«Chronopay AntiVirus»

Содержание

3. Общие положения

Этот документ содержит в себе несколько глав, необходимых для того, чтобы обозначить некоторые предположения по проекту создания антивирусного программного обеспечения компанией Chronopay, а так же некое общее техническое задание на антивирусное программное обеспечение.

В этой главе будут рассмотрены такие немаловажные пункты касающиеся будущего продукта как, схема продаж, политика лицензирования, партнёрская программа, общее видение функционала с точки зрения продаж.

4. Схема продаж

Что касается схемы продаж, прежде всего, необходимо обозначить термины, -

Вендор (от англ. Vendor) – производитель продукта (производитель программного обеспечения, в нашем случае это компания Chronopay)

Дистрибьютор (Distributor) – компания, осуществляющая закупку продуктов у компании производителя и перепродающая продукты компаниям реселлерам или дилерам.

Реселлер/Дилер – компания, продающая продукты компании производителя в розницу (конечным пользователям).

Конечный пользователь (EndUser) – физическое или юридическое лицо, покупающее продукт компании производителя для собственного использования (не для перепродажи).

Таким образом, - типичная схема продаж программного обеспечения выглядит так –

Иногда вендоры отходят от такой схемы, выключая из цепочки дистрибьютора, путём получения партнёром (реселлером) специального статуса (например, Direct Partner) позволяющего покупать продукты напрямую у вендора. Или Вендор просто не видит необходимости в дистрибьюторе и продаёт напрямую своим партнёрам – компаниям реселлерам.

В нашем случае предлагается использовать типичную, классическую схему, так как она может дать больший результат за счёт продвижения продукта самими дистрибьюторами, а так же за счёт возможности заработать на продаже большему количеству участников процесса продажи.

5. Обзор функционала

Предполагаемые функциональные особенности будущего продукта будут детальнее описаны в следующей главе. В этой главе речь пойдёт о функционале в общих чертах и больше с точки зрения продажи и продвижения продукта.

В последнее время среди производителей продуктов (вендоров) на рынке информационной безопасности образовалась тенденция к расширению сферы влиянтия. Это происходит как за счёт расширения продуктовой линейки, так и за счёт расширения функционала конкретного продукта.

Что имеется ввиду? К примеру,- компания McAfee начинала с того, что производила только антивирус для конечного пользователя, теперь же в портфеле вендора имеются продукты для крупных организаций, как антивирусные решения (вышедшие из когда то EndUser продукта – из их первого антивируса), так и решения по защите периметра – межсетевые экраны. И каждый из этих продуктов имеет своё развитие и некую эволюцию. Подобным примером может послужить компания Check Point, начинавшая с программного межсетевого экрана, теперь в продуктовой линейке имеет аппаратно-программные межсетевые экраны, а так же огромное количество продуктов закрывающих смежные задачи информационной безопасности, например, продукт для защиты конечных точек сети – Check Point Endpoint. Если проследить эволюцию продукта Check Point Endpoint - когда то это был продукт для защиты конечных пользователей от компании ZoneAlarm.

Эти примеры даны лишь для того, чтобы обозначить некое видение того, что не имеет смысла создавать продукт с ограниченным функционалом, закрывающим малое количество задач информационной безопасности. Но это не означает, что сразу должен быть создан продукт, закрывающий все задачи, просто необходимо изначально представлять себе то, как изначальный (возможно с малым функционалом продукт) будет эволюционировать. Gartner (ведущий обозреватель в мире IT) в обзоре Magic Quadrant for Enterprise Network Firewalls за2010 год обозначил как один из минусов отсутствие road-map и longer-term strategies, в этой связи хочется предложить выпускать продукт с заранее продуманным путём его развития.

Рынок информационной безопасности заполнен всевозможными продуктами по защите конечных точек сети, но продуктов, которые бы включали в себя некий важный для пользователя функционал, - мало, либо это совокупность продуктов, которая стоит дорого. Поэтому, в конечном итоге (или в некоторой не далёкой перспективе) необходимо, чтобы продукт Chronopay AV являлся продуктом для комплексной и всеобъемлющей защиты конечных точек сети. Для этого необходимо, чтобы продукт обладал следующими основными модулями –

- Модуль Защиты от Вирусов и Вредоносного ПО (Антивирус и Антишпион – могут рассматриваться как единый модуль или как два раздельных модуля).
- Модуль Персонального Межсетевого Экрана
- Модуль Выявления Выгодоприобретателя

А так же дополнительными модулями –

- Модуль Организации Удалённого Доступа (VPN Модуль)

- Модуль Шифрования Дискового Пространства
- Модуль Безопасного Веб-серфинга

6. Политика лицензирования

Что касается политики лицензирования, тут нужно разделить процесс продажи продукта на две части, а именно:

- На покупку самого продукта (Программного Обеспечения, а по закону Лицензии), и тут лучше придерживаться Модульного пути - когда покупатель выбирает необходимые модули и может приобрести как продукт с полным набором функционала, а так же продукт только с необходимым под его конкретные нужды набором функционала
- На покупку сервиса – имеется ввиду сервис обновления антивируса (сигнатур) и сервис поддержки или сопровождения пользователей (Maintenance или Support). Так же к Сервису можно отнести Модуль Выявления Выгодоприобретателя

В таком случае покупка продукта будет выглядеть так:

Пользователь покупает сам продукт (лицензию), который может содержать в себе сервис обновления на первый год и покупает поддержку к этой лицензии (Support) на год.

И могут быть возможны различные варианты покупки самого продукта и покупки поддержки.

Смысл модульной системы состоит в том, чтобы пользователь мог выбрать функционал покупаемого продукта и приобрести продукт с необходимым ему набором программных модулей.

Т.е. если пользователь хочет «только антивирус для своей рабочей станции» - то он покупает Chronopay AV с модулем защиты от Вирусов и Вредоносного ПО - минимально необходимая конфигурация (которая включает в себя подписку на обновление сигнатур атак на первый год). Покупает поддержку к этому продукту и пользуется.

Или если пользователь хочет «антивирус, контроль за приложениями и безопасный веб-сёрфинг» - то он покупает Chronopay AV с модулем защиты от Вирусов и Вредоносного ПО - минимально необходимая конфигурация (которая включает в себя подписку на обновление сигнатур атак на первый год), и докупает Модуль Персонального Межсетевого Экрана (для контроля за приложениями) и Модуль Безопасного Веб-серфинга.

И т.д. пользователь может покупать продукт под свои нужды.

При этом Модуль Выявления Выгодоприобретателя необходимо выполнить как подписку (как сервис, который необходимо покупать каждый год), а не как программный продукт.

Так же пользователь может приобрести продукт с полным набором функционала. Преимуществом такого полнофункционального продукта должна быть меньшая цена (в сравнении с таким же продуктом, покупаемым отдельно модулями) и, допустим, включённая подписка на сервис (обновления сигнатур) и поддержку (support) на первый год.

Какой смысл в разделении продукта на Лицензии и Подписки?

Лицензии как право передаются пользователю на неограниченный срок.

Т.е. купив продукт Chronopay AV с модулем защиты от Вирусов и Вредоносного ПО – пользователь может работать с ним всю жизнь. Но, если он не будет покупать подписку на обновление сигнатур, продукт не будет обновляться и смысл в его использовании пропадёт.

Что касается поддержки пользователей – этот сервис может приобретаться по желанию (если пользователь хочет получать поддержку).

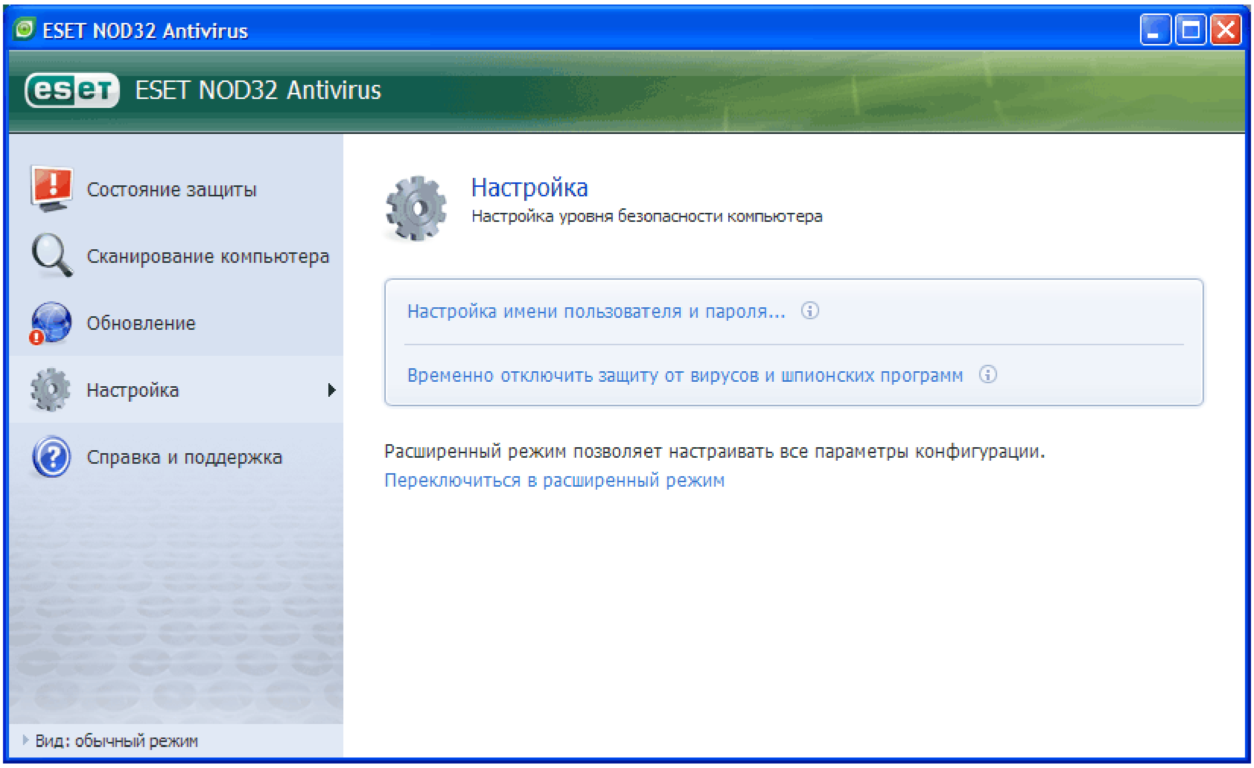
7. Техническое задание

Задача данной главы обозначить некое краткое Техническое Задание на предполагаемый продукт.

8. Интерфейс

Интерфейс создаваемого продукта должен быть простым и понятным, без лишних технических деталей.

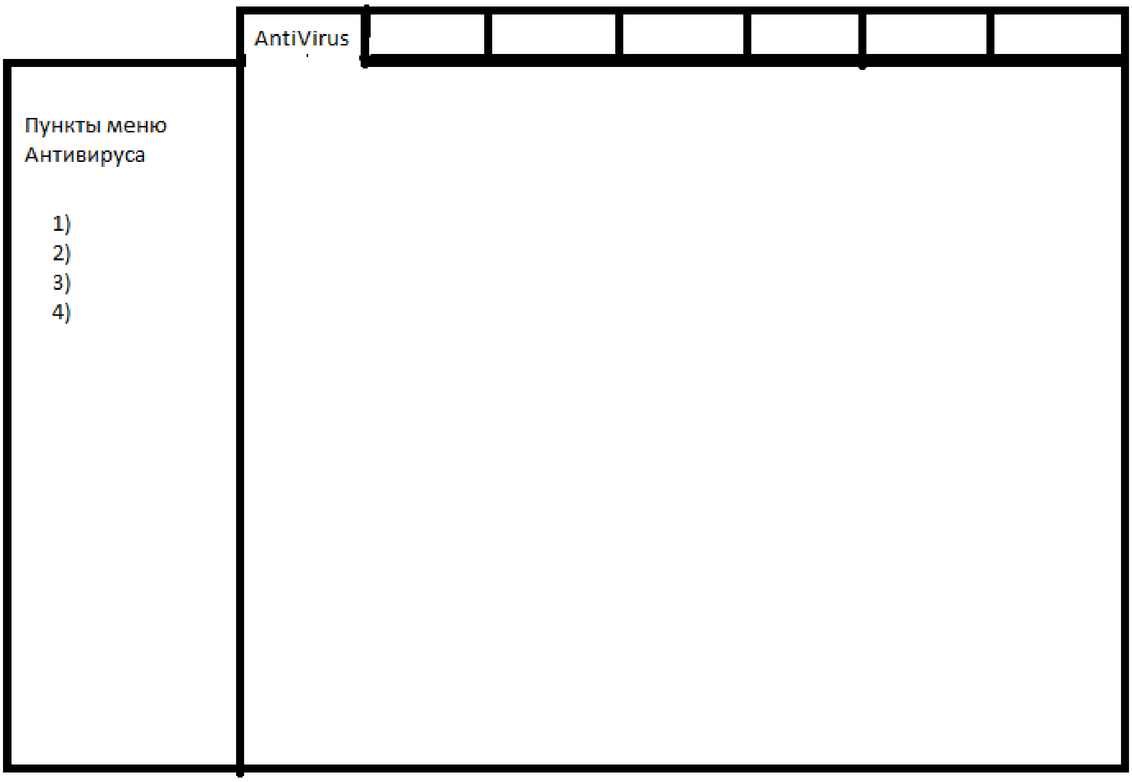
Примером может послужить антивирус Eset Nod32

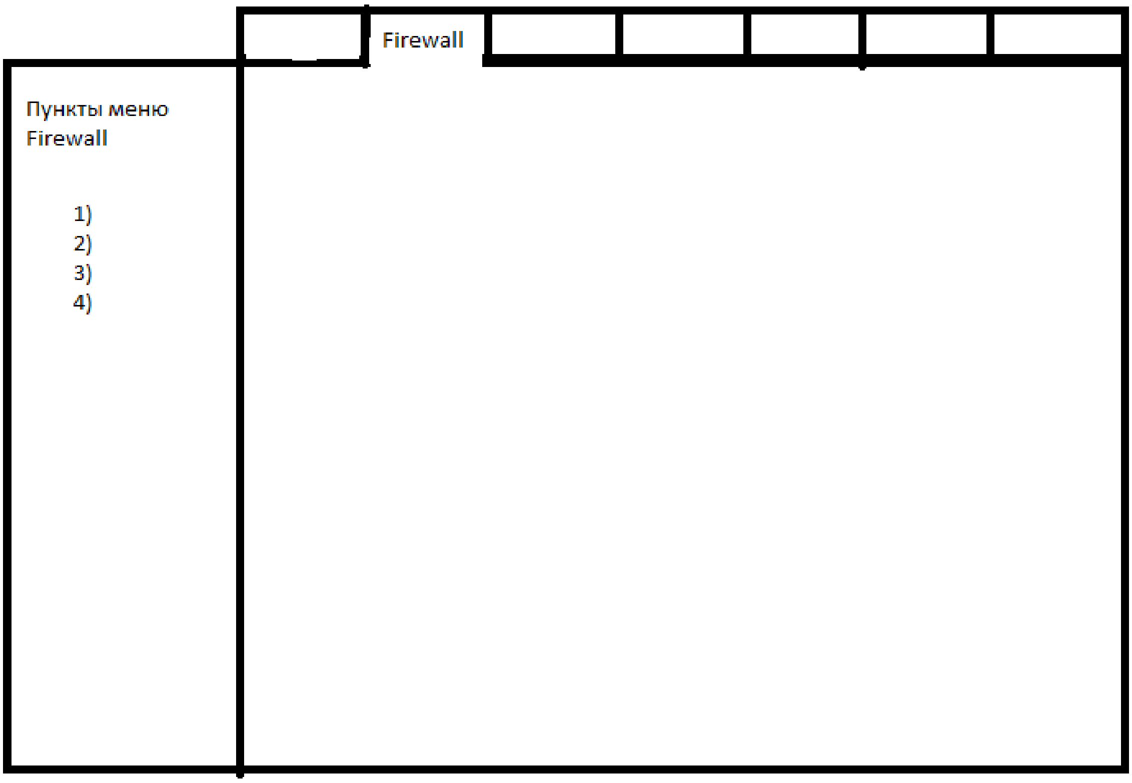


Или окно настройки Межсетевого Экрана (для домашнего использования Safe@Office) Check Point –

Применительно к Chrono AV , - сверху должны находится закладки с Модулями - Модуль Защиты от Вирусов,Вредоносного ПО, Модуль Персонального Межсетевого Экрана и т.д.

А слева пункты настройки и функционирования каждого модуля.





И т.д. по всем модулям.

9. Антивирус и Антишпионский модуль

Антивирусный и Антишпионский модуль должен обнаруживать и уничтожать вирусы, шпионское ПО, регистраторы клавиш, программы типа «троянский конь», руткиты и другие вредоносные программы, основываясь на комбинировании сигнатур, блокираторах поведения и эвристическом анализе. Должен обеспечивать высокие скорости обнаружения вредоносных объектов и ежечасное обновление сигнатур.

10. Персональный межсетевой экран

Персональный межсетевой экран должен блокировать нежелательный трафик, делать невидимым для злоумышленников конечные точки сети (компьютер пользователя) и предотвращать заражение компьютеров (домашней сети) вредоносным ПО.

11. Модуль Выявления Выгодоприобретателя

Модуль должен быть выполнен в качестве сервиса и должен добавлять пользователя в открытый список пользователей использующих данное ПО, а так же выполнять функции расследования инцидента возникновения нежелательного трафика или загрузки нежелательного ПО шпионского или рекламного характера с целью выявления и прекращения функционирования злоумышленника.

12.

13. VPN модуль

Модуль организации удалённого доступа (VPN Модуль) должен обеспечивать защищённый удалённый доступ к корпоративным ресурсам благодаря шифрованию и аутентификации данных, передаваемых во время сеансов удалённого доступа между конечной точкой сети и корпоративной сетью посредством набора протоколов IPsec.

14. Модуль Шифрования дискового пространства

Модуль шифрования дискового пространства должен обеспечивать эффективную защиту персональных данных на стационарных компьютерах, ноутбуках и переносных медиа-устройствах с помощью шифрования содержимого основными известными алгоритмами шифрования (AES, 3DES, ГОСТ 28147-89, Twofish).

15. Модуль Безопасного Веб-серфинга

Модуль безопасного Веб-Серфинга должен обеспечивать безопасность при поиске информации в сети Интернет и просмотре Веб-страниц, должен оберегать от Веб-узлов, которые могут нанести вред пользователю и его личным данным.