



Код безопасности
ГК «Информзащита»

Подтверждение международными экспертами надежности технологий защиты, использованных в Security Studio Endpoint Protection

Данная статья рассказывает о преимуществах использования SSEP не только для выполнения требований ФСТЭК, но и для осуществления защиты информации от современных актуальных угроз и о подтверждении высокого уровня надежности данной защиты международными экспертными организациями.

С вступлением в силу 152-ФЗ для многих компаний-операторов персональных данных стало актуальным обеспечить безопасность АРМ в корпоративной сети таким образом, чтобы выполнялись не только задачи защиты информации, но и требования закона «О персональных данных».

Для соблюдения этих требований и минимизации затрат организации на обеспечение защиты персональных данных, компания «Код Безопасности», являющаяся лидером по разработке сертифицированных средств защиты информации на российском рынке, включила в линейку собственных продуктов сертифицированный программный продукт Security Studio Endpoint Protection.

Благодаря Security Studio Endpoint protection организации получают возможность легитимно использовать автоматизированные системы при обработке персональных данных

Security Studio Endpoint Protection позволяет выполнить требования Федерального закона «О персональных данных» в части защиты информации в информационных системах с применением межсетевых экранов, антивирусов и средств обнаружения вторжений.

Компоненты	Защитные функции	Сертификаты
Персональный МЭ	Безопасный доступ в сеть	НДВ4, МЭ4
Антивирус	Защита от вредоносного ПО	НДВ4, ТУ
Средство обнаружения вторжений	Защита от неизвестных угроз	НДВ4, ТУ

Защита информации на АРМ выполняется благодаря следующим функциональным возможностям продукта:

Программный межсетевой экран с двусторонним контролем трафика предназначен для предотвращения вредоносных или нежелательных соединений компьютера в локальной сети или сети Интернет.

Компонент «Антивирус+Антишпион» предупреждает нежелательные и несанкционированные действия вредоносных программ.

Локальная безопасность (проактивная защита) Благодаря этой функции осуществляется контроль взаимодействия программ, предотвращаются неизвестные или подозрительные операции, и таким образом компьютер защищен от неизвестных угроз.

«Веб-контроль» отслеживает работу интерактивных элементов, встроенных в загружаемые веб-страницы или входящие почтовые сообщения, и разрешает или блокирует их выполнение.

«Внутренняя защита» необходима для того, чтобы противостоять попыткам вредоносных программ отключить средства защиты. С включенной внутренней защитой SSEP охраняет себя от остановки вирусами и шпионским ПО, а также обнаруживает и блокирует попытки имитации нажатия клавиш пользователем, которые могли бы привести к завершению работы.

Аудит событий безопасности События, связанные с работой SSEP, регистрируются и могут быть просмотрены с помощью журнала событий. В этом журнале хранятся сведения обо всех заблокированных или разрешенных соединениях, о специфической деятельности каждого компонента SSEP, о запуске каждой программы и всех изменениях, внесенных в политики продукта, его настройки и пароли.

«Антиспам» Самообучающиеся инструменты защиты от спама позволяют более эффективно распознавать ненужные письма в ходе работы.

Administration Center Данная функция позволяет произвести централизованную установку или обновление SSEP на рабочих станциях, удаленную настройку механизмов защиты и мониторинг событий безопасности. Данный компонент доработан специалистами компании «Код Безопасности» специально для обеспечения удобства использования SSEP в корпоративной сети организаций.

Почему SSEP является одним из самых надежных средств защиты информации среди программных решений для защиты данных на компьютерах в корпоративных сетях?

Доверие к надежности осуществляемой SSEP защиты информации со стороны компаний-пользователей основано в первую очередь на том, что SSEP разработан на базе проверенного средства защиты ПК разработки компании Agnitum и в качестве ядра использует лицензированную технологию Outpost Pro, получившую множество наград и признание у широкой аудитории экспертов и пользователей. Разработки компании Agnitum, легшие в основу SSEP, прошли ряд международных тестов и испытаний, в ходе которых Outpost Pro показал себя как одна из самых эффективных систем по защите персональных компьютеров.

Решением Outpost Pro были получены награды в следующих тестах:

1. Тест антивирусов на быстроедействие (февраль 2010, май 2011) портал Anti-malware.ru

В данном тесте исследовалось, какие персональные антивирусы оказывают наименьшее влияние на осуществление пользователем типовых операций на компьютере, потребляют минимальное количество системных ресурсов.



В ходе испытаний, технологии Outpost Pro завоевали золотую медаль по результатам тестирования скорости сканирования «по требованию» (измерялось время, затраченное на выполнение задачи сканирования набора файлов по требованию пользователя).



Также данными технологиями была получена серебряная медаль в тестировании за скорость сканирования в режиме реального времени (выяснялось насколько сильно «вмешательство» антивируса в файловые операции при запуске, создании, копировании или изменении файлов на жестком диске, замедляет работу системы).



В мае 2011 года, портал Anti-malware.ru повторно провел тестирование, в ходе которого измерялись и сравнивались параметры, которые оказывают непосредственное влияние на восприятие пользователем скорости работы антивируса. Технологии, реализованные в Outpost Security Suite Pro, получили 3 золотые медали, показав лучшие результаты.

2. Тестирование антивирусных решений (Апрель, Июнь, Август, Октябрь 2010), журнал Virus Bulletin

Британский журнал провел исследования (Апрель, 2010) по изучению эффективности антивирусных решений на платформе Windows XP SP3 по обнаружению вирусов (в том числе и полиморфных) и шпионских программ. Outpost Security Suite Pro завоевал награду VB100 в тестировании, успешно пройдя все испытания, обнаружив все вредоносные программы, используя помимо традиционного сигнатурного под-



хода к обнаружению вирусов, шпионского и рекламного ПО, механизмы активного поведенческого анализа.



В июне 2010, журнал Virus Bulletin провел очередное тестирование антивирусных решений на платформе Windows Server R2, в ходе которого технологии Agnitum завоевали награду, продемонстрировав прекрасную способность реагировать на заражение и обеспечивать проактивную защиту под Windows Server R2.



Также, по результатам испытаний журнала Virus Bulletin, прошедшим в августе 2010, продукт Outpost Security Suite Pro, получил еще одну награду, показав отличные результаты по обеспечению защиты на Windows Vista Business Edition.



В октябре 2010 технологии Agnitum были высоко оценены экспертами из Virus Bulletin и отмечены наградой за реактивные и проактивные свойства защиты и способность Outpost Pro обеспечивать высокую степень безопасности на всех современных Windows-платформах.

3. Тестирование на самозащиту на Windows7(x64) (январь 2011) и тестирование на защиту от внутренних атак (сентябрь 2011) портал Anti-malware.ru



В тестировании на самозащиту на Windows 7(x64) изучались возможности самозащиты комплексных антивирусных продуктов класса Internet Security от возможных атак. В ходе теста было выявлено, что Outpost имеет высокие показатели работы при противостоянии изменениям разрешений на доступ к файлам и ключам реестра, несанкционированному завершению процессов, удалению вирусных баз, изменению драйверов на Windows 7. При этом подтверждена полная поддержка 64-битных платформ с учетом их архитектуры и специфических особенностей обеспечения безопасности.



Тестовая лаборатория Anti-Malware.ru провела первый в своей истории «Тест фаерволов на защиту от внутренних атак», где в ходе испытаний выявлялась способность антивирусов к защите против стандартных внутренних атак, нестандартных уте-

чек, несанкционированного завершения процессов, а также нестандартных техник проникновения в режим ядра. Технологии компании Agnitum получили высокие оценки экспертов и завоевали 2 золотые медали в категориях с максимальными и стандартными настройками.

4. Тестирование антивирусных решений (Апрель, Июль, Август, 2011), журнал Virus Bulletin



Компания Agnitum, разработчик продуктов Outpost, удостоилась VB100. Тестирование, проведенное изданием Virus Bulletin на платформе Windows Vista x64, подтверждает проактивные защитные свойства продукта и его позиции как одного из лучших антивирусных продуктов в мире.



В каждом месяце по результатам тестов технологии, разработанные компанией Agnitum, получали наивысшие баллы и награды. Антивирус показал впечатляющие результаты в RAP-тесте на реактивное и проактивное обнаружение вредоносного ПО. Были отмечены отличные результаты обнаружения самых распространенных вредоносных программ и полиморфных вирусов.



Также, награда была вручена за успешное прохождение тестов на платформе Windows Server 2008 R2, и тем самым была доказана эффективность защитных свойств для всех распространенных операционных систем Windows.

Ядро Security Studio Endpoint Protection разработано с использованием технологий Agnitum, признанных одними из самых эффективных в области защиты. Таким образом, все высоко оцененные свойства Outpost Pro сохранены в сертифицированном про-

граммном решении Security Studio Endpoint Protection а именно:

1. Security Studio Endpoint Protection оказывает минимальное влияние на скорость работы АРМ и осуществление типовых операций пользователем. То есть, помимо высоких показателей производительности и успешного детектирования вредоносных программ, данный продукт гарантирует максимально низкую нагрузку на ресурсы ПК.
2. SSEP эффективно защищает АРМ от сетевых атак, как внешних, так и внутренних, при этом гарантирует защищенность целостности собственной системы от воздействия вредоносных программ, направленных на нарушение или подавление работы антивирусной системы.
3. Также SSEP с легкостью обнаруживают полиморфные вирусы, прекрасно осуществляет реактивное и проактивное обнаружение вредоносного ПО.
4. SSEP обеспечивает безопасность АРМ в режиме проактивной защиты, таким образом, предотвращает нарушение целостности системы, несанкционированный автозапуск заведомо опасных приложений, утечку данных, отслеживает шпионские программы, обеспечивая системе высокую производительность, стабильность и надежность.

Security Studio Endpoint Protection сочетает в себе передовые технологии в области защиты данных, которые, являясь основой SSEP, получили признание самых авторитетных тестовых лабораторий и журналов, и сертификацию ФСТЭК.

Таким образом, для обеспечения комплексной защиты рабочих станций организации и выполнения требований Федерального закона «О персональных данных» в части защиты информации с применением межсетевых экранов, антивирусов и средств обнаружения вторжений, следует оборудовать каждое АРМ таким программным средством защиты, как Security Studio Endpoint Protection.



Код безопасности

ГК «Информзащита»

Почтовый адрес: 127018, Россия, Москва, а/я 55.

Адрес офиса в Москве: ул. Образцова, д. 38.

Адрес офиса в Санкт-Петербурге: Свердловская наб., д. 44.

Тел.: +7 (495) 980-2345 (многоканальный).

Факс: +7 (495) 980-2345.

E-mail: info@securitycode.ru

Запрос дополнительной информации о продуктах: info@securitycode.ru

По вопросам стоимости и покупки продуктов sales@securitycode.ru

По вопросам партнерства и сотрудничества info@securitycode.ru

Вы можете узнать подробную информацию о продуктах на сайте

www.securitycode.ru

О компании «Код Безопасности»

Компания «Код Безопасности» – российский разработчик программных и аппаратных средств, обеспечивающих безопасность информационных систем, а также их соответствие требованиям международных и отраслевых стандартов. Продукты «Кода Безопасности» применяются во всех областях информационной безопасности, таких как защита конфиденциальной информации, персональных данных, коммерческой и государственной тайны, а также среды виртуализации. «Код Безопасности» стремится предоставить клиентам качественные решения для любых задач информационной безопасности, как традиционных, так и появляющихся в процессе развития высоких технологий.

«Код Безопасности» входит в группу компаний «Информзащита», которая уже около 15 лет является лидером российского рынка информационной безопасности.

ООО «Код Безопасности» ведет свою деятельность на основании лицензий ФСТЭК России и ФСБ России.