**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 услуг по обеспечению информационной безопасности (далее - СУИБ) осуществляется оперативным центром информационной безопасности Исполнителя (ОЦИБ), осуществляющим свою деятельность на основании лицензии на оказание услуг по выявлению технических каналов утечки информации и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий в соответствии с законодательством Республики Казахстан в области информатизации.Основными целями и задачами при оказании СУИБ 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 Заказчика;
* Снижение рисков информационной безопасности (далее – ИБ) и уменьшение числа актуальных угроз;
* Повышение зрелости процессов ИБ, интеграция и централизация средств ИБ.

Создание ситуационного центра ИБ, для осуществления централизованного контроля за системами ИБ, мониторинга процессов и управления безопасностью. |
| 2 | **Требуемые функциональные, технические, качественные, эксплуатационные характеристики закупаемых товаров, работ и услуг.** |
|  | Состав СУИБВ рамках договора на закуп услуг по обеспечению информационной безопасности Исполнитель обязуется:1. обеспечить обновление и актуализацию баз данных угроз оборудования, используемого для оказания СУИБ;
2. при необходимости осуществлять интеграцию внедряемых СУИБ с существующими системами Заказчика;
3. по запросу от специалистов Заказчика вносить изменения в настройки и политику безопасности СУИБ в соответствии с утвержденными сервисными регламентами;
4. уведомлять специалистов Заказчика о выявленных уязвимостях, представляющих угрозу безопасности ИТ-инфраструктуры Заказчика;
5. предоставить специалистам Заказчика доступ к интерфейсу систем управления СУИБ для просмотра текущего состояния сервиса и отчетности, а именно к системам:
* Система защиты от таргетированных атак;
* Система выявления и предотвращения утечек данных;
* Система защиты информационного периметра и контроля доступа;
* Система фильтрации веб-трафика;
* Система фильтрации почтового трафика;
* Система защиты конечных рабочих станций;
* Система VPN;
* Клиентский портал системы управления инцидентами ИБ.
1. Предоставить специалистам Заказчика доступ к интерфейсу систем управления СУИБ для выполнения самостоятельной настройки правил и политик безопасности с обязательным уведомлением администраторов сервиса о выполненных изменениях, а именно к системам:
* Система защиты от таргетированных атак;
* Система выявления и предотвращения утечек данных;
* Система защиты информационного периметра и контроля доступа;
* Система фильтрации веб-трафика;
* Система защиты конечных рабочих станций.
1. Для оперативного реагирования и выезда на объект Заказчика в аварийных случаях, служба технической поддержки Исполнителя должна находиться в городе дислокации Заказчика.
2. Исполнитель размещает информационную систему в доступном ЦОД, с возможностью аварийного восстановления (disaster recovery) и резервного восстановления для минимизации возможных простоев мониторинга информационной безопасности.
3. Для полноценного охвата периметра региональных филиалов и ОВП (отделов вагонного парка) Заказчика, а также для обеспечения мониторинга информационной безопасности в сети Заказчика, Исполнитель обеспечивает наличие разветвленной инфраструктуры и каналов связи во всех регионах Республики Казахстан.

**Требования к оказанию СУИБ**1. СУИБ Исполнителя должны соответствовать единым требованиям, утверждённым постановлением Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области коммуникационных технологий и обеспечения информационной безопасности», а также требованиям Закона Республики Казахстан от 24 ноября 2015 года № 418-V «Об информатизации»;
2. Исполнитель при работе оперативного центра информационной безопасности должен использовать систему журналирования событий информационной безопасности с подключением к центру мониторинга «электронного правительства» Национального координационного центра информационной безопасности;
3. Предоставлять Заказчику ежеквартальный электронный отчет по оказанным СУИБ по выявлению технических каналов утечки информации и специальных технических средств оперативным центром информационной безопасности;
4. возможность самостоятельного разграничения доступа к работающим в нем информационным системам.
5. Действие лицензий на программное обеспечение входящее в состав СУИБ должны распространяться на весь период действия договора.

Требования к времени реакции и SLA услуг1. Время отклика измеряется информационной системой службы поддержки, как прошедшее с момента поступления и регистрации запроса на обслуживание (сообщение о проблеме) до момента фактического начала устранения проблемы по факту обращения. Время решения проблемы – время, прошедшее с момента фактического начала решения проблемы, описанной в заявке до закрытия заявки. Временем начала устранения проблемы считается момент отправки специалистам Заказчика уведомления о начале устранения проблемы. Временем решения проблемы считается момент отправки специалистами Заказчика сообщения, подтверждающего закрытие заявки. Подтверждение или опровержение о выполненной заявке должно быть отправлено уполномоченным специалистом Заказчика в течение 1 часа с момента поступления от уполномоченных представителей Исполнителя уведомления о выполнении заявки на обслуживание. В противоположном случае заявка считается закрытой автоматически, и временем закрытия заявки является момент отправки уведомления о завершении устранения проблемы. Уведомления о начале и завершении устранении проблемы направляются Исполнителем представителю Заказчика, по электронной почте или телефону. Время разрешения проблемы считается как разница между временем закрытия инцидента и временем, когда исполнитель был назначен.Заявки могут приниматься по следующим видам запросов:- Контактный центр.- Электронная почта.- Портал самообслуживания.**Таблица №1 Требуемые рамки SLA:**

|  |  |  |
| --- | --- | --- |
| **Наименование уровня сервиса** | **Наличие безопасного удаленного доступа** | **Отсутствие безопасного удаленного доступа** |
| **Время обращения на инцидент** | **Время закрытия инцидента** | **Время обращения на инцидент** | **Время закрытия инцидента** |
| **Критичный** | 15 минут | 1 час | 30 минут | 1-2 часа |
| **Высокий** | 30 минут | 1-2 часа | 1 час | 2,5 – 5 часов |
| **Средний** | 1 час | один день | 5 часов | От 2 до 3 дней |
| **Низкий** | один день | по согласованию | один день | по согласованию |

Исполнитель обязуется:Обеспечивать доступность и работоспособность всех сервисов с показателем доступности не менее 99,5% в год. В показателе доступности не включаются согласованные технические перерывы и связанные с этим простои услуг, недоступность услуги из-за внешних факторов (например, неисправности сетевой инфраструктуры, форс-мажорных ситуаций, отключений электричества на площадках оказания услуги, ошибок в эксплуатации системы совершенных представителями Заказчика).Услуги должны быть доступны в режиме 24/7 и функционировать в автономном режиме. Функциональные требования к оказанию СУИБТребования к сервису защиты от таргетированных атакСервис выявления и предотвращения целенаправленных атак должен обеспечивать следующий функционал:1. Поддержка следующих способов интеграции в ИТ-инфраструктуру:
* Интеграция в локальную сеть для получения и обработки зеркалированного трафика и извлечения объектов и метаинформации протоколов HTTP, FTP и DNS.
* Интеграция с прокси-сервером по протоколу ICAP для получения и обработки данных HTTP- и FTP-трафика, а также HTTPS-трафика, если настроена подмена SSL-сертификата на прокси-сервере.
* Интеграция с почтовым сервером для обработки копий сообщений электронной почты, поступающих с почтового сервера по протоколу POP3 (при наличии технической возможности на почтовом сервере).
1. Выявление аномалий и угроз на основе собранной информации.
2. Проверка данных на вирусы и другие представляющие угрозу программы с помощью антивирусных баз.
3. Анализ подозрительных исполняемых файлов и скриптов в «песочнице».
4. Поддержка «песочницей» ОС Windows.
5. Анализ .apk файлов платформы Android, на предмет наличия угроз.
6. Статистический анализ и проверка сетевой активности компьютеров на наличие признаков нетипичного поведения в сети.
7. Репутационный анализ файлов и URL-ссылок.
8. Обнаружение фишинговых и вредоносных ссылок.
9. Хранение исторических данных об инцидентах.
10. Приоритезация выявленных угроз по уровню риска.
11. Наличие графической системы управления для доступа к статистическим данным и отчетности.

*Рисунок 1. Целевая архитектура сервиса ATA*Требования к сервису выявления и предотвращения утечек данных (сервис DLP)Сервис выявления и предотвращения утечек данных должен обеспечивать следующий функционал:1. Агентский контроль на 603 рабочих станций.
2. Контроль информации, передаваемой через корпоративную почтовую систему к внешним почтовым адресам, интернет-ресурсы, средства общего доступа к файлам (POP3, MAPI (MAPI over RPC, MAPI over RPC over HTTP, MAPI over HTTP), OSCAR, XMPP (Jabber), SMTP, HTTP, HTTPS, FTP) MMP (Mail.Ru Агент), YIM.
3. Выявление утечек внутренней почты в случае получения скрытой копии писем.
4. Контроль систем обмена сообщениями (Viber, Google Hangouts и Microsoft Lync ICQ, Skype, Mail.ru Агент, XMPP).
5. Возможность создания политик фильтрации и блокирования трафика на основании атрибутов и содержимого перехватываемых данных.
6. Возможность гибкой настройки исключений из перехвата по IP-адресам (отдельным и диапазону), протоколам.
7. Настройка уведомлений пользователя рабочей станции о блокировке устройств, запуска процессов, сетевого трафика процессов и MAPI-трафика.
8. Перехват web-коммуникаций пользователей в социальных сетях Facebook, Odnoklassniki, VKontakte, Twitter. При этом должны поддерживаться: двунаправленный перехват сообщений в чатах; перехват статусов; перехват комментариев к публикациям и изображениям, перехват комментариев на форумах социальных сетей с контролем всего блока комментариев.
9. Возможность снятия снимков экрана рабочего стола пользователя с заданным интервалом, а также по событию (срабатывание правил блокировки, бездействие компьютера, нажатие клавиши PrintScreen, смена окна активного приложения либо вкладки браузера, запуск определенного приложения).
10. Автоматический поиск конфиденциальных файлов на дисках рабочей станции пользователя (по имени, по заданным атрибутам или значениям хеш-функций).
11. Запись голосового трафика Skype.
12. Возможность интеграции с Lync 2010/2013 посредством установки агентского программного обеспечения перехвата трафика на сервера.
13. Контроль использования периферийных устройств и портов на рабочих станциях.
14. Контроль сетевых соединений на рабочих станциях.
15. Теневое копирование распечатываемых и копируемых на съемные носители документов.
16. Предотвращение утечки конфиденциальных данных путем блокирования процесса передачи в случае нарушения политики безопасности.
17. Автоматическое выявление конфиденциальной информации на основе ключевых слов и фраз.
18. Распознавание конфиденциальной информации на отсканированных документах и изображениях.
19. Распознавание печатей и штампов.
20. Хранение архива всей перехваченной информации для отслеживания маршрутов движения информации не менее 9 месяцев, выявления случаев нецелевого использования корпоративных ресурсов, поиска нарушителей и формирования доказательной базы с последующей передачей архива Заказчику по окончании срока действия Договора.
21. Наличие графической системы управления для просмотра статистики перехваченных данных, выявленных инцидентов и отчетности.
22. Полнотекстовый поиск по содержимому перехваченных сообщений и вложений.
23. Поддержка русского, английского и казахского языков.
24. Мониторинг активности сотрудников в режиме реального времени.
25. Управление работой программы должно осуществляться с помощью командной строки (SSH), так и через специальный веб-интерфейс, работающий на браузерах: Google Chrome.
26. Система должна обеспечивать решение следующих задач:
* Мониторинг событий случайной или преднамеренной пересылки пользователями за пределы периметра вычислительных сетей Заказчика конфиденциальной информации по следующим каналам:
* электронная почта (протоколы POP3, SMTP, IMAP, MAPI, HTTP, в т.ч. шифрованные аналоги);
* электронная почта, переданная через почтовые веб-службы (gmail.com, mail.ru, rambler.ru, yandex.ru и т.д.).
* Двунаправленный перехват сообщений в чатах, комментариев к публикациям и на форумах социальных сетей: Facebook, Odnoklassniki, VKontakte, Twitter.
* Средства мгновенного обмена сообщениями – Skype, SIP, Viber, Microsoft Lync, ICQ, Mail.Ru Агент, Miranda, Google Hangouts, QIP Infium, PSI, Yahoo! Messenger, в т.ч. использующие шифрование.
* Запись файлов на внешние накопители.
* Запись файлов на локальные сетевые ресурсы.
* Отправка файлов в облачные сервисы хранения информации (Dropbox, OneDrive, Google Drive, Яндекс.Диск, Apple iCloud, облако Mail.Ru).
* Отправка файлов на печать на локальные и сетевые принтеры.
* Передача файлов в компьютерных сетях по протоколам FTP и FTPS.
* Мониторинг в режиме реального времени наличия или появления в файловой системе контролируемой рабочей станции конфиденциальных документов.
* Контроль использования периферийных устройств (доступ и копирование на внешние накопители, аудит подключения и доступ к внешним устройствам различного назначения).
* Запрет запуска отдельных программных приложений.
* Возможность блокирования доступа к определенным веб-ресурсам и их функционалу (на основании заданных политик безопасности).
1. В части хранения и обработки данных система должна обеспечивать:
* Возможность централизованного хранения всех собираемых системой данных в СУБД Microsoft SQL Server, Oracle, PostgreSQL, MySQL (на выбор).
* Поддержку работы с базами данных, расположенных на разных серверах.
* Возможность настройки длительности хранения информации в базе данных.
* Параллельную обработку данных, перехваченных по различным каналам передачи информации.
* Настройку максимальной скорости передачи перехваченных данных с рабочих станций модулем контроля на сервер.
* Асинхронный поиск по перехваченным данным (отображение результатов должно выполняться по мере их получения).

*Рисунок 2. Целевая архитектура сервиса DLP*Требования к сервису защиты информационного периметра и контроля доступаСервис защиты информационного периметра и контроля доступа должен обеспечивать следующий функционал:1. Контроль на 603 рабочих станций.
2. Обязательное бесперебойное обеспечение актуального состояния сигнатур и других защитных компонентов IPS в течение всего срока действия сервиса.
3. Обязательная поддержка режима работы в отказоустойчивом кластере. При выходе из строя одной из Нода кластера межсетевых экранов, при условии, что сервисы и сетевая связность доступны и работают в штатном режиме, простой оборудования не учитывается.
4. Обязательная поддержка режима работы IPS (прозрачный режим L2 без маршрутизации).
5. Обязательная поддержка режима определения приложений.
6. Поддержка политик безопасности с возможность применять политики с разделением по пользователям, группам, ip-адресам, приложениям, категориям приложений, подкатегориями, технологиям, факторам риска или характеристике.
7. Поддержка активации политик по расписанию.
8. Контроль пользователей на основе – Active Directory, LDAP, Exchange, XML-api.
9. Проточная защита от вирусов (включая вирусы встроенные в HTML, Javascript, PDF и сжатые данные), шпионского ПО, червей.
10. Поведенческое определение ботнетов, защита от Drive-by скачки.
11. Фильтрация URL на основе базы данных (для защиты периметра площадки)
12. Поддержка безопасного поиска.
13. Поддержка протоколов OSFP, RIP, 802Q, Multicast.
14. Поддержка кластеризации в режимах и Active/Passive.
15. Обязательное наличие в комплекте лицензий для развертывания централизованной системы управления межсетевыми экранами центра обработки данных (далее – ЦОД) и Интернет.
16. Работу на скорости не менее 18 Гбит/c для защиты внутренних сегментов (для каждой площадки).
17. Работу на скорости не менее 8 Гбит/c для защиты периметра площадок.
18. Наличие SSL сертификата EV (Extended Validation) от доверенного сертификационного центра.

Требования к сервису фильтрации веб-трафикаСервис фильтрации веб-трафика должен обеспечивать следующий функционал.1. Обеспечивать веб-проксирование трафика HTTP/HTTPS.
2. Иметь возможность обеспечения проточной антивирусной защиты
3. Обеспечивать следующие типы адаптации контента при его проксировании:
* Добавление, удаление или модификация HTTP заголовка.
* Блокировку запросов в зависимости от URL назначения.
* Блокировку сообщений в зависимости от контента.
* Перенаправление определенных запросов к странице или серверу.
* Ответ на определенные запросы со специальной страницей.
1. Предоставлять возможность контроля доступа в Интернет используя списки доступа со следующими поддерживаемыми критериями:
* IP адреса источника и/или отправителя.
* Доменного имени отправителя и сервера-получателя запроса.
* Регулярных выражений для проверок со стороны клиента и сервера.
* Номера автономной системы отправителя и/или сервера-получателя.
* Времени и даты, протокола или статуса HTTP запроса или используемого метода HTTP.
* Заголовков SSL сертификата пользователя.
* Имени и группы пользователя (включая доменную информацию из LDAP-совместимого сервера)
* Наличие SSL сертификата EV (Extended Validation) от доверенного сертификационного центра.

Требования к сервису фильтрации почтового трафикаСервис фильтрации почтового трафика должен обеспечивать следующий функционал.1. Сервис обеспечивает работу для на 603 рабочих станций.
2. Проверку IP-адреса отправителя на соответствие списку разрешенных адресов для домена с помощью технологии Sender Policy Framework (SPF); Поддержка технологий DKIM/DMARC.
3. Поиск и удаление в режиме реального времени всех типов вирусов, червей, троянских и других вредоносных программ в потоке входящих и исходящих почтовых сообщений, включая вложения.
4. Возможность детектирования вредоносных и фишинговых ссылок в теле письма.
5. Наличие эвристических методов детектирования.
6. Должен иметь возможность подключения репутационных облачных сервисов.
7. Проверка на наличие спама входящий поток почтовых сообщений.
8. Наличие компонента защиты, позволяющего распаковывать и анализировать составные файлы на предмет аномалий для блокировки ранее неизвестных угроз.
9. Контентная фильтрация почтовых сообщений по имени, типу и размеру вложений.
10. Интеграция со службами каталогов Active Directory и Open LDAP.
11. Возможность отправления ловушек и уведомлений по протоколу SNMP.
12. Возможность работы по протоколу IPv6.
13. Фильтрация или исключение из фильтрации сообщения по адресу отправителя письма (e-mail и/или IP-адрес) на основе собственных «черных» и «белых» списков.
14. Проверка наличия IP-адреса отправителя в списках DNS-based realtime blackhole list (DNSBL).
15. Проверка с помощью сервиса SPAM URI Realtime Blocklists (SURBL) адресов и ссылок на сайты, присутствующих в теле письма.
16. Проверка графических вложений на совпадение с известными сигнатурами спам-сообщений.
17. Перенос в карантинный каталог зараженных, подозрительных и поврежденных объектов почтового трафика, определять защищенные паролем файлы.
18. Наличие общего и персонального карантина.
19. Возможность создания персональных черного и белого списков.
20. Осуществление по запросу антивирусной проверки объектов.
21. Обработка почтового трафика в соответствии с правилами, заданными для групп отправителей и получателей.
22. Организация дополнительной фильтрации почтового потока сообщений по именам и типам вложенных файлов и применение к отфильтрованным сообщениям отдельных правил обработки.
23. Использование регулярных выражений при создании правил фильтрации.
24. Возможность уведомления отправителя, получателя и администратора сервера о почтовом сообщении, содержащем заражённые и подозрительные объекты.
25. Управление работой программы должно осуществляться с помощью командной строки (SSH), так и через специальный веб-интерфейс, работающий на браузерах: Internet Explorer, Mozilla Firefox, Google Chrome.
26. Возможность выявления и удаления 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.

Требования к сервису контроля конечных рабочих станций (Endpoint Protection)Сервис контроля конечных рабочих станций должен поддерживать следующий функционал:1. Агентский контроль на 603 рабочих станций.
2. Агентский контроль на рабочих станциях структурных подразделений Заказчика и его филиалов.
3. Резидентный антивирусный мониторинг.
4. Эвристический анализатор, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы.
5. Антивирусное сканирование по команде пользователя или администратора и по расписанию.
6. Запуск задач по расписанию и/или сразу после загрузки операционной системы.
7. Антивирусная проверка и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB.
8. Защита электронной корреспонденции от вредоносных программ с проверкой входящего и исходящего трафика на следующих протоколах: IMAP, SMTP, POP3 независимо от используемого почтового клиента.
9. Защита веб-трафика — проверка объектов, поступающих на компьютер пользователя по протоколам HTTP, FTP, в том числе с помощью эвристического анализа.
10. Распознавание и блокировка фишинг-сайтов.
11. Защита от сетевых атак и сетевых аномалий.
12. Проверка трафика ICQ и MSN для обеспечения безопасности работы с интернет-пейджерами.
13. Защита от еще не известных вредоносных программ на основе анализа их поведения.
14. Поддержка работы с локальными репутационными сервисами.
15. Возможность ограничения привилегий исполняемых программ, таких как запись в реестр, доступ к файлам и папкам. Автоматическое определение уровней ограничения на основании репутации программы.
16. Наличие компонента, дающего возможность создания специальных правил, запрещающих установку и/или запуск программ. Компонент должен контролировать приложения как по пути нахождения программы, метаданным, контрольной сумме MD5.
17. Осуществление контроля работы пользователя с внешними устройствами ввода/вывода по типу устройства.
18. Наличие функционала шифрование съемных носителей, файлов, папок или дисков.
19. Ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось.
20. Запуск специальной задачи для обнаружения уязвимостей в приложениях, установленных на компьютере.
21. Защита от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля, позволяющая избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей.
22. Возможность установки только выбранных компонентов программного средства антивирусной защиты.
23. Централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления.
24. C возможностью настройки доверенных сайтов.
25. Блокировка баннеров и всплывающих окон загружаемых с Web-страниц.
26. Гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства.
27. Возможность определения аномального поведения приложения с помощью анализа последовательности действий этого приложения. Возможность совершить откат действий вредоносного программного обеспечения при лечении.
28. Осуществление контроля работы пользователя с сетью Интернет, в том числе явный запрет или разрешение доступа к ресурсам определенного характера, а также возможность блокировки определенного типа информации (аудио, видео и др.).
29. Программное средство должно позволять вводить временные интервалы контроля, а также назначать его только определенным пользователям из Active Directory.
30. Возможность задания правил для компонента запрета запуска приложений на базе заранее заданных категорий приложений, предоставляемых производителем программного обеспечения, а также для определенных пользователей из Active Directory.
31. Возможность задания правил для компонента контроля работы с внешними устройствами по используемой шине, с возможностью создания списка доверенных устройств по их идентификатору и возможностью предоставления привилегий для использования внешних устройств определенным пользователям из Active Directory.
32. Позволять осуществлять шифрование данных на внешних устройствах хранения информации.
33. Управление лицензиями, учет оборудования и ПО - сводные отчеты об аппаратном и программном обеспечении.

Требования к сервису VPN (Virtual Private Network) удаленный доступ к сети1. Remote Access VPN Используют для создания защищённого канала между сегментом корпоративной сети (центральным офисом или филиалом) и одиночным пользователем, который, работая дома, подключается к корпоративным ресурсам с домашнего компьютера, корпоративного [ноутбука](https://ru.wikipedia.org/wiki/%D0%9D%D0%BE%D1%83%D1%82%D0%B1%D1%83%D0%BA), [смартфона](https://ru.wikipedia.org/wiki/%D0%A1%D0%BC%D0%B0%D1%80%D1%82%D1%84%D0%BE%D0%BD).
2. Установление защищенного туннеля IPSEC или SSL VPN и обеспечение конфиденциальности передаваемых данных и доступа к внутренним приложениям компании.
3. Возможность настройки Заказчиком авторизации пользователя в домене компании по паролю и второму фактору (сертификат по SCEP, смс, звонок ОКТА, DUO, Ubikey, RSA, и т.д.) и обеспечение минимизации риска кражи пароля. Осуществление консультаций Исполнителем по настройке авторизации пользователя в домене компании по паролю и второму фактору.
4. Защита от утечки конфиденциальных данных пользователя на фишинговых сайтах.
5. Активная проверка, что на хосте установлены последние патчи, запущен и обновлен антивирус, стоит персональный firewall и зашифрованы диски и отправка рекомендаций что нужно делать, чтобы исправить ошибки (HIP notification).
6. Интеграция с NGFW: антивирус, IPS, URL фильтрация, Threat intelligence, защита DNS и других приложений, контроля страны подключения по VPN.
7. Разграничение доступа пользователей к только нужным им приложениям, контроль доступа к файлообменникам и веб-почте и другим ресурсам SaaS.
8. Возможность выгрузки отчета по всем подключениям VPN клиентов (время подключения и отключения статистика трафика и т.д.).
9. Наличие SSL сертификата EV (Extended Validation) от доверенного сертификационного центра.

Требования к сервису ситуационного центра (SoC) ИБСервис ситуационного центра должен поддерживать следующие функции:1. круглосуточный мониторинг событий ИБ, зафиксированных системами мониторинга и управления событиями информационной безопасности и системами защиты внешнего периметра для информационных систем и ресурсов, подключенных к SIEM-системе Исполнителя;
2. круглосуточный мониторинг событий ИБ, зафиксированных на серверном оборудовании и сетевых устройствах Заказчика, подключенных к SIEM-системе Исполнителя (далее – Зона мониторинга);
3. выявление инцидентов ИБ, произошедших в Зоне мониторинга;
4. направление Заказчику информации о выявленных инцидентах и методах реагирования на них и предоставления рекомендаций по их устранению;
5. предоставление экспертной поддержки в процессе реагирования на инциденты;
6. обнаружение, регистрация и уведомление об инцидентах, поступающих с внешней сети Интернет на периметр заказчика, посредством регистрации в системе управления инцидентами, клиентского портала регистрации инцидентов, направления почтового сообщения;
7. осуществление консультаций при проведении расследования критичных инцидентов ИБ
8. сервис осуществляет работу для 603 рабочих станций;
9. поддержку стандартных методов сбора журналов событий (например, syslog, WMI, JDBC, SNMP, Checkpoint LEA, и пр.);
10. поддержку сбора информации с серверов и рабочих станций под управлением ОС Microsoft, Linux/Unix и др.;
11. поддержку сбора информации с баз данных класса предприятия, таких как Oracle, MySQL;
12. поддержку сбора информации с коммерческих приложений (т.e. SAP, Web, и др.);
13. поддержку сбора информации с LDAP;
14. поддержку сбора информации по flow протоколам (т.e. Netflow, J-Flow, S-Flow);
15. поддержку доступа к информации об инцидентах на протяжении длительного настраиваемого периода времени для дальнейших расследований;
16. пользователь должен иметь возможность присваивать событиям любые имена;
17. сервис должен иметь возможность хранить информацию о событиях, как в исходном виде, так и в нормализованном виде для использования в дальнейших расследованиях;
18. сервис должен иметь возможность обрабатывать и нормализировать данные из полей, которые не поддерживаются изначально;
19. система должна обеспечивать анализ событий в режиме реального времени;
20. сервис должен предоставлять возможность собирать и анализировать события по предустановленным пользователем фильтрам;
21. сервис должен предоставлять возможность получения дополнительной информации о событиях при необходимости (drill down);
22. сервис должен давать возможность самостоятельной настройки отчетности и создания собственных отчетов пользователем в системе управления инцидентами ИБ;
23. сервис должен иметь возможность планирования генерации отчетов в определенный период времени;
24. сервис должен предоставлять отчеты за определенный период времени по различным сегментам и системам в сети;
25. сервис должен обеспечивать оповещения на основе обнаруженных аномалий и поведенческого анализа и изменений путем реализации сценариев в системе мониторинга и корреляции событий;
26. возможность проведения сканирования сети как по расписанию, так и по требованию;
27. возможность как агентского, так и безагентского сбора информации о защищённости систем;
28. сервис должен предоставлять информацию о перечне уязвимых систем или сервисов, названии уязвимости, уровне критичности уязвимости, статусе уязвимости (новая/активная/устранена);
29. возможность доступа к базе знаний, с описанием уязвимостей, а также с рекомендациями по их устранению;
30. наличие подписки на регулярное обновление базы уязвимостей;
31. возможность маркировки уязвимости (в случае ложного срабатывания);
32. сервис должен предоставлять аналитику по обнаруженным уязвимостям и средства для приоритезации устранения уязвимостей;
33. возможность формирований отчетов как по расписанию, так и по требованию;
34. возможность проведения сканирования на соответствие требованиям как по расписанию, так и по требованию
35. возможность создание политик соответствия как с нуля, так и на основании просканированного устройства;
36. должно осуществляться сканирование сетей, выявление оборудования и сбор данных с целью обеспечения учета активов и контроля состояния и состава ИТ-инфраструктуры;
37. должна обеспечиваться возможность группировки выявленного оборудования, в том числе возможность автоматического включения в группы ИТ-активов по настроенным правилам. В качестве критериев включения могут использоваться следующие параметры: территориальное подразделение, найденное ПО на данном оборудовании, город, домен, рабочая группа, пользователи данного оборудования, помещение, к которому прикреплено данное оборудование, тег, тип оборудования;
38. должна обеспечиваться возможность учета материальных и нематериальных активов, и их взаимосвязей (процессы, информация, системы, сети, оборудование, пользователи и пр.);
39. должна обеспечиваться возможность отправки уведомлений об изменениях в активах (нахождение нового оборудования, нового ПО или пользователя, новых уязвимостей, новых сетей, устранения уязвимостей, в случае если закончились инвентарные номера для присвоения оборудованию). При этом для уведомлений должна обеспечиваться возможность их автоматической настройки;
40. должна быть встроена возможность визуализации сетевой инфраструктуры в формате географического расположения, сетевых схем, схем физического размещения оборудования в помещениях;
41. должна быть встроена возможность визуализации связей между различными элементами базы данных активов (ресурсно-сервисная модель), например, связь бизнес-процессов с информацией или с группами ИТ-активов;
42. сервис должен интегрироваться с системами-поставщиками информации (инвентаризационной информации, информации об уязвимостях, о событиях безопасности, информации об инцидентах и проч.):
* служба каталогов Active Directory (получение сведений о пользователях);
* система обмена почтовыми сообщениями (автоматическое создание инцидентов и отправка уведомлений заинтересованным пользователям);
1. должно обеспечиваться управление инцидентами ИБ, в том числе централизованный сбор, регистрацию и учет данных по инцидентам, проведение разбирательств и оценку уровня ущерба от реализации инцидентов ИБ;
2. должна обеспечиваться возможность автоматической привязки инцидентов к бизнес-процессам, информации и группам ИТ-активов на основании связей этих активов между собой;
3. должна обеспечиваться возможность организации совместной работы различных групп специалистов и экспертов, участвующих в расследовании инцидентов, а также возможность хранения всей информации в единой базе данных;
4. должно осуществляться моделирование угроз и управление рисками информационной безопасности в соответствии с требованиями и рекомендациями национальных и международных стандартов;
5. должна быть возможность определения ценности активов, входящих в область оценки рисков;
6. должна быть возможность проведения оценки рисков информационной безопасности для различных типов активов, а также для отдельных проектов (информационные активы, группы ИТ-активов, бизнес-процессы и пр.);
7. должно быть предусмотрено составление плана обработки рисков на определенный период и его сопоставление с имеющимся бюджетом на информационную безопасность;
8. наличие гибкой и настраиваемой схемы оценки рисков, которая может быть адаптирована под конкретную модель, используемую в организации. Должна быть возможность задавать математический алгоритм оценки;
9. должна предоставляться оценка выполнения законодательных и корпоративных требований по информационной безопасности, а также контроль общего состояния информационной безопасности на всех объектах Заказчика;
10. должна обеспечиваться возможность визуального представления информации по инцидентам, уязвимостям, активам, рискам, выполнению требований информационной безопасности (аудитам), по контролю за состоянием безопасности, а также создания сравнительных графиков по защищаемым объектам в клиентском портале системы управления инцидентами;
11. должно осуществляться учет всех мероприятий по информационной безопасности, нормативных документов, замечаний, проводимых аудитов безопасности;
12. должно осуществляться управление задачами ИБ-подразделения и обеспечение совместной работы различных групп специалистов (ответственных за информационную безопасность на объектах, владельцев активов, аудиторов, контроллеров, руководителей по информационной безопасности);
13. должен формироваться пакет отчетных документов по состоянию системы информационной безопасности, выявленным инцидентам ИБ, реализованным мероприятиям, а также по результатам проводимых оценок рисков и аудитов ИБ;
14. в системе должен быть предусмотрен механизм конструктора отчетов;
15. все отчетные документы должны иметь возможность выгружаться из интерфейса в форматах \*.docx, \*.xlsx или \*.pdf.
16. должна обеспечиваться возможность настройки панелей, содержащих различные графики, настраиваемые пользователем, и отражающие статистическую информацию и динамику основных показателей из разных функциональных модулей;
17. должна обеспечиваться возможность разграничения доступа к определенным функциональным компонентам в соответствии с ролями, определенными в системе. Должна также обеспечиваться возможность дополнительно ограничить доступ к заданным полям в инцидентах информационной безопасности участникам рабочей группы;
18. должен быть предоставлен интерфейс взаимодействия со службой поддержки через интерфейс Сервис-деска;
19. обеспечение контроля и защиты периметра корпоративной сети от вторжений и широковещательных атак;
20. обеспечение контроля внутренних ресурсов Заказчика для выявления и предотвращения целенаправленных атак, при наличии подключения данных ресурсов к сервису защиты от таргетированных атак и сервису ситуационного центра ИБ;
21. Исполнитель предоставляет консультационную помощь, рекомендации и инструкции по подключению (новых) источников Заказчика, а также несет ответственность за корректность информации по настройки и конфигурации агентов;
22. Исполнитель инвентаризирует в системе мониторинга добавленные Заказчиком указанные согласно Приложения 3 настоящей технической спецификации, а также новые источники к системе мониторинга и проверяет корректность получаемых данных;
23. 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.
24. Исполнитель предоставляет рекомендации и инструкции по подключению (новых) источников Заказчика;
25. проведение внешних тестов на проникновение (1 раз в год, не более 3 сетей класса C - 614 IP адресов, не более 10 веб-приложений собственной разработки на внешнем периметре), 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 перепроверкой устранения выявленных уязвимостей;
26. Экспертиза по расследованию наиболее критичных инцидентов (проведение мероприятий по реагированию на площадке заказчика, сбору и исследованию образов жестких дисков, анализ вредоносного ПО, оказания помощи в устранении последствий инцидентов.

**Требования к отчетным документам** В течение 30 рабочих дней после заключения Договора, Исполнитель и Заказчик согласовывают регламент взаимодействия, а также форму ежеквартального сводного отчета, с текстовой, табличной и графической (диаграммы, графики) информацией по ключевым показателям исполнения Договора, в том числе:* 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.
1. 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.
2. Ежеквартально и по запросу Заказчика, но не чаще одного раза в месяц, предоставлять Заказчику сводный отчет и актуальные контактные данные специалистов, ответственных за оказание СУИБ.

Исполнитель при предоставлении СУИБ руководствуется Требованиями СТ РК ISO/IEC 27001-2015 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности». |
| **3** | **Гарантийные сроки (при необходимости)** |
|  | Не требуется |