовательские панели визуализации данных.  • Панели визуализации должны иметь функцию автоматического обновления.  • Система должна поддерживать «drill-down» элементов панели визуализации в отдельное окно (для реализации непрерывного мониторинга, расследования инцидентов).  • Система должна поддерживать предоставление общего доступа к панелям визуализации данных.  • Панели визуализации должны позволять фильтровать информацию с помощью выбора, тэгов, активов, времени и пр.  • Система должна позволять создавать выгружать отчеты на основе отображаемых панелей визуализации данных.  Поддержка API  • Система должна предоставлять API для доступа к информации, находящейся в базе данных системы.  • Система должна иметь API для возможности интеграции с другими системами  • API должно быть предоставлено бесплатно.  • Автоматическое обновление  • Система должна обеспечивать автоматическое обновление конфигураций без дополнительных временных затрат со стороны пользователя системы. Например, обновление баз уязвимостей по отдельным компонентам системы.  • Автоматическое обновление должно включать, но не ограничиваться следующим:  • Обновление по расписанию;  • Обновление в ручном режиме;  • Возможность загрузить обновление и установить в необходимый период.  • Резервное копирование и восстановление  • Система должна обеспечивать автоматическое резервное копирования конфигурации и возможность восстановления конфигурации с резервной копии из графического единого веб-интерфейса.  • Система должна иметь возможность хранить копию конфигурации отдельно от решения.  • Масштабирование  • Система должна обеспечить простое, быстрое масштабирование и расширение функционала без необходимости дополнительных инвестиций со стороны купленного функционала.  • Система должна обеспечить взаимодействия географически отдаленных модулей, без дополнительных затрат на обслуживание.  • Система должна поддерживать балансировку нагрузки, восстановление после сбоя на сканерах уязвимости путем динамического распределения нагрузки между сканерами на основании наличия сканера на протяжении всего задания сканирования.  Сканирование  • Система должна реализовывать возможности: Сканировать по расписанию; Включать/отключать необходимые тесты в заданных задачах сканирования; Приостановить задачу на необходимое время; Иметь возможность автоматически исключить критические ресурсы из сканирования, если они заняты служебными процессами, согласно расписанию; Сканирование изолированного сегмента сети и последующей выгрузкой результатов в единую консоль; Выбор уязвимостей для сканирования; Сканирование определённых портов; Использование учётных записей.  • Система должна иметь возможность при сканировании выполнять как минимум следующие типы аутентификации:  • Для OS Windows: логин и пароль, Kerberos, CyberArk Vault, Lieberman, Thycotic Secret Server, Arcon, Centrify, BeyondTrust, Hashicorp Vault, NTLM Hash, LM Hash;  • Для Unix систем: логин и пароль, Kerberos, CyberArk Vault, Lieberman, Thycotic Secret Server, Arcon, Centrify, BeyondTrust, Hashicorp Vault, Certificate, Public Key;  • Для сетевого оборудования – SNMP;  • Система должна иметь возможность принимать цели сканирования в разных форматах: активами, IP адресам, IP сетям, именами.  • Сканирующий модуль должен устанавливаться как минимум на следующие операционные системы: Windows; Linux; MacOS; Amazon Linux; FreeBSD; Fedora.  • Система должна позволять пользователям писать и использовать собственные проверки при сканировании.  • Система должна включать в себя возможность для пассивного обнаружения активов путем наблюдения сетевого трафика на уровне пакетов, без активного сканирования систем для сетей ipv4 и ipv6. При этом система должна определять, как минимум: Список открытых портов; Перечень используемых протоколов; Перечень атрибутов хоста.  Идентификация уязвимостей  • Система должна обнаруживать и классифицировать проблемы, риски и уязвимости. Также должна предоставить подробную информацию о характере риска и рекомендаций по их минимизации.  • Система должна сообщить об известных уязвимостях в активе которые должны быть определены консультативными организациями в области безопасности (например, Common Vulnerabilities and Exposures database (CVE) или The Open Source Vulnerability Database (OSVDB) или The SecurityFocus Bugtraq (BID) или любой комбинацией из них).  • База Данных уязвимостей продуктов должна включать проверки: OS Security and Patch; CISCO; Firewalls; DNS; FTP; SMTP; RPC; SNMP; LDAP; SMB; CGI; Web Servers; Databases; Backdoors; Denial of Service; Default Accounts; Peer-To-Peer; Remote Shell;  Система должна иметь возможность:  • обнаружения сервисов, которые выполняются на нестандартных портах.  • обнаружения сервисов не настроенных на отображение баннеров подключения.  • тестировать несколько экземпляров одного и того же сервиса, работающих на разных портах.  • сканировать «мертвые узлы» (устройства, которые не отвечают на команду «ping»).  • Аудит  • Система должна предоставить возможность производить аудит конфигурации и наличия исправлений в системах: Windows; Unix/Linux; Adtran NetVanta; Alcatel TiMOS; Arista EOS; ArubaOS; BlueCoat ProxySG; Brocade FabricOS; Check Point GAiA; Cisco ACI; Cisco Firepower; Cisco IOS; Citrix Application Delivery; Database; ExtremeXOS; F5; FireEye; FortiGate FortiOS; HP ProCurve; Huawei VRP; IBM DB2 DB; IBM iSeries; Juniper Junos; MongoDB; MS SQL DB; Netapp API; OpenShift Container Platform; Oracle DB; Palo Alto Networks; PostgreSQL DB; RHEV; Salesforce.com; SonicWALL SonicOS; Sybase DB; VMware vCenter/vSphere; WatchGuard; ZTE ROSNG;  Система должна предоставить политики аудита, включая как минимум: CIS Benchmarks; Microsoft Best Practice; DISA STIGs; NIST; PHI/PII content; Пользовательские конфигурации.  • Система должна иметь возможность дополнительной интеллектуальной приоритезации, с помощью которой система должна определять приоритеты уязвимостей на основе вероятности того, что каждый из них будет использован во время атаки и сочетать в себе независимые источники данных, включая данные об уязвимостях производителя и сторонние данные об уязвимостях и угрозах , используя собственный алгоритм машинного обучения для выявления уязвимостей с наибольшей вероятностью эксплуатации в ближайшем будущем. Данная функциональность должна работать внутри системы без необходимости подключения к сети Интернет.  Оповещения и уведомления  • Система должна поддерживать оповещения на основании результатов сканирования уязвимостей или аудита конфигураций.  • Отчетность  • Система должна предоставлять отчетность по всем событиям, отчетность должна быть доступна через Веб-интерфейс.  • Система должна давать возможность самостоятельной настройки отчетности и создания собственных отчетов.  • Система должна иметь возможность генерации отчетов по запросу.  • Система должна предоставлять примеры сгенерированных отчетов для более простого использования и генерации новых отчетов пользователем.  • Система должна иметь встроенные отчеты.  • Система должна иметь встроенные, либо быстро доступные готовые пакеты отчетов лучших практик (NIST, CIS, ISO).  • Система должна предоставлять отчеты за определенный период времени по различным сегментам и системам в сети.  • Отчеты, формируемые системой, должны как минимум содержать следующую информацию:  • Название уязвимости и уровень ее критичности по шкале вендора и по CVSS;  • Перечень уязвимых систем или сервисов;  • Статус уязвимостей;  • Рекомендации по устранению уязвимости, или ссылку на патч, если таковой существует;  • Дополнительные критерии для приоритезации уязвимости: наличие эксплойта, вредоносного кода, и т.д.  • Управление уязвимостями  • Система должна отслеживать дату обнаружения уязвимости и дату последнего обнаружения для фильтрации и формирования отчетов по времени нахождения уязвимости в инфраструктуре.  • Система должна поддерживать проверку отсутствия исправлений, наличие сервисов, проверки соответствия файлам аудита и другие.  • Система должна иметь возможность импортировать информацию с систем сканирования уязвимостей сторонних производителей.  • Система должна предоставить возможность сканировать ресурсы внутри, вне сети с использование агентов, при необходимости без агентов.  • Возможности расширения  • Система должна иметь возможность расширения функционала путем добавления приложений с официального сайта производителя.  • Система должна иметь возможность расширения функционала путем добавления пассивного сканера, для поиска уязвимостей, того же производителя. Пассивный сканер должен обеспечивать возможность пассивного обнаружения хостов путем наблюдения сетевого трафика без активного сканирования системы.  Лицензирования  • Лицензирования системы должно проходить по количеству IP, не зависимо от лицензирования отдельных компонентов системы.  • В лицензию должны быть включены: Не лимитированное количество сканеров; Не лимитированное количество агентов с полной функциональностью; Политики аудита системы на соответствие мировым стандартам (DISA STIG, CIS, MSCT и др.);  • Rest API.  Интеграции  • Система должна поддерживать интеграции со следующими решениями: AirWatch by VMware – MDM; APCON - Network Monitoring; Apple – MDM; Aruba, a Hewlett Packard Enterprise company – NAC; Axonius – CMDB; Atlassian - Security Operations; BeyondTrust - Privileged Access Management; Bomgar/Lieberman - Privileged Access Management; BMC – Patch Management; Brinqa – TVM; Cisco – NAC; CyberArk - Privileged Access Management; Cymulate – Simulation; Dell - Patch Management; ForeScout – NAC; Garland Technology – Networking; Gigamon – Networking; Good powered by Blackberry – MDM; HCL BigFix - Patch Management; IBM – SIEM; Infoblox - IP Address Management; Kenna – TVM; LogRhythm - SIEM; Microsoft – SIEM; Red Hat - Patch Management; Redseal – TVM; ServiceNow - Security Operations; Splunk – SIEM; Symantec - Patch Management; ThreatConnect - Threat Intelligence; Thycotic - Privileged Account Management.  • Все перечисленные интеграции должны поддерживаться производителем Cистемы.  • Развертывание  • Все компоненты Cистемы должны иметь возможность устанавливаться и поддерживаться локально без необходимости подключения к сети Интернет  • Система должна поддерживать возможность активации оффлайн.  • Система должна поддерживать обновления Системы и информации об уязвимостях без необходимости подключения к сети Интернет.  Требования к лицензированию продукта  • Программный комплекс должен лицензироваться по следующей схеме:  Лицензия на подключение не менее 1200 ресурсов без ограничения количества пользователей.   * + 1. **Система анализа исходного кода**   Общие требования  В составе "Лицензия на программное обеспечение тестирование безопасности приложений" (далее - Продукт) должны быть следующие возможности и функции:  - анализ программного обеспечения (далее - ПО) на соответствие требованиям информационной безопасности по исходному коду;  - поиск недекларируемых возможностей (далее - НДВ) в ПО;  Продукт должен предоставлять возможность автоматически снижать количество ложноположительных и ложноотрицательных результатов.  По результатам анализа приложений информационной системы или автоматизированной информационной системы (далее - ИС или АИС) должно выдавать рекомендаций по настройке средств защиты информации (далее - СЗИ) для таких уязвимостей и НДВ, эксплуатация которых может быть предотвращена при помощи настройки СЗИ;  Продукт должен давать право на использование программного обеспечения, как минимум на одном сервере / рабочей станции / виртуальной машине без ограничений по ресурсам, и как минимум пятерым пользователям в течении года.  Функциональность Продукта по анализу исходного кода должна соответствовать следующим требованиям:  - должен выполнять анализ исходного кода написанного на следующих языках программирования: C/C++ , C#, Java, Java for Android, JavaScript , .NET Core, ASP.NET, TypeScript, Kotlin, Swift, COBOL, SAP ABAP, Scala, VB.NET, Go, Ruby, PHP, Python.  - продукт должен уметь добавлять новые языки программирования и фреймворки;  - продукт должен иметь возможность тестировать код, написанный в следующих средах программирования: AngularJS, Node.js, Vue.js, Apache Struts, .NET 4.5, ASP .NET MVC, ASP .NET, Django, EJB 2, Ionic, J2EE, JJSF 2, Jax – RS, Jax – WS, Objective C, React Native, SAP ABAP, Spring MVC, Xamarin, Symphony.  Продукт должен поддерживать интеграцию с: Azure DevOps Services, Azure DevOps Server (TFS), Apache Ant/Ounce, Apache Maven, Gradle, Jenkins, MSBuild.  Продукт должен обеспечивать возможность сканирования в режиме реального времени в IDE Visual Studio Code.  Продукт должен обеспечивать возможность сканирования как исходного кода, так и сканирования байт-кода (скомпилированного), включая анализ потока данных.  Продукт должен предоставлять возможность отслеживать трафик веб-приложений на наличие уязвимостей и сообщать о них на центральную консоль.  Продукт должен поддерживать Интерактивное тестирование приложений Java, .NET и Node.js.  Продукт должен интегрироваться с системами управления версинностями Git и задачами: Jira, Azure DevOps.  Продукт должен соответствовать следующим требованиям информационной безопасности:  - продукт должен предоставлять возможность определять и использовать роли пользователей в центральной консоли. Эти роли также должны быть распространены на локальные инструменты сканирования на рабочем столе пользователя.  - контроль доступа пользователей к ресурсам должен осуществляться в соответствии с правами пользователей, настраиваемыми офицером безопасности;  - доступ к ресурсам должен осуществляться только при помощи индивидуального логина и пароля;  - пароли пользователей должны храниться в зашифрованном виде;  - доступ к функциям офицера безопасности должен происходить только по индивидуальному логину и паролю офицера безопасности;  - должно быть обеспечено разделение доступа к функционалу по уровням иерархии;  - действия пользователя, администратора и системы на центральной консоли, а также на локальных инструментах сканирования должны журналироваться и храниться централизованно.  - система единого входа на центральную консоль должна поддерживать использование SAML для интеграции с поставщиками удостоверений Microsoft, Okta и PingFederate.  Продукт должен предоставлять следующие функциональные возможности:  - предоставлять всю информацию на русском и/ или английском языках;  - предоставлять единую точку доступа к информации, предоставляемого Продукта;  - должна быть предусмотрена центральная консоль с дашбордами, чтобы обеспечить видимость состояния безопасности всех приложений и их статус с течением времени.  Продукт должен предоставлять информацию о рейтинге угроз безопасности, статусе тестирования, открытых проблемах, основных типах проблем и серьезности проблем.  Требования к базе данных уязвимостей и шаблонов правил  Продукт должна иметь возможность создавать настраиваемые правила для настройки базы данных и интеграции настраиваемых уязвимостей.  Требования к описанию уязвимости/исправлениям  В технической информации о каждой обнаруженной уязвимости должны быть указаны:  • тип уязвимости  • как, где и когда она была выявлена,  • серьезность возможной эксплуатации, если ее не исправить  • четкая классификация уязвимостей  • предложения и рекомендации по исправлению / смягчению последствий  • примеры соответствующего и несоответствующего решения  Требования к отчетности  Продукт должен иметь возможность создавать отчеты в формате PDF и HTML:  • CWE/SANS Top 25 2011  • DISA Application Security and Development STIG  •Open Web Application Security Project (OWASP) Mobile Top 10  •Open Web Application Security Project (OWASP) Top 10 2013, 2017, 2021  • Payment Card Industry Data Security Standard (PCI DSS) Version 3.2  • Software Security Profile  Должны поддерживаться протоколы SSL и TLS (Transport Layer Security).  Должна быть предоставлена техническая поддержка от Исполнителя не менее 12 (двенадцать) месяцев со дня подписания уполномоченными представителями заказчика и Исполнителя Акта ввода в действие услуги.  Исполнитель должен предоставить вычислительные мощности для продукта, осуществить на нее установку и настройку поставляемого сервиса;  Обучить сотрудников заказчика использованию инструмента;   * + 1. **Система управления и мониторинга привилегированного доступа**   Система управления и мониторинга привилегированного доступа должна обеспечивать следующий функционал:  Решения должны работать в режиме ПРОКСИ, без необходимости для администратора устанавливать агенты в системах, защищенных решением PAM.  Решение должно собираться в отказоустойчивый кластер  Решение должно иметь возможность балансировки нагрузки  Запись и контроль сессий привилегированных пользователей (команд и выполненных действий), позволяющие использовать функции безопасности по безусловности выполненных действий и защите материала для доказательной базы.  Решение должно поддерживать реализацию на облачных платформах, таких как Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure. Оно также должен поддерживать виртуальные среды: виртуальную машину на основе ядра (KVM), Microsoft Hyper-V, OpenStack, VMware vSphere. Также должна поддерживаться возможность использования самостоятельной аппаратной платформы.  Решение должно изначально поддерживать подключения для протоколов SSH и RDP к PROXY и SSH / TELNET / RLOGIN / RDP / HTTP / HTTPS / VNC от PROXY к защищаемым системам.  Для нестандартных протоколов (изначально не поддерживаемых решением) должна существовать возможность вызова клиента, поддерживающего такой протокол на инсталляционном сервере таким образом, чтобы пользователю были видны только клиент и его ресурсы.  Для нестандартных протоколов и их вызова клиентом решение должно поддерживать технологии для Microsoft Remote App.  Возможность назначения прав доступа администратора, пользователя, аудитора, в зависимости от настроек профилей.  В случае доступа аудитора профиль пользователя должен, по крайней мере, предлагать возможность ограничения доступа к записям выбранных групп пользователей и целевых групп системы вместе с настроенными для них привилегированными учетными записями.  Конфигурация профиля пользователя должна включать возможность фильтрации входящих соединений на основе исходного IP-адреса, то есть, создание списков управления доступом (ACL) для пользователей с назначенным профилем. Определение ограничения должно разрешать формат: IP-адрес, сетевой адрес и сетевая маска или полное доменное имя (FQDN).  Решение должно позволять определять политику доступа, путем отнесения выбранной группы пользователей к указанной группе целевых систем.  Предварительный просмотр записанных данных должен включать видеозапись сеанса и расшифровку записи, показывающую все метаданные сеанса (RDP), а также полную запись отображаемых данных для консоли (SSH).  Мониторинг соединения в реальном времени, в том числе возможность просмотра сеанса в реальном времени с возможностью его немедленного прекращения.  Управление наборами правил (политиками) паролей локальных пользователей и администраторов.  Возможность включения / отключения записи сеанса для выбранных групп пользователей.  Возможность настройки доступа через веб-портал, браузер, по крайней мере, для сессий SSH и RDP, без необходимости установки специального плагина в браузере.  Решение обеспечивает интеграцию с Microsoft Active Directory без необходимости синхронизации информации пользователя. Это означает, что пользователь Active Directory добавляется в группу пользователей автоматически, в то же время распознается решением PAM.  Для сеансов RDP - возможность блокировать ограничивающие TCP-соединения в целевой системе сервера Microsoft Windows.  Для сеансов RDP - возможность блокировать выбранные процессы в целевой системе сервера Microsoft Windows.  Для сеансов SSH и RDP, возможность создавать шаблоны регулярных выражений для выполняемых команд, и, если такой шаблон обнаруживается, возможность установить одно из действий: завершение сеанса или отправка уведомления об обнаружении шаблона.  Задание шаблонов выполняемых команд для SSH и RDP должно выполняться на уровне создания групп пользователей, для которых создается доступ, или на уровне группы целевых систем, доступ к которой защищен и контролируется PAM-решением.  Защита паролей, введенных во время сеансов, путем обнаружения курсора ввода в полях ввода пароля или в окне управления учетными записями пользователей.  Аутентификация пользователя по логину / паролю, сертификату X.509, ключу SSH.  Поддержка протоколов аутентификации: KERBEROS, RADIUS, Microsoft Active Directory, LDAP, TACACS +.  Возможность установить дополнительное согласование рабочего процесса для подключений к выбранной группе целевых систем указанным количеством утверждающих.  Возможность установить дополнительное разрешение доступа в зависимости от времени входа в систему, например, одобрение не требуется с понедельника по пятницу с 8:00 до 16:00, а для всех остальных дней и часов одобрение требуется.  Возможность автоматической ротации паролей и ключей SSH для определенных хостов или групп учетных записей.  Возможность создавать исключения для автоматических паролей и ключей SSH.  Создание расписаний для автоматической смены паролей в целевых системах.  Создание одноразовых паролей и их автоматическая замена после использования.  Возможность создавать собственные политики / требования для смены паролей:  a. Требуемое минимальное количество символов,  b. Исключение символов, указанных администратором,  c. Обязательное использование букв верхнего и нижнего регистра,  d. Обязательное использование специальных символов,  Возможность устанавливать разные политики смены паролей для разных групп хостов или групп учетных записей.  Установка срока действия пароля в течение указанного периода времени.  Контроль паролей в файлах путем их сокрытия или расшифровки.  Предоставление плагинов, позволяющих изменять пароли или ключи SSH для следующих систем: AIX, F5 BIG IP, SAP, SAP IQ, AWS IAM, Checkpoint, ESX, Fortinet Fortigate, HP iLO, MS SQL Server, ORACLE, Stormshield, Teradata, Unix, Micorsoft Windows, Cisco, Dell iDRAC, IBM 3270, Juniper SRX, LDAP, MySQL, Palo Alto, Grafana.  Решение должно разрешать смену пароля с использованием как минимум REST API.  Требования к лицензированию продукта  Программный комплекс должен лицензироваться по следующей схеме:  Бессрочная лицензия на подключение 1000 ресурсов без ограничения количества пользователей.   * + 1. **Услуга проведения тестирования на проникновение.**   Исполнитель должен ежегодно проводить:   * внешние тесты на проникновение 1 раз в год, не менее 30% от используемых ip-адресов и не менее 10 веб-приложений на внешнем периметре Заказчика; * тестирование на проникновение и отказоустойчивость web-сервисов, отдельных узлов и приложений.   Сценарии проведения тестирования на проникновение и используемые инструменты согласовывается с Заказчиком. По итогам Исполнитель предоставляет отчет с последующим контролем устранения выявленных уязвимостей.  Все работы должны проводиться в соответствии с требованиями нормативных правовых актов РК и внутренних нормативных документов АО «НК «ҚТЖ в области информационной безопасности и информатизации.   * + 1. **Требования к услуге повышения осведомлённости пользователей**   В рамках повышения осведомленности работников Заказчика на весь период действия договора Исполнителем предоставляются следующие материалы в электронном виде и услуги:   * Буклет по основам ИБ; * Изображения по основам ИБ (не менее 15 штук); * Проведение обучение по каждому предоставляемому сервису; * Памятка по основам ИБ.   Теоретический материал курса должен быть представлен в следующих форматах:   * текст; * изображения (фото/графика/иллюстрация); обучающие видео; * цикличные анимации   Практический материал курса должен быть представлен в следующих форматах:   * тесты(pickone). Функциональные требования * Курс должен воспроизводиться в информационной системе (Система), которая предоставляет следующие   возможности:   * Система должна предоставлять доступ к учебным материалам курса через веб-браузер без установки   стороннего ПО (Flash, Java, ActiveX и подобные) и быть доступна по протоколу HTTP или HTTPS;   * Система должна иметь функцию соединения со службами каталогов LDAP для синхронизации   пользователей, групп пользователей и аутентификации пользователей;   * Система должна иметь функцию авторизации учетной записью пользователя из службы каталогов   LDAP;   * Система должна предоставлять функцию настройки структуры курса, его материалов и активностей; * Система должна предоставлять функцию интеграции со сторонними сервисами для проведения   вебинаров;   * Система должна запоминать этап прохождения курса и давать возможность пользователю продолжать с места остановки; * Система должна иметь отчеты о статусе прохождения курса слушателями; * Система должна предоставлять возможность тестирования только по 100% прохождению лекции и   ограниченное количество попыток;   * Система должна предоставлять возможность проходить тестирование независимо от статуса прохождения лекции; * Система должна иметь возможность формирования и использования банка вопросов; * Система должна иметь возможность случайной выборки вопросов теста для исключения одинакового состава вопросов в попытках; * Система должна иметь возможность показа вопросов теста в случайном порядке; * Система выдает результаты тестирования автоматически после завершения тестирования и не дает возможность исправить результат; Система должна иметь возможность автоматически заблокировать учетную запись пользователя в службе каталогов LDAP если он не набрал проходной балл необходимого теста; * Система должна иметь встроенные промежуточные отчеты по статусу прохождения тестирования среди всех слушателей курса; * Система должна предоставлять возможность формировать учебные группы и потоки; * Система должна иметь возможность записать группу пользователей на курс; * Система должна иметь отчет по прогрессу прохождения курса группой слушателей – процент прохождения курса каждым слушателем и график прогресса группы по дням; * Система должна иметь возможность сформировать собственный шаблон сертификата о прохождении курса (конструктор); * Система должна иметь возможность выдавать сертификат о прохождении курса в автоматическом и ручном режимах; * Система должна предоставлять интерактивный отчет (дэшборд) с информацией по запущенным компаниям в разрезе статусов, как в общем, так и по каждому пользователю. * Каждый сотрудник сможет осуществить вход в СДО и начать обучение под своей учетной записью Active Directory. * Администратор системы должен будет назначить пользователей на курс для начала его прохождения.   В рамках повышения осведомленности и квалификации работников Заказчика предоставляются услуги:   * Ежегодное проведение стажировки в течении не менее 5 дней, не менее 5 человек в SOC Исполнителя.   + 1. **Требования к услуге компьютерной криминалистики (форензика)**   Оказание услуги по расследованию критических инцидентов информационной безопасности. В рамках оказания услуг проводятся работы по анализу сетевой активности, логов, изменений настроек, восстановлению удаленной информации, поиску и локализации вектора атаки.   * + 1. **Требования к услуге консалтинга**   Перечень консалтинговых услуг:   * Консалтинг в области технической политики ИБ: * Консалтинг в составлении политик классификации активов * Консалтинг в области выборе методов технического контроля * Консалтинг в области подбора программных и аппаратных средств защиты * Консалтинг по использованию решений ИБ * Консалтинг в области учета информационных активов и централизованного управления ИБ активов. * Консалтинг по информационному взаимодействию: * Составление оптимальных рекомендаций по уровню разрешенного доступа для различных категорий пользователей (включая внешних подрядчиков) для различных систем. * Формирование рекомендаций по выборы технических средств и методов для реализации контроля доступа к ИС/АС * Рекомендации по применяемым мерам для различного информационного взаимодействия (выбор режимов блокировки, мониторинга, дополнительных ручных проверок) * Бизнес-консалтинг: * Оценка собственных рисков ИБ связанных с информационными системами СУИБ и данными этих ИС. * Рекомендации по формированию регламентов доступа сотрудников Заказчика к СУИБ.   + Рекомендации по описанию бизнес-процессов с компонентами СУИБ     1. **Требования к системе очистки DDoS атак**   Основными целями внедрения данной системы являются:  Обеспечение работы легитимных пользователей в случае возникновения DDoS атаки;  Защита сети от много-векторных DDoS атак в режиме реального времени в автоматическом режиме, т.е. без активного участия персонала;  Предоставление службе ИБ отчетной информации об атаках.  Исполнитель обязуется предоставить письменные подтверждения наличия авторизации или партнерского статуса (копии соответствующего дилерского соглашения или документа от производителя, официального дистрибьютора с приложением копии авторизационного письма, подтверждающего наличие авторизации/партнерского статуса на поставку данного Оборудования или экземпляры Программного Обеспечения, заверенного печатью и/или подписью, или факсимиле).  ПО должно быть полностью совместимо с Поставляемым Оборудованием и соответствовать функциональным требованиям настоящего Технического Задания.  Требования к Оборудованию и ПО  Оборудование должно быть актуальным, не вышедшим из поддержки и протестированным на заводах производителя. Вся необходимая техническая документация и руководства пользователя должны быть предоставлены в полном объеме, предусмотренном производителем. В комплект поставки должны входить все необходимые принадлежности для обеспечения работоспособности поставляемого Оборудования.  В том случае, если Оборудование в течение срока действия договора поставки будет снято с производства, поддержки (end of life) или по иным обстоятельствам не сможет быть поставлено Заказчику, Исполнитель будет обязан предложить равноценную замену такого Оборудования без увеличения его стоимости и снижения функциональности.  В том случае, если ПО или его версии в течение срока действия договора поставки будут сняты с производства, поддержки (end of life) или по иным обстоятельствам не сможет быть поставленоЗаказчику, Исполнитель будет обязан предложить равноценную замену такого Программного Обеспечения без увеличения его стоимости и снижения функциональности.  Поставляемое Оборудование должно быть укомплектовано всеми компонентами (крепежными элементами, кабелями электропитания и заземления), необходимыми для сборки и проведения пуско-наладочных и инсталляционных работ на площадке Заказчика.  Оборудование и ПО должны быть поставлены в полном объеме не позднее 5 рабочих дней с даты подписания Договора.  Доставка оборудования по адресу доставки, разгрузка-погрузка оборудования (c обеспечением грузчиками и при необходимости специальными техническими средствами) выполняются силами и за счет Исполнителя. Разгрузка осуществляется в указанное Заказчиком помещение и место.  Система должна иметь модульную структуру и состоять не менее чем из двух подсистем:  Подсистемы подавления DDoS атак работающей в режиме inline (возможно несколько устройств) суммарной способностью подавлять атаки до 10 Гбит/с. Подсистема подавления DDoS атак должна обеспечивать отказоустойчивый режим работы.  Подсистемы управления и анализа  Каждое устройство подавления атак, входящее в предложение участника должно соответствовать или превосходить следующие требования:   |  |  | | --- | --- | | Требование | Значение | | Величина отражаемой атаки в режиме (Гбит/с), | 10 | | Суммарный легитимный трафик, защищаемый системой, не менее (Гбит/c) | 5 | | Количество обрабатываемых пакетов (PPS), не менее | 7.2M | | Максимальная вносимая задержка, не более | 60 мс | | Скорость реакции на изменение вектора атаки, не более | 18 секунд | | Обнаружение и защита от всех типов атак должна осуществляться в автоматическом режиме. | Обязательно | | Настройки должны производиться как в ручном режиме, так и в автоматическом на основе вычисления параметров трафика без атаки | Обязательно | | Система должна блокировать некорректные пакеты (с неправильной контрольной суммой, некорректными заголовками, неполные или дублированные фрагменты, короткие пакеты) | Обязательно | | Поддерживаемые интерфейсы (на одном устройстве) | 8x1G Copper Ethernet и 4х 10GE (SFP+) | | Наличие дополнительного блок питания | Обязательно | | Наличие отдельного интерфейса управления | Обязательно | | Возможность работы в прозрачном режиме (L2 transparent) | Обязательно | | Возможность работы в IP режиме (L3) | Обязательно | | Основной режим работы In-line | Обязательно | | Возможность работы в режиме c как однонаправленным (unidirectional) так и с двунаправленным (bidirectional) трафиком | Обязательно | | Возможность работы в смешанном режиме, когда однонаправленный и двунаправленный трафик смешаны произвольным образом | Обязательно | | Возможность различных вариантов реакции на атаку (блокировка пакетов и уведомление администратора ИБ, только уведомление администратора ИБ). | Обязательно | | Полная поддержка стека протоколов IPv4 и IPv6 | Обязательно | | Защита от мульти-векторных атак DDoS, нацеленных на разные уровни модели OSI (2-7) одновременно | Обязательно | | Защита от атак TCP flood (включая SYN, SYN-ASK, PUSH, FIN, RST, ASK flood, сгенерированный mirai flood, TCP Fragment flood, flood сгенерированный некорректными TCP пакетами) | Обязательно | | Защита от TCP connection flood | Обязательно | | Защита от ICMP flood (echo request, unreachable, source quench) | Обязательно | | Защита от Flood внутри GRE туннелей | Обязательно | | Защита от IGMP flood | Обязательно | | Защита от HTTP connection flood (включая аутентификацию методом Запрос – Ответ используя java-script, 302 redirect и др.) | Обязательно | | Защита от HTTPS connection flood (включая аутентификацию методом Запрос – Ответ используя java-script, 302 redirect и др.) | Обязательно | | Возможность дешифрации только первого HTTPS запроса | Обязательно | | Возможность полной дешифрации HTTPS трафика | Обязательно | | Защита от SMTP и FTP flood | Обязательно | | Защита от атак HTTP и FTP brute force | Обязательно | | Защита от UDP flood (включая random port flood, flood большими пакетами, mirai-originated flood) | Обязательно | | Защита от amplification атак | Обязательно | | Защита DNS, включая  защиту от перебора имен  spoofed source address  Random-Subdomains Attack  Amplification Reflective Attack  Dictionary Attacks и Brute Force Attacks | Обязательно | | Защита DNS посредством позитивной модели, базирующейся на автоматическом составлении белого списка доменов, с возможностью его редактирования в ручном |  | | Защита от SIP flood и SIP brute force | Обязательно | | Защита от атаки неправильно сформированными пакетами SIP | Обязательно | | Защита от медленных атак (Slow Loris, Slow Read и т.д.) | Обязательно | | Защита от пульсирующиx (burst) атак | Обязательно | | Защите от атак, направленных на SSL/TLS (включая renegotiation, handshake, flood) | Обязательно | | Защита от SSL атак без расшифровки трафика (включая L7 connection flood, то есть flood внутри SSL туннеля) | Обязательно | | Зашита от неизвестных атак (Zero-day), автоматическая генерация описаний (сигнатур) атак в режиме реального времени | Обязательно | | Защита от известных уязвимостей в режиме реального времени (Регулярное и экстренное обновление описаний) | Обязательно | | Возможность создания описаний (сигнатур) атак в ручном режиме | Обязательно | | Возможность блокирования хостов, участвовавших в бот сетях за последние 24 часа (возможно с использованием дополнительных лицензий) | Обязательно | | Возможность администратору формировать собственные политики защиты и обеспечивать возможность их оперативной модификации. | Обязательно | | Защита от злонамеренного ПО (malware) | Обязательно | | Возможность создания Черных и Белых списков | Обязательно | | Защита от атак по географическому признаку (возможно с использованием дополнительных лицензий) | Обязательно | | Ограничение скорости трафика от определенного источника, к получателю или по их комбинации (rate limiting, connection limiting) на уровне протокола, приложения, сетевого сегмента, физического порта, группы | Обязательно | | Обнаружение аномальной работы протоколов для обнаружения зловредного/вредоносного трафика в режиме реального времени | Обязательно | | Защита от «вертикального» и горизонтального сканирования портов. | Обязательно | | Возможность фильтрования пакетов на основе информации L3, L4, L7. | Обязательно | | Поддержка API интерфейса для организации взаимодействия со сторонними системами. | Обязательно |   Функционально-технические требования к системе системы управления устройствами защиты от DDoS  Система может разворачиваться в виде аппаратного решения или в виде ПО, разворачиваемого в качестве виртуальных машин в среде виртуализации VMware или KVM (любой).  Один экземпляр ПО Системы должен обеспечивать мониторинг и управление не менее 2 аппаратных или виртуальных устройств.  Доступ к интерфейсу Системы управления должен осуществляться посредством web-браузера.  Система должна поддерживать разграничение доступа пользователей к системе на основе ролей, групп пользователей, в том числе посредствам интеграции с каталогом Active Directory, с ограничением доступа к устройствам.  Визуализация информации о текущих и прошедших атаках;  Генерация отчетов о по статистике атак и их выгрузка в форматах CSV, XML, PDF с автоматической рассылкой через e-mail.  Система должна выполнять следующие функции в части управления устройствами защиты от DDoS:  Отображение информации об устройстве, такой как использование CPU;  Отображение информации о версии установленного ПО устройств и их централизованное обновление;  Управление лицензиями устройств;  Создание резервных копий конфигурационных файлов устройств;  Система должна выполнять следующие функции в части мониторинга устройств защиты от DDoS:  Мониторинг состояния ключевых показателей и оповещение в случае превышения пороговых значений;  Мониторинг изменений конфигураций с возможностью отслеживания учетных записей и времени внесения изменений.  **2.5.18 Требования к системе фильтрации трафика веб-приложений** Требования к оборудованию Система распределения нагрузки (ADC – application delivery controller) и защиты трафика веб-приложений (WAF) предназначена для размещения в сетевой инфраструктуре Заказчика.  Основной целью внедрения системы распределения нагрузки (ADC – application delivery controller) и защиты от атак прикладного уровня является: - Дешифрация трафика шифрованного с использованием шифрования TLS версий 1.0/1.1/1.2/1.3; - Оптимизация веб трафика; - Защита Веб-приложений от атак прикладного уровня, таких как: OWASP TOP-10; - Распределение нагрузки между компонентами сервисных структур, таких как серверы приложений и т.д.; - Запись публичного IP адреса клиента в произвольное поле http-заголовка.  **Пропускная способность и производительность**  Предлагаемое решение должно поставляться в виде программно-виртуального комплекса и обеспечивать обработку HTTP/HTTPs трафика суммарной пропускной способностью не менее 1 Гбит/с.  Поставляемые лицензии должны поставляться в виде продлеваемой годовой подписки, включающей стоимость годовой технической поддержки. Минимальный срок подписки – 1 год.  Предлагаемый программно-виртуальный комплекс должен поддерживать возможность развертывания на распространенных платформах виртуализации, таких как: VmWare vSphere, KVM, Microsoft Hyper-V.  Суммарное количество экземпляров программно-виртуальных комплексов должно быть не менее 8 шт.  Поддержка аппаратной обработки шифрования протоколов TLS 1.0/1.1/1.2/1.3;  Резервирование блоков питания на каждом физическом устройстве.  Наличие ролевой модели при использовании виртуальных машин.  Функциональные требования к программной и аппаратной частям.  Поддержка протоколов (без дополнительных лицензий): IEEE 802.3ad (LACP) агрегации каналов; OSPFv2/3, BGP; GSLB.  Решение должно поддерживать работу в сетях IPv4, IPv6  Поддержка Layer2 и Layer3 Forwarding, если пакеты не предназначены для балансировки;  Поддержка протоколов STP: MST, RSTP  Поддержка протоколов агрегирования каналов (не менее 4-х портов)  Статическая агрегация  Динамическая агрегация (LACP)  Поддержка технологии VLAN (802.1q, не менее 1000 на устройство)  Отказоустойчивость:  Поддержка протоколa VRRP  Наличие не менее одного независимого интерфейса для внешнего управления оборудованием (OOBM);  Техническая невозможность передачи трафика между интерфейсом управления и интерфейсами передачи данных.  Поддержка режимов работы: Обратный прокси-сервер (reverse proxy); Прозрачный прокси сервер (transparent proxy).  Поддерживаемое количество элементов в кластере – не менее 2 устройств. Любой из компонентов кластера должен иметь возможность вывода в режим обслуживания без потери работоспособности кластера в целом.  Поддержка отказоустойчивости в режиме active-standby; Поддержка отказоустойчивости в режиме active-active (не менее 8 устройств); Поддержка отказоустойчивости в режиме active-standby с возможностью позадачного перевода нагрузки между устройствами в ручном режиме.  Поддержка сохранения состояния сессий при переключении между active/standby (stateful-failover);  Возможность построения территориально распределённых GSLB кластерных систем.  Поддержка управления сертификатами SSL.  Поддержка предоставления различных сертификатов в зависимости от Server Name Identification (SNI).  Возможность балансировки SSL трафика с учетом терминирования на устройстве для манипуляций с HTTP трафиком.  Поддержание протоколов TLS 1.0/1.1/1.2/1.3; Возможность полного отключения протокола TLS 1.0 и 1.1;  Возможность использования индивидуально подобранных шифров;  Поддержка одновременно разных профилей шифрования на внешних и внутренних интерфейсах (Front End & Back End);  Возможность отключения функции TLS Renegotiation.  Должна обеспечиваться балансировка не менее 4000 реальных серверов при использовании проверки доступности (health check).  Поддержка виртуализации с разделением аппаратных ресурсов (CPU, RAM и др.) и физических портов;  Наличие ролевой модели управления.  Синхронизация времени на контроллерах от внешних источников NTP  Для поиска неисправностей должны поддерживаться встроенные механизмы анализа проходящего через устройства трафика аналогичные утилите tcpdump  Требования к функциональности балансировки  Возможность проверки работоспособности и доступности серверов и приложений:  Наличие предустановленных проверок L3 (ICMP);  Наличие предустановленных проверок L4 (TCP/UDP port check);  Наличие предустановленных проверок L7 уровня приложений.  Поддержка механизмов распределения нагрузки: Round Robin; по адресу источника / назначения; на основе содержимого приложения; в зависимости от времени отклика приложений; на основе объема обработанного трафика; на основе количества соединений; на основе комплексного распределения (вторичный признак) относительного веса сервера; поддержание постоянной неразрывной сессии L4 (persistency);  Направление сессии на один и тот же сервер (stickiness): на основе IP адреса либо IP+Port; на основе cookie; на основе SSL session ID; на основе данных из заголовка HTTP пакета; на основе данных в XML tag.  Поддержка возможности модификации на уровне L7, в том числе при помощи пользовательских скриптов.  **Требования к функциональности оптимизации**  Поддержка ускорение работы веб ресурсов (Web Performance Optimization (WPO)): Определение платформы браузера / мобильного браузера с соответствующей оптимизацией; Кеширование данных для снижения нагрузки на платформы; Оптимизация изображений, включая прогрессивную обработку изображения, сжатие и консолидацию; Консолидация ресурсов, для CSS, Java скриптов и изображений;  Модификация: JavaScript и CSS.  **Требования к функциональности защиты Веб-приложений (WAF)**  Поддержка работы в режимах:  Режим монитора (просмотр зеркалируемого трафика с оповещением о нелегитимных запросах/ out-of-path);  Режим прозрачного проксирования (Transparent Proxy). В данном режиме система должна поддерживать следующие варианты обработки трафика: блокировка нелегитимных запросов; пропуск и оповещением о нелегитимных запросах.  Режим полного проксирования (Full Proxy). В данном режиме система должна поддерживать следующие варианты обработки трафика: блокировка нелегитимных запросов; пропуск и оповещением о нелегитимных запросах.  Должна поддерживаться как негативная модель безопасности, блокирующая известные атаки, так и позитивная, основанная на изучении нормального для защищаемого приложения трафика и выявлении аномальной активности.  Система должна обеспечивать поддержку, распознавание и проверку на соответствие стандартам протокола HTTP и протокол Websocket;  Поддержка распространённых заголовков HTTP-протокола, включая возможность добавления собственных заголовков;  Защита от переполнения размеров полей HTTP-заголовков;  Система должна защищать приложения от уязвимостей OWASP Top 10;  Система должна поддерживать функционал для целевого противодействия типичным атакам, включая: Session hijacking, Buffer overflows, Forceful browsing, Hidden fields manipulation, Remote File Inclusion, Directory/Path traversal, XXE Injection, Request Header Filtering, Request Method Filtering, Response Header Filtering, SQL Injection, NoSQL Injection.  Система должна обеспечивать защиту от автоматизированных массовых атак и параллельных атак с возможностью ограничения доступа к веб-ресурсу при превышении определённых заранее заданных метрик, в том числе:  Защита от атак на отказ в обслуживании (DoS, DDoS) на прикладном уровне;  Детектирование и блокировка запросов, осуществляющих перебор паролей к аккаунтам веб-приложения (Brute Force);  Система должна обеспечивать защиту от медленных атак (Slow Loris, Slow Read и т.д.)  Система должна обеспечивать блокировку атакующих, на внешних устройствах защиты периметра (т.к. DefensePro), на основе анализа их действий. Расчета баллов «не легитимной деятельности» и время блокировки должен зависеть от уровня серьезности и количества атак.  Система должна считать рейтинговые баллы для каждого источника обнаруженной атаки, для фильтрации по результатам определяемых пороговых значений даже если атакующий находится за NAT или прокси. Легитимные пользователи, находящиеся за тем же NAT или прокси, блокироваться не должны;  Система должна блокировать запросы к запрещенным URL/URI или файлам приложения, с начислением рисковых индикаторов на источник;  Система должна обеспечивать возможности одновременной защиты нескольких хостов (веб-приложений) на том же опубликованном IP-адресе с применением полностью не зависящих друг от друга политик защиты (т.е. изменения в одной политике не влияют на остальные находящиеся на том же IP-адресе).  Система должна предоставлять механизмы защиты от потенциально неблагонадёжных адресов с обеспечением регулярного настраиваемого обновления репутационных списков;  Система должна предоставлять механизмы блокировки адресов на основании географической принадлежности, относящимся к определённым странам  Система должна включать функционал для перехвата ошибок сервера, для отображения настраиваемых служебных страниц;  Система должна обеспечивать защиту от раскрытия чувствительной информации (номера кредитных карт, телефонов и паспортных данных)  Система должна обеспечивать применение/активации интеллектуальных механизмов автоматизированного обучения для любого количества веб-приложений (хостов) на том же опубликованном IP-адресе с применением полностью не зависящих друг от друга политик защиты (т.е. изменения в одной политике не влияют на остальные находящиеся на том же IP-адресе).  Система должна обеспечивать применение интеллектуальных механизмов автоматизированного обучения, детектирование аномалий и блокировка нелегитимной активности, в том числе:  Возможность ручного включения и отключения режима защиты после завершения первоначального обучения для каждого защищаемого веб-приложения по отдельности;  Возможность ручного включения и отключения режима защиты после завершения первоначального обучения для каждого модуля/типа защиты для любого веб-приложения по отдельности;  Возможность обучения в тестовых условиях (staging) и перенос полученной политики в продуктивные условия.  Система должна предоставлять возможности для создания разных политик для каждого/любого уровня приложения (URI);  Система должна иметь функционал автоматического запуска внешнего сканера безопасности при изменении структуры сайта и обработки отчетов от него, с автоматическим применением.  В системе должна быть возможность извлечения реального IP-адреса источника из произвольного поля заголовка HTTP;  Система должна вести подробные журналы об обнаруженных и заблокированных угрозах;  Система должна обеспечивать возможности передачи сообщений, которая включает информацию о конкретных атакующих, которые должны быть заблокированы, на основе L4 или L7 (например, XFF) информации;  Система должна поддерживать создание пользовательских страниц об ошибках. Должна быть возможность размещения данной страницы как на самом устройстве защиты, так и на внешнем веб сервере;  **Мониторинг и управление**  Поддержка управления через протоколы HTTPS, SSH; telnet  Поддержка аутентификации по протоколам TACACS+, RADIUS, LDAP;  Поддержка возможности отключения небезопасных протоколов Telnet & HTTP (если присутствуют);  Поддержка списков доступа на интерфейсах управления;  Поддержка возможности получения расширенной статистики по протоколам SNMP v3;  Поддержка настройки уведомлений используя Syslog, SNMP Traps;  Наличие ПО для централизованного мониторинга и управления.  Возможность гибкой настройки отправки SNMP оповещений (SNMP trap) на разные сборщики SNMP сообщений.  Поддержка прикладного интерфейса RESTful API.  Поддержка ролевой модели администрирования  Система централизованного мониторинга должна поддерживать (возможно при наличии отдельной лицензии):  Встроенные утилиты создания пользовательских отчетов.  Предоставление отчетов о производительности пользовательских приложений: задержка в ЦОД, сетевая задержка, задержка на стороне клиента, в том числе в зависимости от браузера, используемого на стороне клиента.  Встроенные средства мониторинга должны позволять просмотреть все метрики минимум за 90 дней, а также предоставлять исторические отчеты по всем устройствам.  Система должна иметь поддержку автоматизации рутинных операций  сохранения и восстановления конфигурации;  изменения конфигурации по расписанию;  предупреждения об окончании срока действия сертификатов  проверки, что конфигурации всех устройств применены корректно и сохранены в постоянной памяти устройств;  проверки того, что используемые SSL-политики соответствуют политике организации.  Для каждого устройства система должна иметь функцию мониторинга: статуса интерфейсов; загрузки использования процессора, памяти, дискового пространства; состояния кластера;  Система должна иметь возможность показывать список аварий для каждого устройства;  Система должна иметь возможность аудита действий всех пользователей системы.    **2.6** **Требования к отчетным документам**  Исполнитель обязуется:   * в течении 10 рабочих дней после заключения Договора предоставить на согласование Заказчику, а Заказчик в свою очередь в течении 5 дней после предоставления согласовать, форму ежеквартального сводного отчета, с текстовой, табличной и графической (диаграммы, графики) информацией по ключевым показателям исполнения Договора, а именно: * статистические данные по запросам и инцидентам за отчетный период; * анализом состояния инфраструктуры ИБ; * перечень проблемных вопросов и рекомендации по их решению и улучшению работы инфраструктуры ИБ; * актуальные контактные данные специалистов, ответственных за оказание Услуги. * по запросу Заказчика, не чаще одного раза в год, на основании информации по сопровождаемым средствам защиты, событий ИБ и зафиксированных инцидентов ИБ, предоставить аналитический отчет с анализом состояния инфраструктуры ИБ, включая перечень проблемных вопросов, их анализ и рекомендации по улучшению работы инфраструктуры ИБ. * ежеквартально и по запросу Заказчика, но не чаще одного раза в месяц, предоставлять Заказчику сводный отчет и актуальные контактные данные специалистов, ответственных за оказание Услуги/Сервиса.  Требования к Сервису В ходе реализации проекта, в обязательном порядке, должны быть выполнены следующие действия по внедрению сервисных услуг:   * все системы должны быть размещены на территории Заказчика; * осуществлена установка и активирование лицензий на предоставляемые инструменты защиты; * формирование проектной документации в составе: * пояснительной записки: пояснительная записка должна содержать в себе информацию описывающую процесс каждого сервиса, его интеграцию со смежными системами, содержать в себе физические (сетевые, размещение оборудования в шкафах, кабельный журнал), логические, структурные и иные схемы взаимодействия, в пояснительной записке, должен быть описан внедренный функционал каждого сервиса; * руководства администратора сервиса – руководство администратора должно содержать в себе описание механизмов администрации сервиса, изменения его настроек, пере конфигурации сервиса, обновления ПО сервиса или его компонентов, проведения регламентных мероприятий, для сервисов, предусматривающих установку активного сетевого, вычислительного оборудования или систем хранения данных на площадке заказчика – также должно присутствовать руководство по монтажу и установке; * руководства пользователя сервиса – руководство пользователя сервиса должно содержать в себе описание типовых задач пользователя эксплуатирующего сервис, описание типовых проблем и способов их решения, описание интерфейса системы; * ПМИ – программа и методика испытаний должна содержать в себе набор испытаний согласно технической спецификации; * Услуги по инсталляции оборудования: * определение места инсталляции оборудования в стойке; * согласование подключения к источникам питания, линиям связи, технологическим сегментам ЛВС; * инсталляция оборудования в стойки и подключения к источникам питания; * коммутация оборудования согласно физическим схемам и кабельному журналу; * Услуги по настройке систем: * установка серверного оборудования и оборудования фильтрации в необходимых точках инфраструктуры, проведение проверок связности и корректной работы всех систем совместно с представителями Заказчика, с целью исключения влияния сервисов СУИБ на существующие ИС; * настройка всех сервисов на обеспечение требуемого функционала согласно технической спецификации и актуальным возможностям информационной инфраструктуры и ЛВС Заказчика. В случае отсутствия возможности настройки требуемого функционала по причине отсутствия необходимых интеграционных мощностей на площадках Заказчика, услуги по данному пункту выполняются в срок появления возможности; * запуск задач распространения агентов (для агентских сервисов имеющих собственную систему распространения), передача дистрибутивов агентов для установки через централизованные политики AD ответственным сотрудникам службы эксплуатации Заказчика. Консультации по выбору оптимального метода распространения агентского ПО, консультация представителей Заказчика в вопросах корректных настроек сетевой инфраструктуры, инфраструктуры AD и настроек рабочих станций, для обеспечения установки ПО; * интеграция сервисов с существующими системами для обеспечения их корректной работы и получения; * интеграция сервиса ситуационного центра ИБ с существующими системами СУИБ, настройка экспорта логов и журналов событий, данных БД, настройка –api интеграции (в зависимости от сервиса); * настройка ролевой модели управления пользователями сервисов, разделение зон ответственности между сотрудниками Заказчика и Исполнителя, предоставление каждому администратору и пользователю системы только минимально необходимых прав доступа к системам, чтобы избежать получения избыточных привилегий.   **3. Разграничение зоны ответственности.**  При оказании услуг согласно настоящей технической закреплены следующие зоны ответственности Исполнителя и Заказчика, согласно Таблицы 7.  Таблица 7. Разграничение зон ответственности:   | **№** | **Параметр** | **Заказчик** | Исполнитель | | --- | --- | --- | --- | | 1.1 | Мониторинг и анализ событий ИБ (включая предоставление рекомендаций по реагированию на инциденты), зарегистрированных и касающихся элементов инфраструктуры Клиентов, входящих в Зону мониторинга. |  | + | | 1.2 | Мониторинг и анализ событий ИБ, зарегистрированных или касающихся элементов инфраструктуры Клиентов, не входящих в Зону мониторинга. | + |  | | 1.3 | Мониторинг состояния компонентов подсистемы управления событиями ИБ, установленных как на площадке Заказчика, так и на площадке Исполнителя |  | + | | 1.4 | Обеспечение корректного функционирования подсистемы управления событиями ИБ |  | + | | 1.5 | Установка агентов на источниках для отправки логов | + |  | | 1.6. | Предоставление необходимых технологических мощностей для развертывания коллекторов событий/потоков и иных инфраструктурных элементов подсистемы управления событиями ИБ в соответствии с рекомендациями Исполнителя. Поддержка отказоустойчивости и доступности соответствующей инфраструктуры |  | + | | 1.7 | Направление сетевых потоков с источников в коллекторы | + |  | | 1.8 | Реагирование на инциденты ИБ, их локализация, устранение последствий и восстановление штатного режима работы, согласно рекомендациям, предоставленным Исполнителем | + |  | | 1.9 | Обеспечение работоспособности защищенных каналов передачи информации между площадками Заказчика и Исполнителя | + | + | | 1.10 | Выполнение рекомендаций ОЦИБ и своевременное реагирование на инциденты ИБ | + |  | | 1.11 | Предоставление актуального перечня серверного, коммуникационного и компьютерного оборудования, а также информационных систем, входящих в Зону мониторинга | + |  | | 1.12 | Применение рекомендаций Исполнителя с целью исключения вероятности возникновения повторного инцидента | + |  | | 1.13 | Оперативное предоставление информации обо всех изменениях в Зоне мониторинга. | + |  | | 1.14 | Подключение источников к системе мониторинга (обеспечение сетевой связности, исполнение пунктов инструкции по подключению источников к системе мониторинга, установка агентов) | + |  | | 1.15 | Предоставление инструкций по подключению источников к системе мониторинга, проверка корректного поступления событий ИБ. |  | + | | 1.16 | Настройка политик инвентаризации | + |  | | 1.17 | Предоставление учетных записей для инвентаризации/интеграции | + |  | | 1.18 | Настройка интеграции с внешними системами |  | + | | 1.19 | Настройка архитектуры коллекторов |  | + | | 1.20 | Настройка политик назначения атрибутов | + |  | | 1.21 | Добавление пользователей | + |  | | 1.22 | Настройка уровней доступа/роли пользователей |  | + | | 1.23 | Управление с уязвимостями, рисками | + |  | | 1.24 | Настройка сценарии реагирования | + | + | | 1.25 | Управление настройками инцидентов |  | + | | Система защиты сетевого периметра | | | | | 2.1. | Установка и обновление программного обеспечения ПАК NGFW, обновление баз данных угроз и сигнатур оборудования, мониторинг работоспособности. |  | + | | 2.2 | Предоставление консультаций по электронной почте, телефону, средствам удаленного доступа по настройке, оптимизации конфигураций и правил безопасности, средств сетевого взаимодействия ПАК NGFW |  | + | | 2.3. | Организация доступа к системе и взаимодействие с соответствующими подразделениями Заказчика, предоставление серверных помещений, предоставление необходимых прав в инфраструктуре (создание учетных или иных записей). | + |  | | 2.4. | Разработка и настройка правил, политик и профилей безопасности, маршрутизации и сегментации сети, правил веб-фильтрации, VPN групп и правил доступа, правил блокировок вторжений, конфигураций сетевых и системных настроек ПАК NGFW. | + |  | | Система фильтрации почтового трафика | | | | | 3.1 | Установка и настройка ОС, а так же программного комплекса KSMG на серверах.  Обеспечение корректного функционирования системы и всех её компонентов |  | + | | 3.2 | Настройка и внедрения правил фильтрации почтового трафика |  | + | | 3.3 | Изменение правил фильтрации по инициативе заказчика |  | + | | 3.4 | Составление отчетов по событиям обнаружения системы |  | + | | 3.5 | Настройка передачи событий в SIEM систему |  | + | | 3.6 | Монтирование кабельных линий связи и настройка маршрутизации на территории заказчика для серверов платформы | + |  | | Система антивирусной защиты | | | | | 4.1 | Установка и настройка ОС, а также программного комплекса Центр администрирования системы антивирусной защиты на серверах.  Обеспечение корректного функционирования системы и всех её компонентов |  | + | | 4.2 | Настройка политик безопасности для всех типов устройств согласно best practice |  | + | | 4.3 | Внесение изменений в политики безопасности по инициативе заказчика | + |  | | 4.4 | Решение проблем, требующих локального взаимодействия с устройствами заказчика при установке или настройке антивирусного ПО. | + |  | | 4.5 | Техническая поддержка при установке или настройке антивирусного ПО на устройствах заказчика и настройке политик безопасности |  | + | | 4.6 | Установка антивирусного программного обеспечения на конечные точки | + |  | | Система сканирования на уязвимости | | | | | 5.1 | Обеспечение сетевой связанности между целевым узлом и сканнером уязвимостей | + |  | | 5.2 | Настройка целевого узла для сканирования. | + |  | | 5.3 | Сканирование целевых узлов, настройка профилей сканирования |  | + | | 5.4 | Формирование отчетности, отправка отчетов, исключение ложноположительных уязвимостей из отчетности |  | + | | 5.5 | Обработка и устранение уязвимостей найденных в процессе сканирования | + |  | | 5.6 | Поддержание работоспособности, обновление и резервное копирование системы сканирования на уязвимости |  | + | |

**Начальник Службы**

**информационной безопасности О.Жунисбеков**

Таблица 2

**Требования к потенциальному поставщику**

|  |  |  |
| --- | --- | --- |
| **№**  **п/п** | **Требование** | **Подтверждение** |
|  | Квалификационные требования, предусматривающие наличие у потенциального поставщика опыта работы в течение последних 5 (пяти) лет, на рынке закупаемых однородных работ, услуг или в определенной отрасли | - |
|  | Требования о наличии у потенциального поставщика оборудования, техники (технических устройств), зданий (сооружений), помещений с предоставлением подтверждающих документов | - |
|  | Требование о предоставлении потенциальными поставщиками образцов закупаемых товаров до даты вскрытия тендерных заявок | - |
|  | Требования к квалификации потенциальных поставщиков, определенные в ЗКС | - |
|  | Требование о предоставлении разрешения (лицензии), выданного в соответствии с законодательством Республики Казахстан о разрешениях и уведомлениях, с указанием на соответствующую(ие) лицензию(и) и иные разрешительные документы, а также виды (подвиды) деятельности, подлежащих разрешению (лицензированию) в соответствии с законодательством Республики Казахстан.  Информация об уровне ответственности объектов строительства, который определяется в соответствии с законодательством Республики Казахстан. | Потенциальный поставщик в составе заявки на участие в тендере обязан предоставить электронную копию разрешения (лицензия), выданного в соответствии с законодательством Республики Казахстан «О разрешениях и уведомлениях», либо заявление потенциального поставщика, содержащее ссылку на официальный интернет источник (веб-сайт) государственного органа, выдавшего разрешение (лицензию), использующего электронную систему разрешения (лицензирования) в формате электронного документа или электронной копии: лицензия на оказание услуг по выявлению технических каналов утечки информации и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий. |