**Технические требования к GFI unlimited.**

Оглавление

[Общие требования 2](#_Toc374973227)

[Программный межсетевой экран с веб-фильром 2](#_Toc374973228)

Сканер безопасности сети и централизованное управление обновлениями……… ..3

Почтовый сервер………………………………………………………………………....4

Защита почтового сервера Microsoft Exchange…………………...……………………5 Прозрачный веб-прокси сервер…………………………………………………………5

Архиватор для почтового сервера………………………………………………………6

Антиспам и антивирус для почтового сервера………………………………………...6

Система контроля пользователей……………………………………………………….7

Корпоративная платформа для централизованного управления сетевой безопасностью и ИТ……………………………………………………………………..7

Мониторинг событий безопасности……………………………………………………8

VoIP АТС…………………………………………………………………………………8

Факс-сервер………………………………………………………………………………9

Help Desk…………………………………………………………………………………9

# Общие требования

Данная подписка должна включать в себя следующие продукты:

* Межсетевой экран с веб-фильтром;
* Сканер безопасности сети и централизованное управление обновлениями;
* Почтовый сервер;
* Защита почтового сервера Microsoft Exchange;
* Прозрачный веб-прокси сервер;
* Архиватор для почтового сервера;
* Антиспам и антивирус для почтового сервера;
* Система контроля пользователей;
* Корпоративная платформа для централизованного управления сетевой безопасностью и ИТ;
* Мониторинг событий безопасности;
* VoIP АТС;
* Факс-сервер;
* Help Desk.

Межсетевой экран с веб-фильтром

Программный межсетевой экран (далее - ПМЭ) должен обладать достаточным функционалом по осуществлению контроля доступа пользователей ЛВС к ресурсам сети Интернет, в том числе осуществлять возможность идентификации пользователей по уникальным парам «имя пользователя\пароль», хранящимся как в локальной пользовательской базе ПМЭ, так и в базе LDAP Active Directory\Apple Open Directory, а также должен включать в себя следующие модули:

- Модуль обнаружения и предотвращения вторжений (IDS\IPS);

- Модуль антивирусной фильтрации;

- Модуль управления полосой доступа к сети Интернет;

- Модуль непрозрачного прокси-сервера;

- Модуль организации защищённых соединений с

удалёнными пользователями и\или ЛВС (VPN);

- Модуль обнаружения и предотвращения пиринговых соединений (p2p);

- Модуль обнаружения и предотвращения атак с подменой

IP адресов(spoofing);

- Модуль фильтрации MAC адресов;

- Модуль пакетной фильтрации с осуществлением отслеживания

пакетов (SPI);

- Модуль фильтрации Web протоколов на основании

пользовательского списка правил;

- Модуль контентной Web фильтрации;

- Модуль фильтрации запрещённых слов

- Модуль фильтрации FTP протокола

- Модуль DHCP;

- Модуль сбора статистики доступа пользователей к Интернет-ресурсам;

- Модуль переадресации DNS;

- Поддержка входящих и исходящих подключений по протоколу IPv6;

- Возможность интеграции системы управления ПМЭ в единую систему управления компании, выполненную на основе WEB приложений.

В том числе ПМЭ должен обладать возможностью работы с двумя линиями доступа к сети Интернет в режиме обработки отказа (failover) и в режиме распределения нагрузки трафика между каналами (network load balancing); при этом в режиме распределения нагрузки ПМЭ должен поддерживать работу от 2 и более линий доступа к сети Интернет.

Сканер безопасности сети и централизованное управление обновлениями

Сканер безопасности сети и централизованное управление обновлениями должен обладать достаточным функционалом по обнаружению уязвимостей на компьютерах и мобильных устройствах. Должен включать в себя следующие функции:

- Поиск уязвимостей и их исправление;

- Сканер портов;

- Аудит конечных узлов;

- Отчетность;

- Контроль установленного ПО.

Поиск уязвимостей и их исправление

Данная функция должна уметь обнаружить, определить и исправить уязвимости в сети. Данные об уязвимостях должны обновляться постоянно. Поставщиками информации об угрозах могут быть сами производители ПО или зарекомендовавшие себя списки SANS и OVAL. Данный продукт должен уметь закрывать порты, исправлять ключи реестра, устанавливать патчи и обновлять ПО, удалять запрещенные программы и устанавливать недостающие.

Сканер уязвимости должен поддерживать (Определять устройства, сканировать порты, проводить оценку уязвимостей, управлять обновлениями, проводить аудит ПО и HW) следующие ОС: Windows Server 2012R2, Windows Server 2012 Standard, Windows Server 2008 Standard/Enterprise (также R2), Windows Server 2003 Standard/Enterprise, Microsoft Small Business Server 2011, Microsoft Small Business Server 2008, Microsoft Small Business Server 2003 (SP1), Windows 2000 Server, Windows 8.1, Windows 8 Professional/Enterprise/Ultimate/ Home Premium, Windows Vista Business/Enterprise/Ultimate/Home, Windows 7 Professional/ Enterprise/Ultimate/Home Premium, Windows XP Professional (SP2 и выше), Windows 2000 Professional (SP4), Red Hat Enterprise Linux 5 и выше, Mac OS X 10.5 и выше, CentOS 5 и выше, Ubuntu 10.04 и выше, Debian 6 и выше, SUSE Linux Enterprise 11 и выше, Fedora 19 и выше и другие дистрибутивы.

Поддержка виртуальных сред (Определять устройства, сканировать порты, проводить оценку уязвимостей, управлять обновлениями, проводить аудит ПО и HW) таких как: VMware, Microsoft Hyper-V, Microsoft Virtual PC, Oracle VirtualBox, Citrix Xen, Parallels.

Поддержка мобильных устройств (Определять устройства, сканировать порты, проводить оценку уязвимостей): Google Android, Apple iOS, Windows Phone.

## Почтовый сервер

Почтовая система или почтовый сервер (далее - ПС) должна обладать достаточным функционалом по осуществлению взаимодействия пользователей посредством электронной почты, календарей, заметок и задач, в том числе осуществлять возможность идентификации пользователей по уникальным парам «имя пользователя\пароль», хранящимся как в локальной пользовательской базе ПС, так и в базе LDAP Active Directory\Apple Open Directory, а также должна включать в себя следующие модули:

- Модуль безопасности

- Модуль антиспама

- Модуль антивирусной фильтрации

- Модуль резервного копирования

- Модуль архивации почтовых сообщений

- Веб-клиент

- Модуль синхронизации

- Модуль обмена мгновенными сообщениями

- Модуль взаимодействия пользователей

- Модуль администрирования продукта

В том числе ПС должна обладать возможностью установки на любую из операционных систем (Windows, Linux и Mac) без различий в функционале и виртуальную машину (VMware, Parallels или Hyper-V); возможностью интеграции системы управления ПС в единую систему управления компании, выполненную на основе WEB приложений; возможностью синхронизации сервера с любым мобильным устройством на базе мобильных операционных систем Apple, Android, Windows Phone, PalmOS, Blackberry 10 и любым почтовым клиентом, использующим стандартные почтовые протоколы POP3, IMAP и SMTP (MS Outlook, Mozilla, Windows 8 mail, Apple mail, the Bat! и т.д.).

Защита почтового сервера Microsoft Exchange

Защита почтового сервера Microsoft Exchange должна обладать следующими функциями:

- Защита от спама и вирусов. Каждое письмо детально проверяется: отправитель и сервер отправителя, служебные заголовки, цифровая подпись, сигнатуры, встроенные изображения и сценарии, прикрепленные файлы, репутация.

- Архивация писем. Система должна архивировать все ваши письма. Письма должны хранится в неизменном виде так, чтобы после восстановления могли использоваться для внутренних расследований.

- Непрерывность работы. В случае аварии на почтовом сервере или внеплановых работ, сотрудники должны продолжать получать и работать с письмами, а также сохранять доступ до календарей и контактов через веб-интерфейс.

Система должна поддерживать установку на следующие операционные системы 64 битной архитектуры: Windows Server 2008 R2 и выше. Поддерживать защиту следующих серверов Microsoft Exchange: Microsoft Exchange Server 2010/2013/2016.

Прозрачный веб-прокси сервер

Прозрачный веб-прокси сервер должен обладать следующими функциями:

- Контроль доступа до веб-сайтов. С постоянно обновляемой базой из более 460.000.000 прокатегоризированных веб-сайтов и 740.000.000 IP адресов, включая анонимные веб-прокси и сайты, подвергшиеся взлому.

- Контроль приложений. Прозрачный веб-прокси сервер должен знать более 1000 приложений, которые в своей работе используют доступ в веб: мессенджеры, клиенты социальных сетей, медиа-плееры, утилиты Dropbox, Яндекс.Диск, Google Drive и др. Уметь запрещать отдельному приложению или целой группе приложени веб-доступ до своих серверов, иметь базы данных которые постоянно обновляется.

- Защита от вредоносных файлов. Все загружаемые файлы должны проходить проверку двумя антивирусным ядрами: BitDefender и Касперский.

- Расшифровка HTTPS. Прозрачный веб-прокси сервер должен уметь расшифровывать трафик, передаваемый по защищенному протоколу HTTPS.

- Репутационный фильтр. Прозрачный веб-прокси сервер должен уметь фильтровать доступ до веб-сайтов, основываясь на данных о его репутации.

- Защита от неизвестных угроз. Прозрачный веб-прокси сервер должен уметь проводить анализ поведения программ, который позволяет выявлять вредоносные программы, которые еще не известны антивирусам. Загруженный файл должен проверятся в защищенном окружении, включая файлы внутри архивов. Прозрачный веб-прокси сервер должен устанавливаться на следующие операционные системы 64 битной архитектуры: Windows Server 2016, Windows Server 2012 R2, Windows Server 2008 R2, Windows SBS 2011, Windows SBS 2008, Windows 10, Windows8/8.1, Windows 7, Windows Vista SP2.

Архиватор для почтового сервера

Архиватор для почтового сервера должен уметь сжимать файлы до 80% и обладать следующими функциями:

- Архивация документов сотрудников. Архиватор для почтового сервера должен уметь сохранять отдельные файлы и документы с компьютеров пользователей. Также включать общие папки для обмена документами между сотрудниками (аналогично Dropbox, Google Drive и Яндекс.диск, но без публикации файлов в интернет), все версии документов должны сохранятся автоматически с возможностью откатиться на любую из них даже в случае удаления документа.

- Подробный анализ писем. Архиватор должен уметь проводить анализ содержимого писем: находить ненормативную лексику, разделять сотрудников на группы общения, подсчитать скорость реакции сотрудника на письмо, пустующие ящики, выявить утечку информации, по ключевым словам, и шаблонам (номера кредитных карт, документов). Создавать отчеты как по запросу при проведении расследования, так и по расписанию. Архиватор для почтового сервера должен устанавливаться на следующие операционные системы 64 битной архитектуры: Windows Server 2016, Windows Server 2012 R2, Windows Server 2008 R2, Windows SBS 2011. Поддерживать следующие почтовые сервера: Microsoft Exchange 2010,2013,2016, Office 365, Kerio Connect, Google Apps for Business, и другие почтовые сервера поддерживающие протокол IMAP(с функцией journaling-like).

Антиспам и антивирус для почтового сервера

Антиспам и антивирус для почтового сервера должен поддерживать установку на следующие почтовые сервера: Exchange, Lotus Domino, MDaemon и другие почтовые сервера, поддерживающие работу через SMTP-relay. Иметь не менее 14 уровней фильтрации почты. Иметь не менее 5 антивирусных ядер. Также должен обладать следующими функциями:

- Поиск ключевым словам;

- Защита от неизвестных угроз.

- Централизованный карантин

- Фильтрация приложенных файлов

- Серые списки

- Защита от сбора адресов

- Автоматические белые списки

- Обнаружение исходящих рассылок

- Единая панель управления

- Персональный карантин

.

Система контроля пользователей

Система контроля за пользователями должна уметь распределять уровни доступа через свой интерфейс или напрямую через Active Directory. Уметь автоматически устанавливать агенты на компьютеры. Также система должна обладать следующими функциями:

- Защита от утечки данных. Уметь анализировать устройства в сети и показывает комплексную информацию по всем компьютерам, указывая на уровни риска утечки данных, предлагать советы по улучшению защиты и контролировать доступ сотрудников до внешних устройств.

- Контентный анализ. Система должна уметь делать контентный анализ передаваемых файлов: по ключевым словам, или регулярным выражениям.

- Шифрование данных. При записи на внешнее устройства файлы должны шифроваться с помощью надежного алгоритма AES с длиной ключа 256 или 128 бит.

- Иметь подробную отчетность. Отчеты должны содержать полную информацию о действии пользователей: кто, когда, куда, какой файл пытался переместить, было ли это разрешено. Какой реальный тип файла был (в случае подмены расширения).

Корпоративная платформа для централизованного управления сетевой безопасностью и ИТ

Корпоративная платформа для централизованного управления сетевой безопасностью и ИТ должна обладать следующими функциями:

- Корпоративный антивирус;

- Управление обновлениями и патчами;

- Инвентаризация и аудит;

- Контроль подключаемых устройств.

Корпоративная платформа для централизованного управления сетевой безопасностью и ИТ должна поддерживать установку на следующие операционные системы 64 битной архитектуры: Windows Server 2016, Windows Server 2012 R2, Windows Server 2008 R2, Windows SBS 2011, Windows SBS 2008, Windows 10, Windows 7.

Система мониторинга событий безопасности

SIEM система должна включать в себя следующие функции:

- Подключение всех источников событий. Таких как; Windows Events, W3C logs, SNMP, Syslog, XML, CSV, TXT.

- Обработка событий;

- Мониторинг в реальном времени;

- Аудит приложений и узлов в сети.

Иметь предустановленные правила для мониторинга и аудита программного и аппаратного обеспечения следующих вендоров: Microsoft Exchange, MS SQL, Oracle, Cisco и других. И также должна быть возможность добавлять свои правила и корректировать предустановленные.

- Уметь оповещать об опасном тренде до того, как проблема станет причиной остановки бизнеса, по электронной почте или SMS.

SIEM система должна поддерживать следующие операционные системы: Windows Server 2016, Windows Server 2012 R2, Windows Server 2008 R2, Windows SBS 2011, Windows SBS 2008, Windows 10, Windows8/8.1, Windows 7, Windows Vista SP1.

VoIP АТС

Голосовой телефонный шлюз должен иметь свое мобильное приложение для следующих мобильных платформ: Apple iOS, Android. Также VoIP АТС должен иметь свое приложение для компьютера на базе операционных систем MacOS 10.10 и выше, Windows 7 и выше(64 bit), Debian 8, Ubuntu 16.04. Эти приложения должны уметь выполнять и принимать звонки с данной VoIP АТС. VoIP АТС должна предоставлять следующие функции:

- маршрутизация вызовов;

- автосекретарь с голосовым меню;

- голосовые и видеовызовы с автоответчиком;

- настройка добавочных номеров;

- иметь встроенную защиту;

- мобильных приложений на Apple iOS;

- поддержка подключений по протоколу SIP;

- поддержка e1 и FXO подключений.

Также VoIP АТС должна поддерживать виртуальное решение на VMware Hypervisor (VMware Workstation 9 or 10, VMware Player/Player Plus 5 or 6, VMware ESXi 5.1 or 5.5). VoIP АТС должна поддерживать подключение телефонов следующих производителей: Cisco, Linksys, Grandstream, Htek, Mitel/Aastra, Polycom, Snom, Ubiquiti UniFi, Yealink/Well.

Факс-сервер

Факс-сервер должен поддерживать интеграцию с существующей VoIP АТС, также иметь поддержки протокола T.38. Факс-сервер должен поддерживать следующие функции:

- Передачу факсов через VoIP-шлюзы, а также с использованием факс-плат и модемов;

- Распознавание текстов с поддержкой более 100 языков, включая русский, уметь превращать входящие факсы в редактируемые документы, перенаправлять их отдельным сотрудникам, по ключевым словам, а также фильтровать спам;

- Маршрутизация входящих сообщений, по ключевым словам, в распознанном тексте, дополнительному номеру, номеру отправителя, линии, которая использовалась для получения;

- Отчетность по спискам отправленных и полученных факсов, статистикам по сотрудников, отфильтрованным сообщениям.

Система заявок Help Desk

Защита почтового сервера Microsoft Exchange должна обладать следующими функциями:

Приём заявок по средствам:

- почты

- веб сервиса

- чата

-мобильного клиента;

Выставление оценок агентам.

Установка приоритетов и типов.

Возможность установки SLA, переназначение и отслеживание выполнения задач со стороны заказчика и исполнителя.

- Отчетность по агентам, по заказчикам, срокам, SLA, рейтенгу.